SHARED CYBER DEFENSE SOLUTION
Response to Queries from 16 February 2022 Pre-Bid Conference

QUERY/REQUEST	TWG RESPONSE
A. GENERAL QUERIES/REQUESTS:	
1. Request for bid submission extension	Request for extension of bid submission will not be accommodated.
2. SLCC - May we request that the SLCC requirement for aggregate contracts amounting to 50% of the ABC, come from 2 different entities in a Joint Venture Agreement?	Please see Section 5.3 of the attached revised Bid Data Sheet.
3. Section C.2 page 30 (TIA 942 Certification for SOCs in both the GOCCs and the ICs TOR): Could the TWG reconsider allowing Bidders with Data Centers provided by Cloud Service Providers to be included in the Bid. The TIA 942 Certification refers to companies that house their own data centers and refers to site location, the architectural and physical structure of the building, electrical and mechanical infrastructure, fire safety, and physical security, among other things.	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.
4. Incident Response Hours for both clusters: The 200 Incident Response hours per agency is excessive. May this be reduced to 100 hours per agency?	The 200 hours is the requirement of each agency. Should there be an excess from the 200 hours, the remaining hours shall be converted into trainings, among others.
5. What specific certifications are required for the 20 certified onsite support engineers?	Indicated in Item C.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, Security, Information Technology Infrastructure Library (ITIL), or any relevant product certification to the SIEM platform that Service Provider offer.*

QUERY/REQUEST	TWG RESPONSE
6. Is it possible to consider extending the validity of the SLCC from within 5 years to 10 years?	The original requirement is maintained.
7. Is there a geographical (Cloud region) restriction on the customer requirement?	The CSP should be hosted in an identified non-terrorist 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. Please state location.
8. Can the total number of servers including virtual servers of the Customer be provided?	The endpoints indicated in the TOR already include the servers.
9. Can a cloud solution be proposed?	Yes.
10. The service provider's SOC must be housed in a data center with at least TIA-942 Rated 3 Facility Certification. Can it be housed outside the Philippines?	Indicated in item C.5: *The service provider must have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service) and support with at least 20 certified onsite support engineers within Metro Manila.*
11. Is the SLCC negotiable?	Please see Section 5.3 of the attached revised Bid Data Sheet.
12. How much is the budget per Agency?	Budget per agency is indicated in the Invitation To Bid (ITB)
13. What is the SLCC requirement since it will be divided per agency on awarding? Do we need to join the bidding per agency?	Bidding is on a per lot basis: Lot 1 is for the GOCC/GFI Cluster, while Lot 2 is for the Insurance Cluster.
14. What is the expectation after 2 years it is ended since it was a cloud-based subscription?	Each agency has the option to extend the subscription and/or conduct another bidding of the subscription.
15. Can we get a certified Engineer from the Partners-Vendor	No.

QUERY/REQUEST	TWG RESPONSE
16. Are you allowed to have a presentation during the Bid Qualification.	No.
17. Can we do a proper sizing for the SIEM? a. Events per Second (EPS) for SIEM b. Can we install multiple SIEMs instead of one big SIEM? This is for performance and compartmentalization considerations. c. Server count for -siem d. Please fill-out the sizing Questionnaire	Details shall only be provided to the winning bidder.
18. SOAR a. How many analysts are deployed in SOC? b. Is it a 9 – 6 SOC or a 24 X 7 setup? c. What are the different compliances which the SOC must comply with? d. How many incidents does the soc observe daily? e. How many resolver Group are there? f. Please share the list of Servers (Web, APP, DB, R&D) which are integrated to your SIEM or any other log aggregator such as AV server, AD, patch management etc. g. What are the various Devices currently deployed in the SOC? h. How many Planned SOP's are there? i. How many sites and what are the environments that should be covered? (e.g. Production, HA, DR)? j. Actions per month, no. of users	a. Indicated in items C.2: *The service provider must have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service) and support with at least 20 certified onsite support engineers within Metro Manila.* b. Indicated in item A.1.2: *The service provider should have a 24 x 7 x 365 SOC with L1, L2 and L3 support.* c. The SOC must be compliant in local regulatory requirements, as well as to all applicable laws and regulations. In addition, kindly refer to item C.6: *SOC must also be certified to ISO 27001:2013 Information Security Management System (ISMS).* d. Data not yet available e. This will be assigned by service provider as long as they comply with the SLA

QUERY/REQUEST	TWG RESPONSE
	f. Public facing servers, internal servers, etc. Details can be provided to the winning bidder due to confidentiality. g. The SOC to be deployed will monitor perimeter and endpoint events h. The service provider will determine this. i. All endpoint count shall be the basis. j. Data not yet available
19. Can you provide the Asset Inventory list per agency? Do you have EPS or Log Volume ingestion per agency?	This shall be provided to the winning bidder.
20. Is SOC2 Type 2 and TIA 942 specific to the data centre hosting the SOC infrastructure. Eg. Microsoft Azure	The TIA 942 requirement is for the data center hosting, the SOC, and its analysts. However, if the service provider's SOC will be housed in a CSP, the SOC platform must guarantee at least 99.9% uptime or availability.
21. Is client already using any vulnerability scanning tool? If yes, which tool is it?	LBP, UCPB —Yes DBP, HDMF, PGC — None GSIS —Yes BTr, SSS, IC, PDIC — None The identification of the tool shall only be provided to the winning bidder.

QUERY/REQUEST	TWG RESPONSE
22. Can we please get a breakdown of the following tool types by agency which can be leveraged to deliver the service: a. SIEM b. EDR c. SOAR d. UEBA e. Vulnerability Management solution	This shall be provided to the winning bidder.
23. Are the mobile devices part of the number of endpoints cited in the RFP?	Yes.
24. Do we need two Secretary's Certificate? Or one will do?	For JVAs, each party must submit their respective Secretary's Certificate attesting to the designation of their respective authorized representative/s. Further, it is advised that the JVAs should specifically state the name of the person who is appointed as the lawful attorney-in-fact of the JV to sign the contract, if awarded, and the member who is the lead representative of the concerned JV per GPPB NPM No. 098-2004
25. We don't have DTI permit since SGV is a partnership.	DTI Permit is applicable only to sole proprietorship. For partnership, SEC Certificate on Recording of Partnership shall be submitted.
26. What other document can we provide to support that we are a local company? Will a PhilGEPS registration for foreign entities that will join our JV be required or will supporting qualification documents be sufficient?	Only PhilGEPS Certificate of Membership under Platinum Category shall be submitted in lieu of Class "A" documents per GPPB Resolution No. 15-2021
Under A.2 Managed Detection and Response - A.2.1 Deployment and Management 27. The solution works in a Virtual Desktop Infrastructure (VDI) environment. Is this a current or future requirement? Which agency is using VDI? Is this already included in the endpoint counts?	This is a current requirement.

28. The solution shall support Endpoint Detection and Response (EDR) functionality on Windows, Linux, Unix, and Mac Operating System (OS). Unix does not allow the installation of most modern software including EDR agents. If EDR agents can be installed on other devices which remotely access the UNIX systems such as MACOS, Linux, and Windows, can this be considered compliant?	EDR can be installed to supported systems. For non-supported systems, other means of monitoring must be performed, such as network detection and response (NDR or similar).

