



LANDBANK

SERVING
THE NATION

**SUPPLEMENTAL/BID BULLETIN NO. 1
For LBP-HOBAC-ITB-GS-20211222-01(2)**

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

IMPLEMENTOR : **HOBAC Secretariat**

DATE : **July 15, 2022**

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

Modifications, amendments and/or clarifications:

- 1) The bidder/s are encouraged to use the Bid Securing Declaration as Bid Security.
- 2) The Terms of Reference (Annexes D-1 to D-26), Technical Specifications (Section VII), Omnibus Sworn Statement (Form No.6), List of LANDBANK Officers, Employees and Consultant(s) (Annexes E-1 and E-2) and Checklist of Bidding Documents (Item 12 of Technical Documents) have been revised. Please see attached revised various Annexes and specific sections of the Bidding Documents.
- 3) Responses to Bidders' Queries/Clarifications (Annexes F-1 to F-6).


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

SHARED CYBERDEFENSE SOLUTION (REBIDDING)

Terms of Reference (Insurance Cluster)

Version Number : 3
Date : 10 June 2022
Author : Government Service Insurance System
Bureau of the Treasury
Social Security System
Insurance Commission
Philippine Deposit Insurance Corporation

1. Name and Description of the Project

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

For this Terms of Reference (TOR), it will cover the Insurance Cluster composed of the Bureau of the Treasury (BTr), Government Service Insurance System (GSIS), Social Security System (SSS), Insurance Commission (IC), and 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 of endpoints (inclusive of servers) for each agency (i.e., BTr – 1,600, GSIS – 4,200, SSS – 8,000, IC - 1,000, PDIC – 1,200) and includes project management, consulting, requirements validation, customization, training, integration, production deployment, system integration, change management and other out-of-pocket expenses (e.g., transportation allowance, per diem, etc.);
- The Shared Defense subscription shall commence immediately after the Phase 1 implementation of the project.
- Post Go Live support starting from the implementation date; and
- All applicable taxes, service fees and charges (e.g., fund transfers fees, foreign exchange difference)

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

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

Other Requirements

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

3. Functional and Non-Functional Requirements

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

I. Functional Requirements

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

<ul style="list-style-type: none"> ▪ Remediation recommendations <p><i>*Response Time: How soon the security incident must be acknowledged by the service provider</i></p> <p><i>*Report Time: How soon a reference number/ problem ticket must be created by the service provider and received by the agency. The Report Time is included in the Response Time.</i></p>		
<p>7. Monthly monitoring service management:</p> <p>The service provider shall conduct regular meetings with the agencies IT stakeholders to review SOC performance and discuss the overall IT security posture of the agencies, including fine-tuning of configurations and provision of best practices advice, to aid in continuous improvement. Regular written reports must also be available to track the status of cases and the assistance needed. Monthly reports shall contain, but not limited to:</p> <ul style="list-style-type: none"> • SLA Performance • Correlated Events Overview • Correlated Events Graph Distribution Overtime • Correlated Events and Rules Triggered Summary • Summary of Incident Ticket per Use Cases Incident Management 		
<p>8. The service provider shall ensure flexibility and scalability of the agencies SOC platform and shall ingest and process all events sent by the agencies for the SIEM and SOAR requirements including its current and future needs.</p>		
<p>9. The service provider shall facilitate SOC security briefing at least once a month for the agencies to present the latest local and international news and updates in Cyber security.</p>		
<p>10. The Cloud based SOC shall be 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</p>		
<p>A.2 Managed Detection and Response</p>	<p>COMPLIED</p>	<p>REMARKS</p>
<p>A.2.1 Deployment and Management</p>	<p>Y/N</p>	
<p>1. The service provider shall supply Managed Detection and Response services, including the Endpoint Protection / Endpoint Detection and Response (EDR) licenses required for supported endpoints. Supported endpoints refer to Windows endpoints, Windows servers, major Unix and Linux distributions, MacOS, Mobile devices, that is still under support or extended support by the manufacturer.</p>		
<p>2. The solution must be categorized as a leader either in the latest Forrester Wave™ report for Enterprise Detection and Response or Gartner Magic Quadrant for Endpoint Protection Platforms.</p>		
<p>3. 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</p>		

environments.		
4. For non-supported systems, other means of monitoring must be performed, such as network detection and response (NDR or similar) tool shall be provided.		
5. 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.		
6. 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.		
7. 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.		
8. Update of Indicators of Compromise (IOC) and watchlist repository, whenever applicable		

