QUESTIONS & ANSWERS

as of 09 July 2020

Procurement of Consultancy Services as Systems Integrator for the Supply, Delivery, Installation, and Maintenance of the Philippine Identification System (PhilSys)

Query	Queries	Answers
1	On detailed summary of cost as indicated in B.B2. Proposal hardware/infrastructure, How would you do the evaluation if the financial proposal has not yet opened?	Please refer to Bid Bulletin No. 6.
2	What is the basis for points/weight for "virtualization"?	Please refer to Clause 25.3, Bid Data Sheet, Vol. 1. It will be considered under B2. for Proposed hardware/infrastructure.
3	On Bill of Materials	Please refer to Bid Bulletin No. 6.
4	What is the definition of sub-contracting?	Subcontracting or subconsulting is entering into a contract with another firm to deliver the services under the contract. It does not refer to purchases of goods, supplies and materials that are needed to deliver the services. Also, please refer to Bid Bulletin No. 6.
5	Since there are a lot of dependencies on BioSP enrollment kit and MOSIP Platform, will they also be part of the SLA? [Please note that this is a follow up question on query regarding malfunctioning devices (for registration kits)]	No. PSA has existing and distinct SLAs covering the (i) registrations kits with the supplier, and (ii) biometric SDKs installed in the registration laptops with the BioSP.
6	On "endpoints" (i.e. on workstation, registration kits and authentication requirements), how many endpoints does PSA estimate on this project	Total number of "endpoints" shall depend on the SI's proposal. Please note that there are least 5000 registration kits, 4000 android tablets, and 250 PFRC workstations. Also, 250 PFRC workstations is only for the first batch; there is likely going to be more endpoints at the PFRCs.
7	Vol 2, Page 28, 4.5 Table 8 - Estimation of Users PPRC Desktop 1. How Many Desktops are required other then PPRC Desktops, other than users mentioned in this tables? This will be helpful for us to estimate Endpoint calculations.	Please refer to Question No. 6.
8	Vol 2, Page 30 4.6 - Technical Parameters Table 9. Technical Parameter Network Connectivity (DC-DR Replication Link). The link and / or including bandwidth connectivity shall be provided by PSA or its nominated	1. The PSA/DICT shall provide the DC-DR Replication Link including the routers that connect the data centers 2. The SI shall provide redundant switches, firewalls and routers needed for the LAN at the PDC, SDC and DRDC.

Query	Queries	Answers
	agency 2. It has been mentioned that there will be Dual links of 1 Gbps capacity. Please Clarify if the SI needs to procure respective routers and switches infrastructure required for this.	
9	Vol 2, Page 30 4.6 - Technical Parameters Table 9. Technical Parameter Network Connectivity (Primary DC, Secondary DC and DR Site link) 3. It has been mentioned that there is Dual links of 500 Mbps capacity. Please Clarify if the SI needs to procure respective routers and switches infrastructure required for this.	PSA shall provide the network connectivity for each of the central sites. The SI is responsible for providing the necessary network equipment, based on its technical proposal, which is responsive to the KPI and SLA requirements.
10	Vol 2, Page 30 4.6 - Technical Parameters Table 9. Technical Parameter Network Connectivity (Data Validation) at the Data Center It has been mentioned that Initially, 200 Mbps leased line will be used. Please Clarify: 4. If the SI needs to procure respective routers and switches infrastructure required for this. 5. More Clarification is required for the purpose of data validation mentioned for this link	PSA shall provide the network connectivity for each of the central sites. The SI is responsible for providing the necessary network equipment, based on its technical proposal, which is responsive to the KPI and SLA requirements.
11	Vol 2, Page 185, 8.3.2. a Partner Network 1) Relying Parties Connectivity 2) Trusted Service Providers – Authentication Services to DC/DR 1. What will be the Relying Party Bandwidth? 2. Relying Party Link will be MLPS Link? 3. Does SI will be responsible for Relying Party and Trusted Partner links and their Routers and Switches? 4. What will be the Link Bandwidth of Trusted Partner Link? 5. How Many Trusted Service Providers will be there?	1. The relying party will connect to the Trusted Service Provider (TSP). The TSP connects to the PhilSys. The Relying Party (RP) bandwidth shall be provisioned by the RP based on their transaction projections. 2. RPs will be connecting to the PhilSys through TSPs. RPs and TSPs will be responsible for their network connectivity. 3. The SI must deploy at least one TSP in order to process requests sent over by pilot authentication applications that will be rolled out at PSA and DSWD, but there should ultimately be more TSP "nodes" for business continuity purpose (e.g. protection against DDoS attacks). 4. TSP network connectivity is the responsibility of each TSP. 5. PSA estimates that there will be 2 TSPs that will connect with the PhilSys (with PSA as the first TSP).
12	Vol 2, Page 185, 8.3.2. b PhilSys WAN – 1) Card Production to DC/DR	6. The PSA will provide the P2PLink bandwidth for Card Production and DC/DR is initially estimated at 200 Mbps leased line.