QUERY/REQUEST	TWG RESPONSE
29. Endpoint Protection, machine learning, behavior analytics and EDR including the remote response should be part of a one single agent and should not require multiple agent deployment. In the system process tree, the modules should not show multiple process entries. Our EPP and EDR are both from the same brand but it shows multiple processes depending on modules enabled. Based on our research, there is no vendor that uses only a single process tree. Can this item be modified to using the "Same brand" rather than "single agent that should not show multiple process"?	Endpoint Protection, machine learning, behavior analytics and EDR including the remote response should be part of the same brand.
30. The solution should support EDR for Mobile supporting Android and IOS from the same platform and without installing any additional management infrastructure How many mobile agents are needed per agency?	This shall be provided to the winning bidder.
31. EDR events should be enriched and correlated with service provider's own Threat Intelligence and not using any third-party Indicator of Compromise (IOC). Also, the solution should be one of the leaders in analyst Threat Intelligence reports. The only vendors in the leaders group for Analyst Threat Intelligence report are FireEye, Crowdstrike and Kaspersky. Does it mean that we are only limited to these vendors for EDR functionality? We have helped international government and law enforcement agencies, including Interpol, the United Nations, the FBI, and the US Department of Homeland Security, create security policies and apprehend many cybercriminals over the years. Trend Micro also runs the world's largest bug bounty program (ZDI) responsible for the disclosure of vulnerabilities since 2005. Can these two items be considered as proof of our leadership in threat intelligence?	EDR must be in the Analyst Threat Intelligence Report.

QUERY/REQUEST	TWG RESPONSE
32. Endpoint Security should not require any signatures to protect known and unknown attacks. It should be 100% based on Machine Learning and Behavior Patterns. Endpoint security should be owned by the service provider and not by a third party. We can use machine learning and behavioral analysis to protect against known and unknown threats. However, we still offer other techniques, and this includes signature-based protection. More security technologies are better than just relying on machine learning and behavioral patterns. Can we still comply if we also rely on signature-based but still provide Machine learning and behavior patterns capability?	Yes. As long as the solution is 100% based on machine learning and behavior patterns. Reliance on signature-based shall only be an add-on.
33. The Threat Intelligence service as part of the MDR shall be a leading threat intelligence in any of the third-party analyst. We have helped international government and law enforcement agencies, including Interpol, the United Nations, the FBI, and the US Department of Homeland Security, create security policies and apprehend many cybercriminals over the years. Trend Micro also runs the world's largest bug bounty program (ZDI) responsible for the disclosure of vulnerabilities since 2005. Can these two items be considered as proof of our leadership in threat intelligence?	Must belong to the leading Threat Intelligence in any of the third-party analyst report under A.2.3. Detection, #4.
34. Should be able to manage workflows including sorting, filtering, tracking status, assigning ownership, and creating commentary or annotations of alerts Assigning ownership is a roadmap feature for us. Can we comply with this feature if we commit to provide it?	No.
35. The MDR solution must have been in the industry for at least 5 years TM MXDR was productized 4 years ago. It was launched in 2018. However, we have been offering Threat Management services since 2011. Will this comply with the said requirement? Can this be relaxed to three (3) years?	No.

QUERY/REQUEST	TWG RESPONSE
36. Must be able to view the amount of time required to network contain and lift containment Is it possible to expound on this item through a use case? Will network containment status suffice for this requirement?	Yes. Network containment status shall suffice for this requirement.
37. Must be able to manage whitelisted IP addresses for network containment If this is a roadmap feature, can we comply if we commit to provide it?	No.
38. Other Items: There are agencies that already have existing tools for EPP, EDR, MDR. What happens if the Shared SOC project has been awarded to another security vendor who is not the incumbent of these agencies?	The Shared Cyber Defense solution shall serve as another layer of defense for the agencies.
39. Assuming the agencies will be allowed to use their existing tools until they've finished their existing contracts, are they required to shift to the other security vendor who won the Shared SOC bid?	The agencies' existing tools should be working in parallel with the Shared Cyber Defense solution.
40. Third Party Validation The solution should be a leader in both Endpoint Point Protection and EDR as per latest Forrester Report. Since Forrester Wave EDR 2021 does not exist, can Forrester Wave "Endpoint Security Software as a Service" be considered?	The basis shall be the 2020 Forrester Wave EDR or the latest available report.
41. The solution should be leader in the latest Gartner's Magic Quadrant for EPP. Can this be relaxed since our solution is an XDR and not an EPP. Currently, there's no Gartner review for XDR.	The solution should be leader in the latest Gartner's Magic Quadrant for EPP or any similar category related to security threat detection and incident response.
42. Referring to the SLCC requirement under Bid Datasheet ITB Clause 5.3: Please consider a completed contract of Information Technology Security SOFTWARE ONLY as similar contract for this project.	Please see Section 5.3 of the attached revised Bid Data Sheet.

QUERY/REQUEST	TWG RESPONSE
43. Referring to the schedule of requirements regarding the start of the subscription, may I know when is the issuance of Certificate of Acceptance. Is it along with the release of NTP?	Indicated in Item 5. Payment Milestone Certificate of Acceptance is on a per agency basis, after the implementation of each phase.
44. Referring to the Checklist under Other Documents to Support Compliance with Technical Specifications, should these come from the bidder or can come from our principals/distributor?	Indicated in item C.12 *The winning bidder shall likewise be required to submit a Certification from the manufacturer stating therein that the proposed solutions to be finally delivered per SCC Clause No. 4 of the issued Bidding Documents are fully compliant with the technical specifications stipulated under Section VII. Technical Specifications.*
45. What is the specific name of certifications that is being referred to the certificate below: Any two (2) of the unexpired professional certifications listed in the GOCC/GFI Cluster Terms of Reference. Is this an exam certification?	Indicated in item C. Personnel Qualifications/ requirements
46. Can the Principal Vendor of the Solution do the implementation without doing a JVA with them?	No.
47. What would be the approach to be undertaken with respect to the procurement aspect of both projects? What would Landbank's role be, a single procurement entity for both clusters? If yes, how will the license entitlements since each clusters will have 5 agencies each with varying endpoint count requirements? If no, then will the procurement be per agency for both clusters? If this is the case then procurement process timeline must be synched across agencies for uniform start dates per cluster	LBP will be the Procurement Agent for both clusters. License entitlements shall be by agency.
48. If the SIEM requirement is a cloud hosted based solution, should it be explicitly stated in the tender in which the solution provider should be taking care of its maintenance?	No need. Since the SIEM shall be provided by the vendor, the maintenance should also be included.