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

1. The service provider must provide 24x7 Managed Threat Hunting Service, supported by experienced and certified analysts or incident responders for the remote response on endpoint incidents/events		
2. The service provider must have pre-built threat hunting applications and queries		
3. The service provider must be able to get context from indicators such as IP's, URL's, domains, or hashes using the tools within the platform, including associated events with unique visibility including account creation, login activity, local firewall modification, service modification, sources of remote operations (including scheduled task creations, registry changes, WMIC execution, among others)		
4. The solution shall be able to isolate "at-risk" endpoints, including the blocking the launching of suspicious or malicious applications.		
5. The solution shall allow blacklisting and whitelisting of hashes manually through the solution.		
6. The solution shall provide remote response by administrators, analysts, or incident responders such as containment, deleting files, killing process among others without the need for additional tools or agents.		
7. The solution shall provide root cause analysis of all identified malicious activity.		
A.3 Security Information and Event Management (SIEM)	COMPLIED Y/N	REMARKS
1. The solution provided must be 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)		
2. 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.		
3. 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.		
4. 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.		
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 have a 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 for at least twelve (12) months with comprehensive searchability. The retention of the logs shall be within the duration of the contract, after which, the logs will be archived and given to the agencies in an agreed format. The logs, including evidences of security incidents, should be tamper proof and made available for legal and regulatory purposes, as required.		
A.4 Security Orchestration, Automation and Response (SOAR)	COMPLIED Y/N	REMARKS
1. The solution must be able to integrate with the SIEM and fully orchestrate security operations and provide security teams with case management, automation, and investigation within a single pane of glass		
2. The solution must have visibility into the security operation provided via dashboards, KPIs and customizable reporting		
3. The solution must be able to support machine driven and analyst led response to remediate threats in a consistent and auditable manner		
4. The solution must render alerts, cases, query reports, and events into clustered and contextualized threat storylines with a high degree of visualization		
5. The solution must be an open architecture that allows for easy connectivity and integrations to any existing system, bringing them all together into a single, contextual language. Integration with other solutions can either be out of the box or customized.		
6. The solution must be able to accelerate security incident processes by automating or semi automating workflows		
7. The solution must be include out of the box or customizable playbooks of best practices to scale operations, drive consistency in response and meet compliance requirements. Playbooks deployed shall include at least: <ul style="list-style-type: none"> • Phishing enrichment and response • Malware endpoint response • Login Anomalies (multiple failed logins, unusual activity such as login attempts outside office hours, etc) • Unusual browsing activity • Web attack profiling and blacklisting 		
8. The solution should provide pre-set and customizable KPI metrics to monitor threat response efficacy and team performance.		

B. Vulnerability Management and Penetration Testing		
B.1 Vulnerability Management	COMPLIED Y/N	REMARKS
1. The solution provided must be a cloud based service, integrated within the SIEM, that shall give immediate global visibility into where the Agency IT system might be vulnerable to the latest Internet threats and how to protect them.		
2. It should be able to continuously identify threats and monitor unexpected changes in the network before they turn into breaches. The solution can be agentless or agent-based if continuous monitoring is required on specific systems.		
3. The solution should be able to scan systems anywhere in the Agency environment, from the same console: whether the asset is on the perimeter, the internal network, or cloud environments (such as Amazon Web Services, Oracle Cloud, Microsoft Azure or Google Cloud) with the ability to create custom reports showing each audience just the level of detail it needs to see.		
4. The solution should be able to identify and prioritize critical vulnerabilities and risks to enable the agencies to prioritize the remediation of the highest business risks using trend analysis, zero-day and patch impact predictions.		
5. The solution should be able to track vulnerability data across hosts and time, to give a better understanding of the agencies security posture. The reports can be changed through existing pre-built templates, without the need to rescan. The reports can be generated on demand or scheduled automatically and then shared with the appropriate recipients online, in PDF or CSV		
6. The solution should be able to automatically gather and analyze security and compliance data in a scalable backend, with provisioning additional capabilities as easy as checking a box.		
7. The solution should be able to proactively address potential threats whenever new vulnerabilities appear, with real-time alerts to notify the agencies immediately, without the need to schedule scan windows or manage scanning credentials.		
8. The solution must be able to conduct a continuous compromise assessment, which shall include at the minimum: <ul style="list-style-type: none"> • Identification of the specific vulnerabilities, at risk, and/or compromised assets • Evaluation of scanned assets and identification of possible vulnerability linkages through a detailed analysis of the results 		
B.2 Vulnerability Assessment and Penetration Testing (VAPT)	COMPLIED Y/N	REMARKS
1. Vulnerability Assessment and Penetration Testing (VAPT) shall be performed annually on an agreed schedule and scope with the agencies. The VAPT scope may include network infrastructure, applications (e.g., public-facing web and mobile applications), Application Programming Interfaces (APIs), endpoints, hosts and databases, including member service systems or kiosks, if any and among others.		

<p>2. The service provider shall deliver and maintain a vulnerability database with relevant software version upgrades and security policy update recommendations, inclusive of changes to existing and new vulnerability and threat signatures.</p>		
<p>3. The service provider shall provide online reporting and metrics capability:</p> <ul style="list-style-type: none"> • VAPT results/data (including risk, remediation status, and data compromised, if any) and access to historical test result and trend analysis delivered via the service provider's portal shall be accessible to the agencies. This would also include handholding with the agencies concerned to properly remediate/mitigate vulnerabilities, findings, and observations. 		
<p>4. The service provider shall have predefined fields/templates for the generation of reports, such as, but not limited to:</p> <ul style="list-style-type: none"> • VAPT Report (i.e., Executive Summary, Conclusion for Management Area, and Specific Action Plans) • Security Profiling Results (including reports from automated scanning tools) • Detailed observations and recommendations 		
<p>5. Common Vulnerability Scoring System values:</p> <ul style="list-style-type: none"> • The service provider shall use CVSS v3.0 or later for risk ranking and prioritizing security vulnerabilities. 		
<ul style="list-style-type: none"> • The service provider shall be capable to generate multi-format reports, including exporting of report data in PDF, Microsoft Excel, XML, CSV, and HTML. 		
<p>6. The service provider shall perform Host discovery and Operating System (OS) fingerprinting functionalities for the following, but not limited to:</p> <ul style="list-style-type: none"> • Windows (all versions) • Linux and other Unix flavors (all versions) • Network and security related equipment, whether software or hardware-based • User profile settings • Advanced password analysis 		
<p>7. The service provider shall perform common service discovery and fingerprinting functionalities for the following, whether on-premise or cloud-based:</p> <ul style="list-style-type: none"> • Application servers • Authentication servers • Backdoors and remote access services • Backup applications/tools • Database servers • Active Directory, Lightweight Directory Access Protocol (LDAP) • Domain Name Systems (DNS) • Mail servers and Simple Mail Transfer Protocols (SMTP) • Network File Systems (NFS), Network Basic Input/Output System (NetBIOS) and Common Internet File Systems (CIFS) 		

