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: Agency: BTr — Scope: 7 External resources, up to 80 IP addresses Agency: GSIS — Scope: 20 External resources, 2 mobile apps, up to 80 IP addresses Agency: SSS — Scope: 25 External resources, 1 mobile app up to 150 IP addresses Agency: PDIC — Scope: 8 External resources, up to 80 IP addresses
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

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 wherethe 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 totalnumber 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 existingtools 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 onboardedin 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/orrisk(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 be provided 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) 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)? 10. Is there an internal threat data collection process in place?	8. VAPT shall include authenticated and unauthenticated scans. 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. 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? 12. What is the network interface required? 13. Do you require a dual PSU for theNDR appliance	11. This information shall ONLY beprovided to the winning bidder. 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

ANNEX H-4

<table>
<tr><td>4.</td><td>Not specified in the submitted queries</td><td>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?</td><td>14. This information shall ONLY beprovided to the winning bidder

15. This information shall ONLY beprovided to the winning bidder</td></tr>
<tr><td>5.</td><td>Not specified in the submitted queries</td><td>Non-technical questions

1. Why is IC included in the list forVAPT Scanning?

2. Where can we get Annex D1 toD25?

3. Can we have the documents digitally signed or do we need tohave a wet signature?

4. Do we need to counter-sign eachpage?

5. Is consortium allowed?

6. Kindly confirm indicate whether theprice mentioned is inclusive or exclusive of VAT.
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.

12. In the RFP document we see two pricing tables with detailed breakdowns asking</td><td>1. IC is not part of the project anymore. The requirement shall be:

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

<table><tr><th>Agency</th><th>Scope</th></tr><tr><td>BTr</td><td>7 External resources, up to 80 IP addresses</td></tr><tr><td>GSIS</td><td>20 External resources, 2 mobile apps, up to 80 IP addresses</td></tr><tr><td>SSS</td><td>25 External resources, 1 mobile app up to 150 IP addresses</td></tr><tr><td>PDIC</td><td>8 External resources, up to 80 IP addresses</td></tr></table>
Can be provided by LANDBANK Procurement Department thru email.

Either of the two is acceptable

No, only those portions as required in the bidding documents, must be signed by authorized representative/s as designated per Secretary's Certificate
Yes, in the form of Joint Venture Agreement by and between multi-parties

The ABC is VAT inclusive

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.

There are two (2) schedules provided in the bidding documents, however, the bidder may choose which is</td></tr>
</table>

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.
		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 sub-contracting 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 ofmonitoring must be performed, such as network detection and response (NDR or similar) tool shall be provided."	Part of our offer is to provide NDRsolution 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 forthe 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 #-6

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 ofautomation 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, andprojects they were involved in for the dedicated 24x7 x 365 team that will be assigned to the Insurance Cluster" .	The disclosure of the required information is critical for the proper assessment /evaluation of the bidder with the Lowest Calculated and Responsive Bid.
		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?	

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.

ANNEX H-8

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 bythe bidder.

ITEMNO.	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 eachagency 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.

ITEMNO.	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, maywe know what deployment tool the agencies will provide to be used?	Agencies can use their available software deployment tool, if any, ordeployment 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 beat 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 ordocument 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 whenyou say "leased" to the agencies? Is there any specific solution you requirefor Access Management? **Question 2:** Since there are multiplesolution stacks in this project, can weask 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 providedby the Insurance Cluster Agencies. May we know what is the MFA that willbe 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 BasedSOC 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 willbe provided only refers to the brand thatwill be provided to the agencies? Brandsfor (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 forthe 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 theircertifications only?	Please refer to the documents that willbe submitted during post-qualification.
11.	Under D. Personnel	Can we clarify what does "dedicated" means? Is he only should be assignedto 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, 2Tier-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 willbe submitted during post-qualification.
14.	Under D. Personnel Qualifications/Requir em ents > Item 6 > ProjectManager	For Project Manager Certificate, wouldeither Certified Associate in Project Management (CAPM) or Project Management Professional (PMP) be acceptable?	PMP certification will be required as thiscertification ensures that the Project Manager has extensive experience andadvanced project management skills and capabilities.
15.	Under B. Training and Other Requirements	How many attendees will be inclusive inthe 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 Agencystart 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 Clusterwithin 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 nceimmediately after the Phase 1 implementation of the project."	Does this mean the 2 years subscription, will start on the day 1 ofimplementation?	Yes. Upon the implementation of Phase1 - 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 wouldrequest the NTP for all the Agency willstart at the same time.	NTP shall be released by the memberagencies 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) forthe 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 TechnologiesInc.)	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 agencies security posture.	*Does this dashboard pertain to the SOC Dashboard 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 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:	*: Is this face-to-face meeting? Who will attend this regular meeting?*	The meeting should be face-to-face, with option to attend online. At least (2) representatives from the member agencies should attend.