QUERY/REQUEST	TWG RESPONSE
49. If they will be requiring a SIEM cloud hosted solution, it normally requires to deploy a log collector software which will require a server/hardware. Can both clusters' respective agencies provide their own server/hardware? Or does the bidder will be expected also to provide the required server/hardware? If yes, should the tender also states explicitly to include into the SIEM requirements that the "log collection software and hardware that needs to be deployed for on-premise data sources collection should be provided as well by the bidder"?	Regardless of the service (in-Cloud or in-premise), the SIEM shall be provided by the vendor.
50. Should the proposed EDR and SIEM solution be open to other vendors that is included in either the Forrester or Gartner Magic Quadrant? This will help the Technical working group to have wider options on the required solutions instead of just focusing on the vendors that commands a price premium being part of the leaders' quadrant?	No.
51. Since the technology solution will be deployed to each agencies, should there be a central federated view of alerts coming from all the agencies? If yes, which agency will own the federated view?	No.
52. How many mobile devices per agency that requires installation of EDR?	This will be provided to the winning bidder.
53. Does each agency has existing Mobile Device Management (MDM) solution to deploy the EDR solution for their mobile devices? If none, then will the agency be expected to deploy the agents manually?	No. The agency, together with the vendor. is expected to deploy the agents manually.
54. Does each agency has existing software deployment tool (i.e. SCCM) to deploy the EDR software across their endpoints and servers?	GOCCs/GFIs - Yes Insurance Cluster - Partial
55. The ToR only provides the user/endpoints counts per agency, does it mean that we should just estimate the sizing only based on the number of endpoints? We need to know the number of existing security devices the each agencies need to be integrated to our proposed SIEM to be able to provide the sizing and costing.	This will be provided to the winning bidder.
56. How many Firewalls for each agencies? We need this to properly size the SIEM.	This will be provided to the winning bidder.
57. How many IPS for each agencies? We need this to properly size the SIEM.	This will be provided to the winning bidder.
58. How many VPN device/s for each agencies? We need this to properly size the SIEM.	This will be provided to the winning bidder.

QUERY/REQUEST	TWG RESPONSE
59. How many Anti-virus (EPP) solution for each agencies? We need this to properly size the SIEM.	This will be provided to the winning bidder.
60. How many Active-Directory servers for each agencies? We need this to properly size the SIEM.	This will be provided to the winning bidder.
61. How many Web proxy devices for each agencies? We need this to properly size the SIEM.	This will be provided to the winning bidder.
62. Please provide the other security perimeter tools and its counts that each agency wanted to be integrated with the proposed SIEM. We need this to properly size the SIEM.	This will be provided to the winning bidder.
63. How much is the total Internet bandwidth of each agencies? We need this to properly size the SIEM.	This will be provided to the winning bidder.
64. Does each agencies have an existing SIEM solution? Is it on-prem SIEM? Please provide the number of the agencies that has existing SIEM.	This will be provided to the winning bidder.
65. For Threat Intelligence, how many digital assets (domains, IP ranges, cloud storage, sub domains, name of executives, brand names, logo's, social media sites, and "key words") to be covered by Threat Intel?	This will be provided to the winning bidder.
66. May seek for an extension for 2 weeks (March 16, 2022)? To allow us time to get approval from our clients of completed projects.	No.
67. May we know the inventory of the devices of all the Data Centers that will be part of this project, no. of endpoints have been defined but not complete inventory and details	This will be provided to the winning bidder.
B. GOCC/GFI CLUSTER	
1. EDR ownership (A.2.2 Prevention page 5 of the GOCC TOR): We would like to request that the TWG reconsider this item as it will severely limit the number of SOC that can participate. There are providers that specialize in providing the SOC services and not necessarily in the creation of security technology. These SOCs display expertise in a number of security tools that would be advantageous given a project with a wide scope.	The provision of ownership does not only mean "developed/created" by the service provider, however, it should be owned by the service provider.

QUERY/REQUEST	TWG RESPONSE
2. Are the GFIs willing to negotiate on a different SLA?	No.
3. Aside from the number of endpoints, can we get the list of devices/systems to be in scope?	This will be provided to the winning bidder.
4. For the SOC and SOC Team, is it dedicated to the GFI and IC but shared across agency? Or SOC and SOC Team are dedicated per agency?	Shared across agencies.
5. Do the agencies need to access and administer the SOAR? Or just monitoring (MSSP to share dashboard for monitoring)?	The agencies must have a dashboard for monitoring.
6. Does the SOC needs to integrate to the existing ticketing/ITSM per agency for their internal workflow and ticketing requirements? Or MSSP SOC will just use its own ticketing system?	No need to integrate. The service provider shall provide a ticketing tool.
7. For the regular meetings with the agencies, should it be per agency? Or just one session per month for example for all agencies?	Per agency, per cluster, and as the need arises.
8. For the Endpoint Security/EDR requirement, what if the agency already has one? Do we need to replace it or just integrate it to our SOC?	The Shared Cyber Defense project shall serve as another layer of defense for the agencies. The service provider must be able to integrate the agencies' existing endpoint security/ EDR requirement.
9. For the Endpoint Security/EDR requirement, can you provide the list of operating systems in scope?	Indicated in item A.2.1.3: *The solution shall support Endpoint Detection and Response (EDR) functionality on Windows, Linux, Unix, and Mac Operating System (OS).*
10. For the SIEM log archiving , should it be on MSSP SOC or in the premise of agency? If in the premise of the agency, who will provide the archiving storage?	Archiving is part of the scope to be provided by the service provider
11. For the SIEM requirement, what if the agency has existing SIEM? Do we replace it or just manage it?	The service provider's SIEM should be able to connect to the agency's SIEM through API.

QUERY/REQUEST	TWG RESPONSE
12. For VM and VAPT a. What is the method of testing (whitebox, greybox, blackbox). Or we can recommend it? b. Preferred time of testing (off hours or office hours) for the intrusive type of VAPT? c. Preferred time of testing (off hours or office hours) for the non-intrusive. Type of VAPT? d. How many Ips will be tested for the following: (1) External VAPT i. Number of External Ips? ii. Number of URLs? (2) Mobile App VAPT i. Number of Mobile Apps? ii. Does this apps use an API? If yes, do we need to included scanning of APIs? (3) Internal VAPT i. How many Internal Ips and Subnets? ii. Number of URLs?	VM and VAPT details shall be discussed and with the winning bidder.
13. For threat intelligence how many assets are we looking at (combination of names, VIP emails, credit cards, etc.)?	To be discussed and agreed upon by the service provider and the agency.
14. Can we utilize/integrate existing VPN and MFA of the agency?	To be discussed and agreed upon by the service provider and the agency.
15. Under TOR (GOCC) — Section C: Service Provider's Qualification and Requirements: #2. The service provider must have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service) and support with at least 20 certified onsite support engineers within Metro Manila. a. Does this requirement pertain only to the local vendor submitting or the GOCC will accept the assigned resources to be deployed by our Principals/Partners? b. Can the requirements include support engineers from our Principals & Disti Partners, as the 20 manpower requirements is very hard to comply. c. Is the 20 support team different from the SOC analyst?	At any given time, there must be 20 certified onsite support engineers. The 20 certified onsite support engineers are inclusive of the SOC analysts.