<ul style="list-style-type: none"> • Network Time Protocols (NTP) • Remote Procedure Calls • Routing protocols • Simple Network Monitoring Protocol (SNMP) • Telecommunications Network (Telnet), Trivial File Transfer Protocol (TFTP), Secure Shell (SSH) • Virtual Private Network (VPN) • Web and mobile applications • Web servers 		
---	--	--

C. Threat Intelligence	COMPLIED	REMARKS
1. The solution shall deliver threat intelligence on the following:		
• 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		
• Unlimited Site take downs during the duration of the contract(i.e., phishing, social media sites, and others)		
• 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:		
• 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: <ul style="list-style-type: none"> • Escalation process • Incident containment process • Incident eradication process • Incident recovery process • Incident identification process • Process flow 		

2. The service provider shall act as the Incident Response (IR) Manager and facilitate the six (6) phases of IR. The service provider must be on-call and will conduct the IR activities onsite, as necessary (i.e., in cases of breach). The IRs per agency shall cover 200 accumulated hours per year. Beyond the required 200 hours, the agencies shall shoulder the cost. In case the 200 hours allotted for IR is not fully or not consumed, it can be converted to other services, such as training among others, that the provider can render for information security.		
3. The service provider shall conduct an annual, or as needed, IR readiness training to the agencies Computer Security Incident Response Teams (CSIRT), including IT security awareness trainings to both technical and non-technical audiences of the agencies. The readiness training shall include best practices recommendation in isolation, containment, and remediation activities of the security incident.		
4. The service provider shall conduct an annual, or as needed, incident response drill or simulation exercises with the agencies-CSIRTs to improve detection and internal readiness for cyber security incidents. This will include internal and external incident communications, reduced impact on operation continuity, reporting to regulators (e.g., NPC, DICT), CSIRT readiness, blue team capability, tabletop exercises, among others.		
5. The Service Provider shall map security playbook and runbooks for applicable security use cases to guide client on their incident response.		
6. The service provider shall deliver technical assistance to the agencies CSIRTs during emergency (successful) breach response.		
7. The Service Provider shall have a facility to receive client's reported incident (via authorized point of contact from client) for incidents not captured on the monitoring tool.		
8. The service provider shall deliver network/firewall/web applications breach response.		
9. The service provider shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks.		
10. The service provider shall deliver root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities.		
11. The service provider shall identify indicators of compromise and scan the network to search for other related infected systems.		
12. The service provider shall deliver insider threat investigation, as needed.		
13. The service provider shall deliver employee misconduct investigations, as needed.		
14. The service provider shall deliver incident and investigation reports.		
15. The service provider shall have a certified and recently trained (at least in the past 12 months) in-house cyber security forensics specialist, to support advanced investigation.		
16. The service provider shall assist in the following: <ul style="list-style-type: none"> • Incident handling preparation and execution • Crisis management • Breach communication • Forensic analysis including preservation of evidence for chain of custody 		

requirements • Remediation		
17. The Service Provider shall rate the prioritization and severity of security incidents and create a service ticket as per agreed Service Level Agreement (SLA).		

Service Level Agreement (SLA)							
1. Acknowledgement SLA - The Acknowledgement SLA Percentage shall be computed per month base on the total number of missed hours exceeding the Acknowledgement SLA guarantee of fifteen (15) minutes per incident							
<table border="1"> <thead> <tr> <th>Service Level Target</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>98%</td> <td>Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket.</td> </tr> </tbody> </table>		Service Level Target	Description	98%	Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket.		
Service Level Target	Description						
98%	Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket.						

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

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

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

II. Non-functional Requirements

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

enterprise management software that allows for maintenance and access control management.		
6. The service provider shall provide physical and environmental controls at the primary and secondary sites for this project.		
7. The agencies data shall be logically separated by using unique tagging to ensure segregation of data from the other agencies. The agencies should retain as the legal owner of the data processed and managed by the service provider.		

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

C. Service Provider's Qualification and Requirements	COMPLIED Y/N	REMARKS
<i>Note: Submission of required documents shall be during the submission of bids.</i>		
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 have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service), with at least 20 IT or Information Security related certified onsite support engineers within Metro Manila.		
3. The service provider must have local sales and technical offices in the Philippines. The service provider must submit the list of local sales and technical offices in the Philippines. This is subject for actual site visit to the facility.		
4. The Security Operations Center (SOC) with their SOC analysts 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. 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.		
5. 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.		
6. 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		

<p>provider must have a SOC 2 Type II Attestation Report done at least in 2021, to ensure controls related to security, availability, processing integrity, confidentiality and privacy are in place.</p>		
<p>7. The service provider shall ensure that the data ingested from the insurance cluster is not shared or disclosed to or accessed by parties not mentioned in the contract unless explicitly granted permission by the cluster.</p>		
<p>8. The winning bidder shall be required to demonstrate the salient features of the proposed Shared Cyber Defense solution at the Project Site or via online.</p>		