Query	Queries	Answers
	6. What will be the P2PLink bandwidth for Card Production and DR? 7. Do we need to procure and provide the routers at Switches for this card management?	7. The SI shall provide the cabling, switches, and router for the Local Area Network for Card Personalization at the BSP.
13	Vol 2, Page 186 8.3.2. b PhilSys WAN – 2) PhilSys Fixed Registrations Centers to DC/DR 8. What will be the P2PLink bandwidth for Fixed Registration Center to DC & DR? 9. This P2P link to be provided by PSA or SI?	8. The PFRC to DC-DR bandwidth will be at least 10Mbps. 9. The P2PLink bandwidth will be provided by the PSA.
14	Vol 2, Page 186 8.3.2. b PhilSys WAN - 3) DC-DR Replication Links 10. What will be the P2PLink bandwidth replication for DC - DR? 11. This P2P link to be provided by PSA or SI? 12. Do we need to procure and provide the routers at Switches for DC and DR Replication?	10. The P2PLink bandwidth replication for DC-DR is 1Gbps. Please refer to Section 4.6, Table 9, Vol. 2: Technical Specifications. 11. The P2PLink bandwidth replication for DC-DR will be provided by PSA. 12. The SI shall provide the switches, firewall and routers needed for the local area networks within the PDC, SDC and DR sites.
15	Vol 2, Page 186, 8.3.2. b PhilSys WAN - 4) Primary DC-DR – Secondary DC Links 13. Please clarify and purpose for this link as the similar link is mentioned in point Vol 2.5 - 8.3.2b-3? 14. This P2P link to be provided by PSA or SI? 15. Do we need to procure and provide the routers at Switches for Primary DC, Secondary DC and DR Link too?	13. Secondary DC to PDC/DR link is to enable mirroring of critical applications of the PDC. 14. PSA will be providing the network connectivity between central sites. 15. The SI is responsible for the network equipment for the connectivity between the central sites.
16	Vol 2, Page 186, 8.3.2. b PhilSys WAN - 5) Contact Center – CRMS to DC/DR 16. What will be the P2PLink bandwidth for Contact Center - CRMS to DC/ DR? 17. Do we need to procure and provide the routers for this CRMS? 18. How many LAN Switches are required for CRMS? 19. What is the location of Contact Center - CRMs?	16. The SI is responsible for the network connectivity between the Contact Center and the central sites. 17. The SI is responsible for network equipment to connect the Contact Center to the central sites. 18. The SI shall propose the network solution for the CRMS which is responsive to the KPIs and SLA requirements. 19. The SI is responsible for selecting the location of the Contact Center.
17	Vol 2, Page 186, 8.3.2. b PhilSys WAN6) IT Operations i. NOC to DC/DR ii. SOC to DC/DR	20. The P2PLink Bandwidth of IT Operations Center will be at around 200 Mbps. 21. The router for IT Operations Center shall be provided by the PSA.