QUERY/REQUEST	TWG RESPONSE
16. #4. The service provider's SOC must be housed in a data center with TIA-942 Rated 3 Facility Certification. Does collocation of the SOC in either Globe or ePLDT data center acceptable to meet the Data Center TIA-942 Rated Facility Certification?	Yes, acceptable.
17. For Personnel Qualifications/Requirements: One (1) Project Manager One (1) Team Lead At least One (1) Team Member a. Can the BAC relax the 1 year tenure requirement since the resources are still for hire? b. Can the BAC accept that all these personnel are from our principals and or Distributor Partner?	a. No. b. Yes, acceptable.
18. Under Schedule of requirements, does LBP expect to finish the deployment of 7,600 endpoints side by side with the other agencies within 65 working days?	All deployments shall be simultaneous with the other agencies.
19. Under Schedule of requirements, does Bureau of Treasury expect to finish the Lot 2 deployment side by side with the other agencies within 65 working days?	All deployments shall be simultaneous with the other agencies.
20. GOCC (GFI) – page 4; A.2.1 – Deployment and Management The solution is capable to deploy endpoint technology to workstations and servers, including all versions of Windows, Mac, Unix and Linux assets. As per online bid clarification which the TWG responded and confirmed, endpoints with legacy OS (end of support) shall be considered as unsupported devices and will be excluded. Further, the TWG has agreed also on the proposal that unsupported endpoints shall only cover monitoring to which existing network-based solutions (monitoring and prevention solutions) of a particular agency will be used. May we also confirm that open-source OS and other multitasking, multiuser computer operating systems to which are mostly used for specific applications shall be classified also as unsupported devices and same as legacy OS, it will be excluded?	OS covered: 1) Windows 7 and up 2) Windows Server 2012 and up 3) Linux 6.3 and up 4) Unix

QUERY/REQUEST	TWG RESPONSE
"As per online bid clarification the TWG responded … As all endpoint security solutions are dependent on the operating systems lifecycles (eg end-of-support announcement of the OS types and versions), and there are some instances where critical systems are not allowed by to install endpoint agents. Can we request that unsupported devices will be excluded and propose to include in the security monitoring watchlist instead? For a Service Provider we shall provide recommendations to utilize any existing network-based controls of each agencies in the detection and/or prevention of such threats for unsupported devices?	
21. GOCC (GFI) – page 4; A.2.1 – Deployment and Management The solution shall support Endpoint Detection and Response (EDR) functionality on Windows, Linux, Unix and Mac Operating System (OS). As per online bid clarification which the TWG responded and confirmed, endpoints with legacy OS (end of support) shall be considered as unsupported devices and will be excluded. Further, the TWG has agreed also on the proposal that unsupported endpoints shall only cover monitoring to which existing network-based solutions (monitoring and prevention solutions) of a particular agency will be used. May we also confirm that open-source OS and other multitasking, multiuser computer operating systems to which are mostly used for specific applications shall be classified also as unsupported devices and same as legacy OS, it will be excluded?	OS covered: 1) Windows 7 and up 2) Windows Server 2012 and up 3) Linux 6.3 and up 4) Unix

QUERY/REQUEST	TWG RESPONSE
22. GOCC (GFI) — page 5; A.2.1 Deployment and Management The solution should support EDR for Mobile supporting Android and IOS from the same platform and without installing any additional management infrastructure. Please confirm that this item is covered in the total endpoints declared by each agency May we also confirm that the supported Android and IOS versions are required by each agency that it is updated?	Yes, covered in the count of endpoints. To be discussed and agreed upon by the service provider and the agency.
23. GOCC (GFI) — page 5; A.2.1 Deployment and Management EDR events should be enriched and correlated with service provider's own Threat Intelligence and not using any third-party Indicator of Compromise (IOC). Also, the solution should be one of the leaders in analyst Threat Intelligence reports Since we understand that every financial service put emphasis on security effectiveness of an endpoint solution, does this pertain to the Forrester or Gartner leadership on Threat Intelligence Services in addition to what is stated on A.2.7 Third Party Validation?	Yes.
24. GOCC (GFI) — page 5; A.2.1 Deployment and Management The solution must be able to conduct a continuous compromise assessment, which shall include at the minimum: • Identification of the specific vulnerabilities and/or compromised assets • Evaluation of scanned assets and identification of possible vulnerability linkages through a detailed analysis of the results • Update of Indicators of Compromise (IOC) and watchlist repository, whenever applicable	No.

QUERY/REQUEST	TWG RESPONSE
Since part of the requirement is Threat Hunting stated on items in Section A.2.4 and is similar to the compromise assessment requirement and is a more of proactive tactic for security, can we remove this item instead?	
25. GOCC (GFI) – page 5; A.2.2 Prevention Machine Learning and Behavior IOA patterns should have support for Windows, Mac, Unix, and Linux and other non-supported or legacy endpoints. Same with items in A.2.1 (Items 1 and 3) As per online bid clarification which the TWG responded and confirmed, endpoints with legacy OS (end of support) shall be considered as unsupported devices and will be excluded. Further, the TWG has agreed also on the proposal that unsupported endpoints shall only cover monitoring to which existing network-based solutions (monitoring and prevention solutions) of a particular agency will be used. May we also confirm that open-source OS and other multitasking, multiuser computer operating systems to which are mostly used for specific applications shall be classified also as unsupported devices and same as legacy OS, it will be excluded?	OS covered: 1) Windows 7 and up 2) Windows Server 2012 and up 3) Linux 6.3 and up 4) Unix
26. GOCC (GFI) – page 6; A.2.3 Detection The Threat Intelligence service as part of the MDR shall be a leading threat intelligence in any of the third-party analyst report. Since we understand that every financial services put emphasis on security effectiveness of an endpoint solution, does this pertain to the Forrester or Gartner leadership on Threat Intelligence Services in addition to what is stated on A.2.7 Third Party Validation?	Yes.

QUERY/REQUEST	TWG RESPONSE
27. GOCC (GFI) — page 7; A.2.4 Threat Hunting Managed Threat Hunting Service should be from EDR service provider itself and not from any 3rd Party Services Solidify that TH must be part of MDR offering and augment it to the IR services.	No clarification was raised
28. GOCC (GFI) — page 7; A.2.4 Threat Hunting Service Provider should have experience with their own MDR offering for more than five (5) years Does this also pertains to this item? The MDR solution must have been in the industry for at least 5 years	Same with items in A.2.1 (Items 1 and 3) Yes.
29. GOCC (GFI) — page 7; A.2.5 Response Connection to remote host should be supported for Windows, Mac, Unix and Linux As per online bid clarification which the TWG responded and confirmed, endpoints with legacy OS (end of support) shall be considered as unsupported devices and will be excluded. Further, the TWG has agreed also on the proposal that unsupported endpoints shall only cover monitoring to which existing network based solutions (monitoring and prevention solutions) of a particular agency will be used. May we also confirm that open-source OS and other multitasking, multiuser computer operating systems to which are mostly used for specific applications shall be classified also as unsupported devices and same as legacy OS, it will be excluded?	OS covered: 1) Windows 7 and up 2) Windows Server 2012 and up 3) Linux 6.3 and up 4) Unix

QUERY/REQUEST	TWG RESPONSE
30. GOCC (GFI) – page 8; A.3 Security Information and Event Management (SIEM) The service provider 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. Validate with McAfee regarding encrypted communications between individual component (ERC, ELM and ESM) of the SIEM without any need for additional module	No clarification was raised
31. GOCC (GFI) – page 15; B.1 Vulnerability Management The solution must provide the ability to configure ports, protocols, and services for connections to scanners deployed throughout the network Ports and protocol are industrial standard and is required to be triggered a scan, may we request this item to be removed.	No.
32. GOCC (GFI) – page 16; B.1 Vulnerability Management The solution must be able to discover mobile devices and integrate with several different Mobile Device Management Systems (MDMs). Please confirm that the mobile devices referred are part of the total endpoints declared by each agency Kindly provide which of the agencies has MDM solution in place. Confirm as well that this item pertain only to the discovery of mobile devices through integration with MDM solution and not mobile scanning by the vulnerability solution	Yes. LBP has an MDM solution in place. Yes, scanning can be done through integration with the MDM solution, but the endpoints must also be scanned for vulnerabilities.