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

<p>6. Threat Containment (Using Existing EDR or agreed process) 7. Incident Response/Recommendations</p> <ul style="list-style-type: none"> • 1-Tier 3 senior analyst who will be responsible to manage critical incidents. Tier 3 analysts are also responsible for actively hunting for threats and assessing the vulnerability of the business. <ul style="list-style-type: none"> 1. Manage High Severity Triage 2. Incident Response and Forensics Capabilities 3. Threat Containment (Using Existing EDR or agreed process) 4. Reporting and Post Incident Review 5. Use Case Development 6. Threat Searches 7. New Correlation Rules • 1-Tier 4 analyst or the SOC manager, who will be in charge of strategy, priorities and the direct management of SOC staff when major security incidents occur. The SOC manager will also be responsible for the management of the MSOC operations for the agency and cluster. 		
<p>5. The service provider should ensure that there will be alternate personnel deployed to the cluster should the primary personnel be unavailable for whatever reason.</p>		
<p>6. Qualifications</p>		
<ul style="list-style-type: none"> • Project Manager: <ul style="list-style-type: none"> • Must be with the service provider's organization at least one (1) year before the bid opening • Has handled project management for at least two(2) financial corporations. • Must provide a list of projects handled in the last 5 years, indicating the Project Name and Project Duration (Start date and end-date). • Must have a valid project management certification • SOC Manager/Tier 4 Analyst: <ul style="list-style-type: none"> • Must be with the service provider's organization one (1) year before the bid opening • 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 (GCDNA), GIAC Web Application Penetration Tester (GWAPT), GIAC Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Intrusion Analyst (GCIA), Cisco 		

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

4. Delivery Time/Completion Schedule

The Project must be implemented by phases: Phase 1 - Threat Intelligence, Security Monitoring and Management and Incident Response , 45 working days from the issuance of the Notice to Proceed, Phase 2- Vulnerability Management, 65 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.

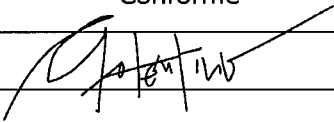
All deliverables shall become the property of the concerned agencies.

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:

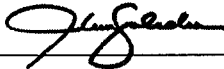
Milestone	Percentage of the Total Contract Price
Year 1:	
Upon implementation of Threat Intelligence, Security Monitoring & Management, and Incident Response for the Insurance Cluster (Phase 1)	15%
After Phase 1 and upon implementation of Vulnerability Management for the Insurance Cluster (Phase 2)	15%
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:	
Upon Insurance Cluster issuance of Certificate of Completion and Acceptance of the License subscription covering another period of 12 months (2nd Year)	50%
TOTAL	100%

Insurance Cluster TWG:

	Conforme
Head: AVP Archie Tolentino (LBP)	

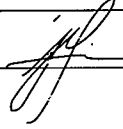
[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Insurance Cluster TWG:

Member:	
1. BTr - Mr. Thomas Solido	


[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Insurance Cluster TWG:

Member:	
2. GSIS - Mr. Jonathan Pineda	

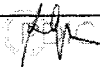
[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Insurance Cluster TWG:

Member:	
3. SSS - Ms. Jocelyn Dela Peña	

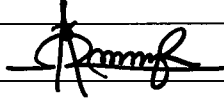
[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Insurance Cluster TWG:

Member:	
4. PDIC - Ms. Maria Belinda San Jose	 Digitally signed by Gonzales Renar Mojica Date: 2022.07.13 14:41:56 +08'00'

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Insurance Cluster TWG:

Member:	
5. IC - Mr. Jason Ampoloquio	

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Technical Specifications

Specifications	Statement of Compliance										
<p style="text-align: center;">Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster (Lot 2)</p> <table border="1" data-bbox="185 1258 783 1476"> <tr> <td>1. Bureau of Treasury</td> <td>1,600 endpoints</td> </tr> <tr> <td>2. Government Service Insurance System</td> <td>4,200 endpoints</td> </tr> <tr> <td>3. Social Security System</td> <td>8,000 endpoints</td> </tr> <tr> <td>4. Insurance Commission</td> <td>1,000 endpoints</td> </tr> <tr> <td>5. Philippine Deposit Insurance Corporation</td> <td>1,200 endpoints</td> </tr> </table> <p>Phase 1:</p> <ul style="list-style-type: none"> ▪ Threat Intelligence ▪ Incident Response ▪ Security Monitoring and Management <p>Phase 2:</p> <ul style="list-style-type: none"> ▪ Vulnerability Management and Penetration Testing <p>Notes:</p> <p>1. Minimum technical specifications and other requirements per attached revised Terms of Reference (Annexes D-1 to D-26).</p>	1. Bureau of Treasury	1,600 endpoints	2. Government Service Insurance System	4,200 endpoints	3. Social Security System	8,000 endpoints	4. Insurance Commission	1,000 endpoints	5. Philippine Deposit Insurance Corporation	1,200 endpoints	<p style="text-align: center;">Statement of Compliance</p> <p>Bidders must state below either “Comply” or “Not Comply” against each of the individual parameters of each Specification preferably stating the corresponding performance parameter of the product offered.</p> <p>Statements of “Comply” or “Not Comply” must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer’s un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.</p> <p style="text-align: center;">Please state here either “Comply” or “Not Comply”</p>
1. Bureau of Treasury	1,600 endpoints										
2. Government Service Insurance System	4,200 endpoints										
3. Social Security System	8,000 endpoints										
4. Insurance Commission	1,000 endpoints										
5. Philippine Deposit Insurance Corporation	1,200 endpoints										

LBP-HOBAC-ITB-GS-20211222-01(2)

2. The documentary requirements enumerated in Section 3.II.C (Service Provider's Qualifications/Requirements) and Section 3.II.D (Personnel Qualifications/Requirements) of the **revised TOR** shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements.

Nor-submission of the above documents may result in the post-disqualification of the bidder.