ANNEX H-12

	• 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 data ingestion shall be as follows: Agency | Daily Event Log Aggregate Size in Gigabytes (GB) BTr | 17 GB GSIS | 24 GB SSS | 45 GB PDIC | 15 GB	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.

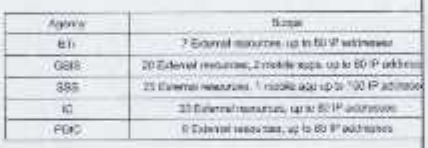
ANNEX H-13

		3.3 Will SIEM log sources be centralizedor accessible in Head Office?	This is not specified in the TOR. TheSIEM 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 monthlybasis?*	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 operatingsystems of these endpoints?*	This information will ONLY be provided to the winning bidder.

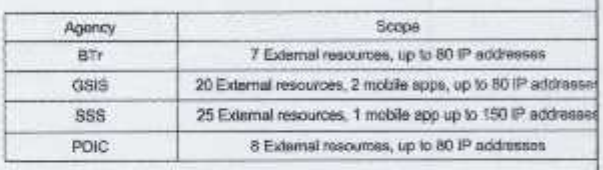
ANNEX H-14

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?* *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*	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. Yes.

ANNEX H KS

	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

ANNEX H-16

	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 mixof application servers?* ***11.2** : If the external resources pertain toweb applications, can we assume that the number of external resources pertainto FQDNs? If not, kindly provide the totalnumber of FQDNs.* ***11.3.** We noticed that the Insurance Commission (IC) was not considered onthe number of servers and desktops under page 2 and daily event logs underpage 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: 
12.	Page 11, Section VII. Technical Specification, under C. ThreatIntelligence 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. IncidentResponse 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, tosupport advanced investigation.	***13.1.** Are you referring to specific certifications (e.g. Computer HackingForensic 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 12months)?*	Any certification related to cyber-securityforensics will be accepted. We will accept a valid certification, which should indicate a validity date. Otherwise it should be issued at least inthe past 12 months.

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

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. Canyou explain more about this requirement?*	The requirement pertains to the physicaland 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/infrastructu re and service), with a pool of at least 20 IT or Information Security related certified onsitesupport engineers within Metro Manila. Alist 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 statedon the Item no. 3 below D. Personnel Qualifications / Requirements?* 3. The service provider must submit the following for all the personnels to be assigned duties and failure to submit the any of the requirement below to in any disqualification: • Resume/CV of the Proposed Personnel • Company ID • Certificate of employment	Yes.
16.	Page 16, Section VII. Technical Specification, under C. Service Provider's Qualification and Requirements Item 5. The SOC canbe provided on the cloud or within the premises of the serviceprovider. Should the Security Operations Center (SOC) with theirSOC 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, which should 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 receiptof Notice To Proceed (NTP) by the winning bidder. The vendor must therefore providea project schedule which should present the project milestonesand deliverables at each milestone. License subscriptionswill start upon contract implementation.		
18.	Page 18 of the Termsof Reference, 6. Qualifications forProject manager • Project Manager: Must have a valid project management certification	***18.1**: Is this Project Management Professional Certification?*	Any valid project managementcertification 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 onthe 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