QUERY/REQUEST	TWG RESPONSE
33. GOCC (GFI) — page 16; B.1 Vulnerability Management The solution must provide patch auditing for Microsoft operating systems and applications to include Windows XP, Windows 7, Windows 8 / 8.1, Windows 10, Windows Server 2008 / 2008 R2, Windows Server 2012 / 2012 R2, Windows Server 2016, Windows Server 2019, Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange, and more. "Same with items in A.2.1 (Items 1 and 3) As per online bid clarification which the TWG responded and confirmed, endpoints with legacy OS (end of support) shall be considered as unsupported devices and will be excluded. Further, the TWG has agreed also on the proposal that unsupported endpoints shall only cover monitoring to which existing network based solutions (monitoring and prevention solutions) of a particular agency will be used. May we also confirm that open-source OS and other multitasking, multiuser computer operating systems to which are mostly used for specific applications shall be classified also as unsupported devices and same as legacy OS, it will be excluded?	OS covered: 1) Windows 7 and up 2) Windows Server 2012 and up 3) Linux 6.3 and up 4) Unix
34. GOCC (GFI) — page 17; B.1 Vulnerability Management 60. The solution must provide patch auditing for all Unix operating systems to include macOS, Linux (multiple distributions), Solaris, IBM AIX, HP-UX, and more. Same with items in A.2.1 (Items 1 and 3)	OS covered: 1) Windows 7 and up 2) Windows Server 2012 and up 3) Linux 6.3 and up 4) Unix

QUERY/REQUEST	TWG RESPONSE
As per online bid clarification which the TWG responded and confirmed, endpoints with legacy OS (end of support) shall be considered as unsupported devices and will be excluded. Further, the TWG has agreed also on the proposal that unsupported endpoints shall only cover monitoring to which existing network based solutions (monitoring and prevention solutions) of a particular agency will be used. May we also confirm that open-source OS and other multitasking, multiuser computer operating systems to which are mostly used for specific applications shall be classified also as unsupported devices and same as legacy OS, it will be excluded?	
35. Public cloud (e.g., AWS, Microsoft Azure, Salesforce) and cloud-native infrastructure (e.g., Docker, Kubernetes) The sizing consideration is based on the number of endpoints declared per agency, this line item pertains to the public cloud and cloud infra. Kindly confirm if this is part of the requirement as this is not part of the endpoint. If yes, kindly provide the number of assets .	Yes, included as part of the requirement. This shall be provided to the WINNING BIDDER.
36. The threat intelligence solution must be able to minimally provide data leakage detection capabilities such as account sale, CC sales credentials leak in open/dark web, domain leakage on code repositories and leakage on ransomware extortion sites Credit card sale not applicable to the Fund	HDMF has VISA disbursement cards.

QUERY/REQUEST	TWG RESPONSE
37. 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. As the Fund is very much cautious on data sovereignty, the collective operation of the SOC should be within the Philippines. It must have security analyst who are residing in the country.	Yes.
38. One (1) Project Manager credentials: Since the role described is a Project Manager, can we replace the requirements with this below; • 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 Professional certification	No.
39. GOCC TOR - under A.1 Security Operations Center (SOC), Item no. 6 (page 3) – Risk matrix May we know the scope of Potential Business Impact	To be discussed and agreed upon by the service provider and the agency.
40. GOCC TOR – under D. Incident Response, items no.8, 9 and 12 (page 26) The service provider shall deliver network/firewall/web applications breach response The service provider shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks.	The requirements on the indicated items stated the role of the service provider and its expected outputs.

QUERY/REQUEST	TWG RESPONSE
The service provider shall deliver insider threat investigation, as needed. What will be the role of the service provider? What are the expected outputs? Does the service provider will cover the response or provide guidelines only?	
41. Service Provider's Qualification and Requirements 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). Will you allow submission of a back-to-back certification for this requirement? Manufacturer authorizing the Distributor and the Distributor authorizing the Reseller.	Yes.
42. Service Provider's Qualification and Requirements The service provider must have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service) and support with at least 20 certified onsite support engineers within Metro Manila If the bidder is joining both lots, can they submit a total of 20 certified onsite support engineers? Or do you require total of 40 certified onsite support engineers for both lots?	20 dedicated for the GOCC/GFI Cluster
43. From GFI Cluster TOR, page 10, item 20 and item 26. Generally, SIEM vendors has the pre-built report templates for compliance like PCI DSS and HIPAA. But for the rest like FISMA, GPG13, JSOX, NERC, SOX, etc. needs to be build based on the agencies' use cases and requirements. Do all the agencies under the GOCC/Banking ToR will require all of these mentioned compliance reports? Or Can we start first on the PCI DSS and HIPAA, then later build the other compliance upon needed by each agencies?	No, not all agencies under the GOCC/GFI Sector will require all of the mentioned compliance reports, but all these reports are expected to be pre-built and readily available in the solution.

QUERY/REQUEST	TWG RESPONSE
44. From GFI Cluster TOR, page 19, mentioned about the several pre-defined playbooks which still needs to be customized based on the existing security solutions that each agency is using. Please provide each existing security devices and brands that each agencies are using that needs to be integrated with the proposed SOAR. This is for us to identify the required man-power hours needed to build the playbooks.	This shall be provided to the winning bidder.
45. GOCC Document: Section C - #4 Since there is a discussion during that bid that SOC can be hosted to an AWS or Azure that can comply with TIA 942 Rated 3 Certification, meaning are we allowed to host it internationally?	Yes. The SOC solution can be in a CSP, but the Security Operations Center with their SOC analysts should be housed in a Data Center with TIA-942 Rated 3 Facility Certification.
46. GOCC Document: Section C - #6 It is required to have a SOC 2 Type 2 Certified. Our current SOC is already SOC Type 2 but it is under renewal and legal papers will be out by April. Are we allowed to submit the old certification and resubmit once we have the latest?	This is not in the GOCC/GFI Sector TOR.
C. INSURANCE CLUSTER	
1. Under the Insurance Cluster "I. Functional Requirements B.2 - Vulnerability Assessment and Penetration Testing (VAPT)" So we can properly price your requirement out we request for the count (as we know this is a security risk) and not the actual details: a. Can you please provide the unique number/count of external IP assets and IP internal assets per group? b. For the Mobile (1) Applications can you please provide the unique number/count of Android (2) Applications and the unique number/count of iOS Applications for each?	To be discussed and agreed upon by the service provider and the agency.
2. Under the Insurance Cluster "I. Functional Requirements - B. Vulnerability Management and Penetration Testing - B.1 Vulnerability Management"	To be discussed and agreed upon by the service provider and the agency.