**Please state here either
"Comply" or "Not Comply"**

Conforme:

Name of Bidder

Signature over Printed Name of
Authorized Representative

Position

Form No. 6

Omnibus Sworn Statement

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.

AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. *[Select one, delete the other:]*

[If a sole proprietorship:] I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

[If a partnership, corporation, cooperative, or joint venture:] I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. *[Select one, delete the other:]*

[If a sole proprietorship:] As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

[If a partnership, corporation, cooperative, or joint venture:] I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, **by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;**

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. *[Select one, delete the rest:]*

[If a sole proprietorship:] The owner or sole proprietor is not related to the following LANDBANK Officers, employees and consultants: 1) members of the Board of Directors; 2) President and CEO; 3) members of the Head Office Bids and Awards Committee (HOBAC); 4) members of the Technical Working Group, if applicable; 5) personnel of Procurement Department; 6) personnel of the implementing unit or the end-user unit; and 7) project consultants, if applicable, by consanguinity or affinity up to the third level degree;

[If a partnership or cooperative:] None of the officers and members of [Name of Bidder] is related to the following LANDBANK Officers, employees and consultants: 1) members of the Board of Directors; 2) President and CEO; 3) members of the Head Office Bids and Awards Committee (HOBAC); 4) members of the Technical Working Group, if applicable; 5) personnel of Procurement Department; 6) personnel of the implementing unit or the end-user unit; and 7) project consultants, if applicable, by consanguinity or affinity up to the third level degree;

[If a corporation or joint venture:] None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the following LANDBANK Officers, employees and consultants: 1) members of the Board of Directors; 2) President and CEO; 3) members of the Head Office Bids and Awards Committee (HOBAC); 4) members of the Technical Working Group, if applicable; 5) personnel of Procurement Department; 6) personnel of the implementing unit or the end-user unit; and 7) project consultants, if applicable, by consanguinity or affinity up to the third level degree;

7. *[Name of Bidder]* has no unsatisfactory performance with its ongoing projects:
8. *[Name of Bidder]* complies with existing labor laws and standards; and
9. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:
 - a. Carefully examining all of the Bidding Documents;
 - b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
 - c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
 - d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.
10. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.
11. In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

IN WITNESS WHEREOF, I have hereunto set my hand this ___ day of ___, 22__ at _____,
Philippines.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

SUBSCRIBED AND SWORN to before me this _____ day of _____, in _____,
Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her [insert type of government identification card used], with his/her photograph and signature appearing thereon, with no. _____ and his/her Community Tax Certificate No. _____ issued on ___ at _____.

Witness my hand and seal this ___ day of *[month]* *[year]*.

Notary Public

Doc. No. _____;
Page No. _____;
Book No. _____;
S. of _____.

The names of specific LANDBANK officers, employees and consultants being referred to are shown in revised Annexes E-1 to E-2.

List of LANDBANK Officers, Employees and Consultant(s)

A. Board of Directors

Ex-Officio Chairman: Sec. Benjamin E. Diokno, Department of Finance
 Vice Chairperson: Ms. Cecilia C. Borromeo, President and CEO
 Members: Pres. Ferdinand R. Marcos Jr., Department of Agriculture
 Sec. Bienvenido E. Laguesma, Department of Labor and Employment
 Sec. Conrado M. Estrella III, Department of Agrarian Reform
 Mr. Virgilio D. Robes, Representative - Agrarian Reform Beneficiaries Sector
 Mr. Jaime L. Miralles, Representative - Agrarian Reform Beneficiaries Sector
 Ms. Nancy D. Irlanda, Representative - Private Sector

B. President and CEO: Ms. Cecilia C. Borromeo**C. Bids and Awards Committee (HOBAC)**

Chairman: Mr. Reynaldo C. Capa, First Vice President – Banking Services Group
 Vice Chairman: Mr. Alwin I. Reyes, Vice President – Procurement Department
 Regular Members: Ms. Adelfa R. Masacupan, First Vice President – Asset and Liability Management Group
 Mr. Emmanuel G. Hio, Jr., Vice President – Facilities Engineering Services Group
 Ms. Esperanza N. Martinez, Vice President – Public Sector Department
 Ms. Elenita C. Rapanut, Vice President - Branch Banking Services Department
 Provisional Member: Atty. Joseph Dennis C. Castro, Legal Manager - Legal Services Group

D. HOBAC Secretariat

Head: Atty. Honorio T. Diaz Jr.
 Officers and Staff: Ms. Remedios S. Lacaden, Senior Management Associate
 Ms. Ruby S. Cortez, Acting Procurement Specialist III
 Ms. Farah Eva B. Esguerra, Administrative Specialist II
 Ms. Maribel J. Paredes, Procurement Specialist I
 Mr. Mark Anthony C. Pantalla, Procurement Analyst
 Ms. Jenica V. De Vicente, Procurement Assistant
 Mr. Jerome C. Relucio, ASO I

E. Technical Working Group

AVP Archie Tolentino (Land Bank of the Philippines)
 Mr. Thomas Solido (Bureau of Treasury)
 Mr. Jonathan Pineda (Government Security Insurance System)
 Ms. Jocelyn Dela Peña (Social Security System)
 Ms. Maria Belinda San Jose (Philippine Deposit Insurance Corp.)
 Mr. Jason Ampoloquio (Insurance Commission)