QUERY/REQUEST	TWG RESPONSE
So we can properly price your requirement out we request for the count (as we know this is a security risk) and not the actual details. Can you please provide the unique number/count of external assets and internal assets per group?	
3. Under the Insurance Cluster "I. Functional Requirements - B.2 Vulnerability Assessment and Penetration Testing (VAPT)" As you know the pricing for Mobile, Web, and network VAPT engagements are all different. So we can properly price your requirement out we request for the count (as we know this is a security risk) and not the actual details. a. Can you please provide the unique number/count of external IP assets and IP internal assets per group? b. For the Web - Applications can you please provide the unique number/count of FQDN? c. For the Mobile (1) Applications can you please provide the unique number/count of Android (2) Applications and the unique number/count of iOS Applications for each?	This will be provided to the winning bidder.
4. SOC/NOC facilities (IC TOR section C.2 page 15): Could the TWG reconsider this and allow the facility to be located outside Metro Manila but still be within the Philippines? (ex. Pampanga)	No
5. 45 Days of delivery for Phase 1. It might be too short of a time depending on the number of the endpoints / phyisical locations. Can this requirement only apply to servers/critical systems? Can we Request for 6mos completion after NTP if 6 months is not feasible can we ask to provide the a Priority List (Server).	No

QUERY/REQUEST	TWG RESPONSE
6. The solution is capable to deploy endpoint technology to workstations and servers, including all versions of Windows, Mac, Unix and Linux assets. Please provide specific versions (A.2.1.1) is it the same version with B.1.59 p17 of GFI?	As per TOR, this refers to Windows endpoints, Windows servers, major Unix and Linux distributions, MacOS, Mobile devices, that is still under support or extended support by the manufacturer.
7. Aside from the number of endpoints, can we get the list of devices/systems to be in scope?	To be discussed and agreed upon by the service provider and the agency.
8. For the SOC and SOC Team, is it dedicated to the GFI and IC but shared across agency? Or SOC and SOC Team are dedicated per agency?	SOC Team is dedicated per cluster.
9. Does the agencies need to access and administer the SOAR? or just monitoring (MSSP to share dashboard for monitoring)?	The agencies must have a dashboard for monitoring.
10. does the SOC needs to integrate to the existing ticketing/ITSM per agency for their internal workflow and ticketing requirements? or MSSP SOC will just use its own ticketing system?	No need to integrate. The service provider shall provide a ticketing tool.
11. For the regular meetings with the agencies, should it be per agency? or just one session per month for example for all agencies?	Per agency, per cluster, and as the need arises.
12. For the Endpoint Security/EDR requirement, what if the agency exists? Do we need to replace it or just integrate it to our SOC?	The Shared Cyber Defense project shall serve as another layer of defense for the agencies. The service provider must be able to integrate the agencies' existing endpoint security/ EDR requirement.
13. For the Endpoint Security/EDR requirement, can you provide the list of operating systems in scope?	Already stated in the TOR. Windows endpoints, Windows servers, major Unix and Linux distributions, MacOS, Mobile devices, that is still under support or extended support by the manufacturer.

QUERY/REQUEST	TWG RESPONSE
14. For the SIEM log archiving , should it be on MSSP SOC or in the premise of agency? if in the premise of the agency, who will provide the archiving storage?	Archiving is part of the scope to be provided by the service provider.
15. For the SIEM requirement, what if the agency has existing SIEM? do we replace it or just manage it?	The SIEM will be provided by the service provider. Agency SIEM can be integrated through API for event collection if needed.
16. For VM and VAPT a. What is the method of testing (whitebox, greybox, blackbox). Or we can recommend it? b. Preferred time of testing (off hours or office hours) for the intrusive type of VAPT? c. Preferred time of testing (off hours or office hours) for the non-intrusive. type of VAPT? d. How many IPs will be tested for the following: (1) External VAPT i. Number of External IPs? ii. Number of URLs? (2) Mobile App VAPT i. Number of Mobile Apps? ii. Does this apps use an API? if yes, do we need to included scanning of APIs? (3) Internal VAPT i. How many Internal IPs and Subnets? ii. Number of URLs?	To be discussed and agreed upon by the service provider and the agency.
17. For threat intelligence how many assets are we looking at (combination of names, VIP emails, credit cards, etc.)?	Already defined in the TOR.
18. For threat intelligence how many take downs?	Already defined in the TOR.
19. Can we utilize/integrate existing VPN and MFA of the agency?	Yes, if existing

QUERY/REQUEST	TWG RESPONSE
20. Under B.2 Vulnerability Assessment and Penetration Testing (VAPT) Item #1, may we ask for the inventory of 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 that will be included in the VAPT Scope?	To be discussed and agreed upon by the service provider and the agency.
21. Under D. Personnel Qualifications/Requirements, would the Analysts assigned to the Insurance Cluster requires to be dedicated? Meaning they cannot monitor other customers of the Service Provider other than the Insurance Cluster?	Yes, they are dedicated.
22. We would like to confirm that we may use our principal manufacturer/ providers personnel to implement and perform parts of the project/service as to leverage on their global insight and expertise like on the areas but not limited to services/product like Threat Intelligence, MDR and the likes which shall be beneficial for all agencies strengthening their security posture.	As long as they are identified and contracted for the project.
23. We would like to request the bid submission to be extended from March 2 2022 to March 14 2022. Given the enormous scope of the project that needs to be fully studied and prepared for, one week preparation shall unfortunately shall be an unattainable for us and other bidders and will assure of us to not be able to comply with the declared submission date.	Request for extension of bid submission will not be accommodated.
24. For Insurance Cluster, under B.2 Vulnerability Assessment and Penetration Testing (VAPT) Item #1, may we ask for the inventory of 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 that will be included in the VAPT Scope?	To be discussed and agreed upon by the service provider and the agency.
25. For Insurance Cluster, under D. Personnel Qualifications/Requirements, would the Analysts assigned to the Insurance Cluster requires to be dedicated? Meaning they cannot monitor other customers of the Service Provider other than the Insurance Cluster?	Yes, they are dedicated.
26. For Insurance Cluster, under C. Service Provider's Qualification and Requirements Item #6, can we provide other certifications as substitute for SOC 2 Type 2 such as ISO QMS and ISMS certifications OR attestation document that the Service Provider is scheduled to re-certify its ISO QMS and ISMS?	ISO QMS and ISMS may not provide assurance for the service and organizational control capability , specifically on System Security, Availability, Processing Integrity, Confidentiality, and Privacy.