F. Procurement Department

Head: Mr. Alwin I. Reyes, Vice President
 Officers and Staff: Ms. Ma. Victoria C. Viray, Acting Senior Procurement Officer/Team Leader
 Ms. Rosemarie S.J. Mirando, Acting Senior Procurement Officer/Team Leader
 Ms. Leonor F. Santos, Acting Senior Procurement Specialist/Team Leader
 Mr. Joel R. Perez, Acting Senior Procurement Specialist/Team Leader
 Ms. Helen S. Purificacion, Acting Senior Procurement Specialist/Team Leader
 Mr. Donato DR. Cariaga, Acting Senior Procurement Specialist/Team Leader
 Ms. Kristi Ann P. Rutab, Acting Senior Procurement Specialist/Team Leader
 Atty. Karla May M. Temporosa, Administrative Officer
 Mr. Rommel C. Pascua, Acting Procurement Specialist III
 Ms. Cathrina Marie A. Garcia, Acting Procurement Specialist III
 Mr. Ruel V. Marca, Procurement Specialist II

Mr. Rosalino V. Cruz, Procurement Specialist II
Ms. Lubelle B. Lumabas, Procurement Specialist II
Ms. Nadia G. Ileteo, Procurement Specialist I
Mr. Jerome V. Bueno, Acting Procurement Specialist I
Ms. Ma. Angela Q. Emeterio, Procurement Analyst
Ms. Jeramae F. Concepcion, Procurement Analyst
Ms. Kimberly Joy A. Sto. Tomas, Procurement Analyst
Mr. Jollianzen Jenkin G. Dy, Procurement Analyst
Ms. Charmaine F. Mangilit, Procurement Analyst
Ms. Jeah Crysel L. Escalona, Procurement Analyst
Mr. Marlon R. Faraon, Acting Procurement Analyst
Mr. Aaron V. Sedanto, Procurement Analyst
Mr. Rudyrick B. Silva, Administrative Analyst
Ms. Fretch Camille J. Japole, Procurement Assistant
Mr. Mark Anthony M. Abad, Administrative Assistant
Ms. Almay Joyce B. Ruz, Procurement Assistant
Ms. Ma. Theresa N. Cruz, Acting Executive Assistant
Mr. Roman R. Eala, ASO I
Mr. Jesus David, SCW
Mr. Emil Dela Cruz, SCW
Mr. Erikson Guani, SCW
Mr. Vicente Gutierrez, Jr, SCW
Mr. Andrew Palma, SCW
Mr. Dexter Naguit, SCW
Mr. Ramil Pendilla, SCW
Mr. Frederick Reyes, SCW
Mr. Pablo Tenoria, SCW

G. Implementing/End-user Unit:

Head:

Officers and Staff:

Checklist of Bidding Documents for Procurement of Goods and Services

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

Eligibility and Technical Components (PDF File)

1. The Eligibility and Technical Component shall contain documents sequentially arranged as follows:

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

Legal Eligibility Documents

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

Technical Eligibility Documents

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

Financial Eligibility Documents

5. The prospective bidder's audited financial statements, showing, among others, the prospective bidder's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the

preceding calendar year which should not be earlier than two (2) years from the date of bid submission.

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

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

- **Other Documents to Support Compliance with Technical Specifications [must be submitted inside the first bid envelope (Eligibility and Technical Component)]**
- 14. Current Certifications from the manufacturer that Service Provider is a certified/ authorized reseller of the brand being offered.
- 15. Information Security-related certifications of the onsite support engineers.
- 16. List of local sales and technical offices in the Philippines.
- 17. TIA-942 Rated 3 Facility Certification.
- 18. Certifications of the SOC analysts.
- 19. SOC 2 Type II Attestation Report.
- 20. Certifications of the network and security engineers.
- 21. Documents regarding the Project Manager:
 - Company ID
 - Certificate of employment
 - List of projects handled
 - End-User/Client company name of the projects handled
 - Project Name and Project Duration (Startdate and end-date).
 - Project Management Certification
- 22. Documents regarding the SOC Manager/Tier 4 Analyst:
 - Company ID
 - Certificate of employment
 - List of engagements
 - Any two (2) of the unexpired professional certifications in the Insurance Cluster Terms of Reference.
- 23. Documents regarding the Team Lead/Tier 3 Analyst:
 - Company ID
 - Certificate of employment
 - List of engagements
 - Any two (2) of the unexpired professional certifications in the Insurance Cluster Terms of Reference.
- 24. Documents regarding the Team Member/Tier 2 or Tier 1 Analyst:
 - Company ID
 - Certificate of employment
 - List of engagements
 - Any one (1) of the unexpired professional certifications in the Insurance Cluster Terms of Reference.

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

Financial Component (PDF File)

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

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

Bidder	Query/Clarification	Responsible	Reply
Cloud4C	<p>1. Is there any preference of 1 option over the other? Cloud-based over local? Local over cloud-based? As indicated in respective sections?</p> <p>a. "Local" technology center (SOC facility)</p> <ol style="list-style-type: none"> i. AnnexD, Page15, Section 3.11.C.2 <p>b. "cloud-based" SOC facility</p> <ol style="list-style-type: none"> i. AnnexD, Page15, Section 3.11.C.4 ii. AnnexD, Page3, Section 3.1.A.1.1 iii. AnnexD, Page4, Section 3.1.A.1.10 iv. AnnexD, Page8, Section 3.1.B1.1 <p>2. Will hybrid SOC facility be allowed, i.e. combination of cloud-based and local facilities?</p> <p>3. For any SOC facility platform (local, cloud-based or hybrid), do all technical resources (PM, SDM, Experts, Engineers, etc.) need to be local (in-country)? Or some can be remote (off-shore)?</p> <p>4. Onsite support engineers are required as stated in AnnexD, Page15, Section 3.11.C.2. In the case of full cloud-based SOC facility, will remote/off-shore engineers & experts be accepted? Full or partial?</p> <p>5. Can a detailed list of endpoints from each entity be shared</p> <ol style="list-style-type: none"> a. Quantity b. Type (server, firewall, switches, storage, etc) c. Web/public URLs d. Operating system e. Private IPs f. Public IPs g. Location (on-premise, AWS cloud, Oracle cloud, etc?) h. Databases i. Front-end: desktop, laptop 	TWG	<p>This facility refers to the service provider's local technology operation center where their Information Security related certified onsite support engineers shall operate from.</p> <p>b. This refers to the SOC platform for the cluster, where the solutions shall integrate, and it must be cloud based.</p> <p>The SOC platform must be cloud based, however the facility where the personnel providing support to the cluster are operating from, must be located locally.</p> <p>As stated in Section 3.11.C.2, they will be located within Metro Manila.</p>
TIM	<p>1. Will IVA for 4 Entities be allowed? What are the conditions if any?</p> <p>2. For item C. Service Provider's Qualification and Requirements, under Manufacturers Certification (Reseller/Distributor), can we provide Manufacturers Certification that we are certified MSSP for a specific solution for the requirement that is requiring services only like the VMPT part.</p>	LBP HOBAC	<p>IVA for 4 entities is allowed as long as they are compliant with the IVA provisions of RA 9184.</p> <p>As mentioned in the TOR, the certification requirements refer only to brands offered as part of the project.</p>
		TWG	<p>Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)</p>

Bidder	Query/Clarification	Responsible	Reply
	3. For SOC - To scope the volume of alerts, how many network devices (fw, routers), servers (application servers), is expected to be monitored by the SOC?	TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)
	4. For VM/PT: How many assets to be assessed (vulnerability management) and pen-tested? Web applications? Mobile applications? Servers? Workstations?	TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)
	5. For VM/PT: How frequent is the pen-testing schedule?	TWG	Pen-testing is annual as indicated in the TOR
	6. For VAPT: How many mobile apps, web apps, APIs, and kiosk (if any) for each agency? Please indicate the mobile app platform to be tested – Android and/or IOS for each mobile app.	TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)
	7. On item 5.2.1 – Vulnerability Assessment and Penetration Testing (VAPT) shall be performed annually on an agreed schedule and scope with the agencies. The VAPT scope may include network infrastructure, applications (e.g., public-facing web and mobile applications), Application Programming Interfaces (APIs), endpoints, hosts and databases, including member service systems or kiosks, if any and among others.	TWG	
	Q1. Annually means once a year VAPT of the assets in-scope?	TWG	Yes
	Q2. Are Kiosks like ATM?	TWG	Yes
	8. For Vulnerability Management, does it include OT and IOT (Operational Technologies and Internet of Things)	TWG	No
	9. For Access Management, item A. 2, we assume the MFA will be provided by each Agency? What is the existing MFA of each Agency?	TWG	MFA to be provided by vendor
	10. For Access Management, item A. 5, we assume that VPN and Internet/MPLS will be provided by each agency?	TWG	Agency will work with provider to establish vpn and connectivity to the SOC platform (Agency Side)
	11. For Access Management, item A. 6, this primary and secondary site is referring to SOC facility?	TWG	Yes, this is the service provider facility.
	12. For this engagement who will technically own the license subscription? The service provider or the agencies?	TWG	Agencies
	13. For C. Service Provider's Qualification and Requirements, item no. 4, aside from TIA-942 Rated 3 Facility Certification, what are the other certs that can be provided? Can we provide SOC 2 Type II Cert for this requirement as well?	TWG	SOC 2 Type II Attestation report is also part of the requirement
	14. Under B. Training and Other Requirements, how many attendees per agency?	TWG	Up to five (5) per agency
	15. Under D. Personnel Qualifications/Requirements, can 2 persons fulfill the certificate requirement for SIEM, SOAR and VM, if they have these 3 certs?	TWG	No. There must be at least 2 certified personnel for each of the solutions required: SIEM, SOAR, and vulnerability management. The identified personnel cannot be listed on more than 1 solution.
	Can we request the breakdown of Endpoints per Agency?	TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)

Bidder	Query/Clarification	Responsible	Reply
	Entity/Total # of Endpoints #Laptop/Desktop#Server#Mobile SSSB0000 GISB2000 BTB6000 PDI/CM2000 ICB0000	TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)
CYBERQ GROUP, INC.	For the VAPT requirements: 1. May we ask for at least just a count of mobile and web apps? This to come up with a commercially viable proposal? - How many mobile apps, web apps, APIs, and kiosks (if any) for each agency? Please indicate the mobile app platform to be tested – Android and/or iOS for each mobile app 2. On Item 5.2.1 - 1. "Vulnerability Assessment and Penetration Testing (VAPT) shall be performed annually on an agreed schedule and scope with the agencies. The VAPT scope may include network infrastructure, applications (e.g., public-facing web and mobile applications), Application Programming Interfaces (APIs), endpoints, hosts and databases, including member service systems or kiosks, if any and among others."	TWG TWG TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB) Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)
	Q1: Annually means once a year VAPT of the assets in-scope? Q2: Are kiosks like ATMs?	TWG TWG	Yes Yes
	3. For VM. Is this only for the internal and external infrastructure/networks?	TWG	This will include all endpoint count of assets per agency.
	4. Does it include OT and IoT (Operational Technologies, Internet of Things)?	TWG	No
	5. Can we have 4 or more companies in the JV?	LBP HOBAC	JVA for 4 entities is allowed as long as they are compliant with the JVA provisions of RA 9184.
	6. For the training part – how may attendees per agency?	TWG	Up to five (5)
	- 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.		
	Once a month? What is the frequency?	TWG	At least once a month, unless there is a critical risk that must be escalated to the agencies.
TTSDI	1. May we please request the breakdown of the endpoint to following:	TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)