QUERY/REQUEST	TWG RESPONSE
27. For Insurance Cluster, under A.3 Security Information and Event Management (SIEM), can the Service Provider will just provide the specs for the SIEM Log Collector, and the insurance agency will provide the virtualized environment where the on-premises log collector software is to be installed?	No. The service provider shall provide all components of the subscription.
28. For Insurance Cluster, does each Agency have Firewall/Router in place where the VPN will terminate from the Service Provider SOC. If Yes, can we ask for the brand per Agency?	To be discussed and agreed upon by the service provider and the agency.
29. For Insurance Cluster, under II. Non-Functional Requirement #5, does each agency will provide its own Internet Connectivity/MPLS that will be used for VPN to connect to the Service Provider SOC?	Yes, using existing network facility of the agencies.
30. For Insurance Cluster, under D. Personnel Qualifications/Requirements, item #1, that means the Service Provider should have the certified engineer based on the brand they will be using for SOAR, SIEM and Vulnerability Management?	Yes
31. For Insurance Cluster, can we request for at 2 weeks extension for the submission, given that there are several components that needs to include in the solution and processing of eligibility documents?	Request for extension of bid submission will not be accommodated.
32. For Insurance Cluster, under A.3 Security Information and Event Management (SIEM) item #1, The solution provider must be categorized as a leader in the latest Forrester or Gartner Magic Quadrant for SIEM, may we ask if can be also recognized a leader at least once in the last 5 years?	TOR requires latest Forrester or Gartner report.
33. For Insurance Cluster, may we ask for the estimated EPS (Events per Second) per Agency for us to come up with the right size of the SIEM?	You can estimate through the number of endpoints per agency.
34. For Insurance Cluster, under C. Service Provider's Qualification and Requirements Item #6, stating that Service Provider must have 3 Years providing SOC Services. Can we ask this to relax for 1 Year Experience only in providing SOC Services?	No.
35. For Insurance Cluster, under II. Non-Functional Requirements, item #2, may we ask the estimate no. of users that will access the portal per Agency? As well as the MFA they are currently using?	Users will be around 1-5, however the MFA to be provided by bidder

QUERY/REQUEST	TWG RESPONSE
36. For Insurance Cluster, under II. Functional Requirement, item # 6, does this means the SOC Facility should be two sites/redundant?	Yes. For cloud implementation, the service provider shall ensure physical and environmental controls are implemented.
37. For Insurance Cluster, under B.2. VAPT, item # 7, can we ask for actual no. and inventory of the servers, and applications?	To be discussed and agreed upon by the service provider and the agency.
38. For Insurance Cluster, under 4. Delivery Time and Schedule, does this mean Phase 1 will commence simultaneously per Agency which is 45 days upon issuance of NTP?	Yes
39. For Insurance Cluster, under 4. Delivery Time and Schedule, does 45 days after NTP for Phase 1 means that Threat Intelligence, Security Monitoring, and Incident Response should be implemented already?	Yes
40. For Insurance Cluster, If you will allow the vendor of the service provider as part of the channels agreement to implement and perform other part of the service.	Only if they are contracted by the service provider for the project.
41. For Insurance Cluster, May we request for a 2 week extension for the submission of bid.	Request for extension of bid submission will not be accommodated.
42. 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. Still request ro remove UNIX Same with Item 1 in the A.2.1 Deployment and Management. As per online bid clarification which the TWG responded and confirmed, endpoints with legacy OS (end of support) shall be considered as unsupported devices and will be excluded. Further, the TWG has agreed also on the proposal that unsupported endpoints shall only cover monitoring to which existing network-based solutions (monitoring and prevention solutions) of a particular agency will be used.	EDR can be installed to supported systems. For non-supported systems, other means of monitoring must be done, such as network detection and response (NDR)or similar.

QUERY/REQUEST	TWG RESPONSE
May we also confirm that open-source OS and other multitasking, multiuser computer operating systems to which are mostly used for specific applications shall be classified also as unsupported devices and same as legacy OS, it will be excluded?	
43. 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 provider's deployment tool, and must support both physical and virtual environments Still request ro remove UNIX Same with Item 1 in the A.2.1 Deployment and Management. As per online bid clarification which the TWG responded and confirmed, endpoints with legacy OS (end of support) shall be considered as unsupported devices and will be excluded. Further, the TWG has agreed also on the proposal that unsupported endpoints shall only cover monitoring to which existing network-based solutions (monitoring and prevention solutions) of a particular agency will be used. May we also confirm that open-source OS and other multitasking, multiuser computer operating systems to which are mostly used for specific applications shall be classified also as unsupported devices and same as legacy OS, it will be excluded?	EDR can be installed to supported systems. For non supported systems, other means of monitoring must be done, such as network detection and response (NDR) or similar.
44. Vulnerability Management and Penetration Testing Please validate that the VA PT session is once a year as explained during pre-bid conference	For IC, VAPT is annual as per TOR
45. Vulnerability Assessment and Penetration Testing (VAPT) Please validate that the VA PT session is once a year as explained during pre-bid conference	For IC, VAPT is annual as per TOR

QUERY/REQUEST	TWG RESPONSE
46. The service provider shall perform Host discovery and Operating System (OS) fingerprinting functionalities for the following, but not limited to: • Windows (all versions) • Linux and other Unix flavors (all versions) • Network and security related equipment, whether software or hardware-based • User profile settings • Advanced password analysis Same with Item 1 in the A.2.1 Deployment and Management. As per online bid clarification which the TWG responded and confirmed, endpoints with legacy OS (end of support) shall be considered as unsupported devices and will be excluded. Further, the TWG has agreed also on the proposal that unsupported endpoints shall only cover monitoring to which existing network-based solutions (monitoring and prevention solutions) of a particular agency will be used. May we also confirm that open-source OS and other multitasking, multiuser computer operating systems to which are mostly used for specific applications shall be classified also as unsupported devices and same as legacy OS, it will be excluded?	EDR can be installed to supported systems. For non supported systems, other means of monitoring must be done, such as network detection and response (NDR)or similar.
47. 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. SOC must also be SOC 2 Type II Certified, to ensure controls related to security, availability, processing integrity, confidentiality and privacy are in Since SOC 2 Type I and Type II Certifications are similar in terms of attesting of controls at a service organization which provides user entities with reasonable assurance and peace of mind that the non-financial reporting controls at a service organization are suitably designed, in place, and appropriately protecting sensitive client data, may we request that the baseline requirement should be a SOC 2 Type I Certification instead.	No. SOC 2 Type I report is an attestation of controls at a service organization at a specific point in time, whereas a SOC 2 Type II report is an attestation of controls at a service organization over a minimum six-month period. The SOC 2 Type I attests that the controls are suitably designed and implemented while the SOC 2 Type II attests that the controls are not only suitably designed and implemented, but also attests to the operating effectiveness of the controls.