Bidder	Query/Clarification	Responsible	Reply
	Entity/Idba1 # of Endpoints: Laptop/Desktop Server Mobile SSS0000 GISIS2002 BTR06002 PDI/CI2002 ICR00002	TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)
	2. To properly scope the SOC, We would like to request for the list of the network devices per agency to be onboarded (# of firewall, IPS/IDS, WAF, etc) 3. For VAPT, We would like to request for the following details per agency. a. # of Web applications b. # of Mobile applications c. # of API d. # of Kiosk and what is the operating System e. # of Databases	TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)
	4. Under Schedule of Requirement, Phase 1 delivery period of 45 days is very tight based on the number of endpoints to onboard. May we request that the 45 days delivery period is for pilot deployment only with at least 10% of the total endpoint per agencies are onboarded. The rest of the endpoints will be completed within 6 months period.	TWG	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.
	5. For the SIEM and SOAR, does the agency need admin access control or monitoring access only that has dashboard which shows the status and reports? How many users per agency need to be have access?	TWG	Monitoring only, however, request for dashboard addition or tuning can be requested.
	6. We would like to confirm that we may use our principal vendor personnel to implement and perform parts of the project/service as to leverage on their expertise like on the areas but not limited to services/product like Threat Intelligence, MDR, IR and the likes which shall be beneficial for all agencies strengthening their security posture?	TWG	Yes, however, they will not be counted as part of the local SOC team requirement.
TRENDS and TECHNOLOGIES			

Bidder	Query/Clarification	Responsible	Reply
	<p>1. A.1 Security Operations Center (SOC) Page 4 Item 10 The Cloud based SOC shall be hosted in a country where confidentiality of the information shall be ensured. The platform provider or country where the platform is hosted shall not be able to access or force the service provider to disclose the information without agency and/or cluster approval.</p>	TWG	<p>This is to be reworded to : 10. The Cloud based SOC shall be 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</p>
	<p>Question # 1, in our response where we will indicate "YES" for our compliance, what is the needed supporting documents for this?</p>		<p>2. A.2.1 Deployment and Management Page 4 Item 3 The solutions provider must be capable to deploy the endpoint technology to workstations D73and servers, including Windows, Mac, Unix and Linux assets, using the agencies or the solutions providers deployment tool, and must support both physical and virtual environments.</p>
	<p>2. A.2.1 Deployment and Management Page 4 Item 3 The solutions provider must be capable to deploy the endpoint technology to workstations and servers, including Windows, Mac, Unix and Linux assets, using the agencies or the solutions providers deployment tool, and must support both physical and virtual environments.</p>	TWG	<p>2. A.2.1 Deployment and Management Page 4 Item 3 The solutions provider must be capable to deploy the endpoint technology to workstations D73and servers, including Windows, Mac, Unix and Linux assets, using the agencies or the solutions providers deployment tool, and must support both physical and virtual environments.</p>
	<p>Question # 2.1 May we request the list of operating systems of all workstations and servers in each agency's environment including the quantity per OS of workstation and servers? Question # 2.2 In addition to question # 2.1, please provide for the breakdown of quantity of O.S. for all workstations and servers on each agency based on the declared total endpoint count.</p>		<p>Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)</p>
	<p>3. B.1 Vulnerability Management, Page 8 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 might be vulnerable to the latest Internet threats and how to protect them.</p>	TWG	<p>Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)</p>
	<p>Question # 3.1 Please expound the requirement of "WITHIN" in the statement "integrated within the SIEM" Does this mean that the Vulnerability Management should be the same brand/solution as that of the SIEM? Does with SIEM means that the SIEM should have a built-in Vulnerability Management capabilities and functionality? Or does this mean that the VM can be a different brand/solution as that of the SIEM brand/solution but can be integrated?</p>		<p>The vulnerability management must be able to integrate with the SIEM, not necessarily the same brand.</p>
<p>PERIMETER ESSECURITY PHLS</p>	<p>1. For SOC To scope the volume of alerts, how many network devices (fw, routers), servers (application servers), is expected to be monitored by the SOC?</p>	TWG	<p>Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)</p>

Bidder	Query/Clarification	Responsible	Reply
	2. For VMPT: How many assets to be assessed (vulnerability management) and pen-tested? - web applications - mobile applications - servers - workstations	TWG	Details shall only be provided to the Lowest Calculated Responsive Bid (LCRB)
	3. For VMPT: How frequent is the pen-testing schedule?	TWG	Annual

OTHER CHANGES TO THE TOR, BASED ON SUMMARY OF CHANGES PREVIOUSLY SUBMITTED BUT NOT CAPTURED

From

3.I.A.10
 10. The Cloud based SOC shall be hosted in a country where confidentiality of the information shall be ensured. The platform provider or country where the platform is hosted shall not be able to access or force the service provider to disclose the information without agency and/or cluster approval.

To

10. The Cloud based SOC shall be hosted in a provider categorized as a leader either in the latest Forrester Wave™, Public Cloud Development And Infrastructure Platforms report or Gartner Magic Cloud Quadrant for Cloud Infrastructure and Platform Services

3.II.C

(add item 7 and 8)

(Add)

7. 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.
 8. The lowest calculated bidder shall be required to demonstrate the salient features of the proposed Shared Cyber Defense solution at the Project Site or via online.