QUERY/REQUEST	TWG RESPONSE
48. Personnel Qualifications/Requirements The service provider must have at least Two (2) local Certified Network and Security Engineer on each of the following security tools below: • SOAR • SIEM • Vulnerability Management Instead of total of 6 engineers, can we submit a total of 4 engineers only, since SOAR & SIEM can be covered by the same engineer?	No.
49. Last December 2021, SSS issued ITB-SSS-GOODS-2022-00 for the SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION INTO OPERATIONAL STATE OF ENDPOINT SECURITY SOLUTION WITH ENDPOINT DETECTION AND RESPONSE (EDR). Will the new System replace what SSS has recently purchased? Or can we use the new EDR that SSS just acquired.	The Shared Cyber Defense project shall serve as another layer of defense for the agencies. The service provider shall include all licenses required by the Shared Cyber Defense project. The service provider must be able to integrate the agencies' existing endpoint security/ EDR requirement.
50. Other government bids with the same technical requirements of the same nature (SIEM and EDR solution) don't have the limiting requirements as mentioned from Insurance Cluster TOR, page 4, under section A.2.1, item 2 (The solution must be categorized as a leader in the latest Forrester or Gartner Magic Quadrant for Endpoint Protection). Can this be 'loosened up'? We may suggest to the Technical Working Group to consider other SIEM and EPP/EDR vendors that is been listed from the Forrester or Gartner Magic Quadrant for the past 5 years.	Some government bids require this as well. The Forrester/Gartner requirement is in place to ensure solutions provided have been attested by these companies. The solution must be categorized as a leader in the latest Forrester or Gartner Magic Quadrant for Endpoint Protection or any similar category related to security threat detection and incident response.
51. Other government bids with the same technical requirements of the same nature (SIEM and EDR solution) don't have the limiting requirements as mentioned from Insurance Cluster TOR, page 6, under section A.3 SIEM, item 1 (The solution provided must be categorized as a leader in the latest Forrester or Gartner Magic Quadrant for SIEM). Can this be 'loosened up'? We may suggest to the Technical Working Group to consider other SIEM and EPP/EDR vendors that is been listed from the Forrester or Gartner Magic Quadrant for the past 5 years.	Some government bids require this as well. The Forrester/Gartner requirement is in place to ensure solutions provided have been attested by these companies. The solution must be categorized as a leader in the latest Forrester or Gartner Magic Quadrant for

QUERY/REQUEST	TWG RESPONSE
	Endpoint Protection or any similar category related to security threat detection and incident response.
52. From IC Cluster TOR, page 5, A.2.2 Prevention and Detection, Item #4, malware-free tradecraft using Behavior IOA patterns. Please note IOA is an exclusive feature of CROWDSTRIKE. We request to rephrase "Item # 4, malware free tradecraft using behavior patterns."	IOA or Indicator of Attack is not proprietary to Crowdstrike as security companies like McAfee, Watchguard, and Tenable among others use this.
53. It mentioned in the Insurance Cluster ToR that the training should be bundled. Are you expecting on administration training of the proposed solution? If Yes, how many attendees are expected from each agencies?	At least 2 per agency
54. For Insurance Cluster, D. Incident Response Item # 13. The service provider shall deliver employee misconduct investigations, as needed to be rephrased "The service provider shall deliver employee misconduct investigations as it relates to insider threats."	Retain the TOR wording.
55. For Insurance Cluster, D. Incident Response Item # 16. The service provider shall assist in the following: - Breach communication to "The service provider shall assist or advise in the following: - Breach communication"	Retain the TOR wording.
56. For Insurance Cluster, under B.2 Vulnerability Assessment and Penetration Testing (VAPT) Item #1, may we ask for the inventory of 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 that will be included in the VAPT Scope?	To be discussed and agreed upon by the service provider and the agency.
57. For Insurance Cluster, under D. Personnel Qualifications/Requirements, would the Analysts assigned to the Insurance Cluster requires to be dedicated? Meaning they cannot monitor other customers of the Service Provider other than the Insurance Cluster?	Yes, they are dedicated.
58. For Insurance Cluster, under C. Service Provider's Qualification and Requirements Item #6, can we provide other certifications as substitute for SOC 2 Type 2 such as ISO QMS and ISMS certifications OR attestation document that the Service Provider is scheduled to re-certify its ISO QMS and ISMS?	ISO QMS and ISMS may not provide assurance for the service and organizational control capability , specifically on System Security, Availability, Processing Integrity, Confidentiality, and Privacy.

QUERY/REQUEST	TWG RESPONSE
59. For Insurance Cluster, under A.3 Security Information and Event Management (SIEM), can the Service Provider will just provide the specs for the SIEM Log Collector and the insurance agency will provide the virtualized environment where the on-premise log collector software is to be installed?	No. The service provider shall provide all components of the subscription.
60. For Insurance Cluster, does each Agency have Firewall/Router in place where the VPN will terminate from the Service Provider SOC. If Yes, can we ask for the brand per Agency?	To be discussed and agreed upon by the service provider and the agency.
61. For Insurance Cluster, under II. Non-Functional Requirement #5, does each agency will provide its own Internet Connectivity/MPLS that will be used for VPN to connect to the Service Provider SOC?	Yes.
62. For Insurance Cluster, under D. Personnel Qualifications/Requirements, item #1, that means the Service Provider should have the certified engineer based on the brand they will be using for SOAR, SIEM and Vulnerability Management?	Yes
63. For Insurance Cluster, can we request for at 2 weeks extension for the submission, given that there are several components that needs to include in the solution and processing of eligibility documents?	Request for extension of bid submission will not be accommodated.
64. For Insurance Cluster, under A.3 Security Information and Event Management (SIEM) item #1, The solution provider must be categorized as a leader in the latest Forrester or Gartner Magic Quadrant for SIEM, May we ask if can be also recognized a leader at least once in the last 5 years?	TOR requires latest Forrester or Gartner report.
65. For Insurance Cluster, may we ask for the estimated EPS (Events per Second) per Agency for us to come up with the right size of the SIEM?	Estimate can be done using the no of endpoints per agency
66. For Insurance Cluster, under C. Service Provider's Qualification and Requirements Item #6, stating that Service Provider must have 3 Years providing SOC Services. Can we ask this to relax for 1 Year Experience only in providing SOC Services?	No
67. For Insurance Cluster, under II. Non-Functional Requirements, item #2, may we ask the estimate no. of users that will access the portal per Agency? As well as the MFA they are currently using?	Users will be around 1-5, however, MFA to be provided by bidder
68. For Insurance Cluster, under II. Functional Requirement, item # 6, does this means the SOC Facility should be two sites/redundant?	Yes. For cloud implementation, the service provider shall ensure physical and environmental controls are implemented.
69. For Insurance Cluster, under B.2. VAPT, item # 7, can we ask for actual no. and inventory of the servers, and applications?	To be discussed and agreed upon by the service provider and the agency.

QUERY/REQUEST	TWG RESPONSE
70. For Insurance Cluster, under 4. Delivery Time and Schedule, does this mean Phase 1 will commence simultaneously per Agency which is 45 days upon issuance of NTP?	Yes
71. Do we need to submit two sets of (1 for GFI Cluster and 1 for Insurance Cluster) of documents e.g., Class A, B, etc?	Only one (1) set of Eligibility and Technical Component (Items 1 to 13 of the Checklist of Bidding Documents) and Financial Component (Form Nos. 1 & 2) may be submitted. However, requirements for each lot (Items 14 to 33) shall be submitted as applicable.