Query	Queries	Answers
	20. What will be the P2PLink bandwidth for IT Operations Center at DC/ DR? 21. Do we need to procure and provide the routers for this IT Operations Center? 22. How many LAN Switches are required for IT Operations (NOC and SOC)? 23. What is the location of IT Operations Center (for NOC/ SOC)? 24. IT Helpdesk is part of this, if Yes, how many LAN Switches are required for IT Helpdesk?	22. The number of LAN switches for IT Operations Center for NOC/SOC shall be included in the Technical Proposal of the SI. 23. The location of the IT Operations Center shall be provided to the winning bidder. 24. IT helpdesk is not part of the IT Operation Center. Please refer to Sec. 9.8.5, Vol. 2: Technical Specifications.
18	Vol 2, Page 205 9.6.5.1 Process/ Component-wise Recovery Strategy 25. Please clarify that will Infrastructure in terms of Network, Compute and Storage will be the same as Primary DC, Secondary DC and DR Site.	Yes, infrastructure across all sites should be the same.
19	Data Center Network Infrastructure 26. Will the SI provide all routers for all WAN connectivity between data centers? 27. Who will provide the network link and bandwidth for Network Connectivity (Data Validation) at the Data Center? 28. How many users and endpoints/desktops are needed for this PhilSys bid? 29. Are we to provide the network devices such as switches routers. for Card Registration, Contact Centers, IT SOC/NOC and LAN?	26. The SI is responsible for network equipment for each of the central sites. 27. PSA is responsible for the network connectivity between the central sites. 28. Please refer to response on previous questions regarding estimated no. of endpoints. 29. The SI shall provide the cabling, switches, firewall, and routers needed for the local area networks within the PDC, SDC DR sites, SOC, NOC, Contact Center, Card Personalization, and PFRCs.
20	Call Center 30. Are we to include a VOIP solution for the Contact Centers?	30. The SI should propose a solution which is responsive to meet the KPI and SLA requirements.
21	Cloud and Containers 31. What are the actual requirements from the Systems Integrator? 32. What are the requirements of the containers, how many nodes would they need to deliver the solution? 33. Will the solution be integrated to public clouds?	SI should design and apply appropriate technologies that are responsive to PhilSys requirements and SLAs. SIs are encouraged to outline how containerized technologies will benefit PhilSys in their technical proposal. 31. Containerization was defined to aid PSA in the rapid DevOps cycle of development, test and release of software with the aim of minimizing system outages and downtime. 32. SI shall propose the number of nodes appropriate to the scale of the PhilSys Requirements. 33. SI shall ensure that the solution is ready for public cloud deployment.

Query	Queries	Answers
	34. What container orchestration are they using?	34. SI shall propose container orchestration as part of their solutions design.
22	Cybersecurity 35. There is a requirement that states that perimeter FW and Internal FW should be of different vendor, need to know if Cisco will be perimeter or internal? 36. How our tools will be integrated to the required SOC?	The SI should propose a solution that is responsive to meet the KPI and SLA requirements.
23	Enterprise Network 37. RFP states dual router with dual links for the DC / DR. What is the network connectivity (Internet / MPLS / etc.)? What other services will be running on the edge routers? 38. Annex E states that there will be 10 pilot sites for 2020. Is the acquisition of the links between the sites and PFRC part of the scope? If yes, what are the specifications? If not, what are the type, count of links, and throughput requirement per site? 39. How will the PRFC sites connect to the applications on the DC / DR sites? 40. For the PFRC sites, will there be additional equipment to be added for this project, i.e. desktops, biometrics machines, printers, servers, etc.? Will the vendor provide LAN switches for these equipment? If yes, how many switch ports per site will be required to accommodate these equipment? 41. If LAN switches will be provided by vendor, do you require PoE? Please specify input power requirement to your devices. 42. Do you require wireless connectivity on the PFRC sites? If yes, please provide desired throughput as well as floor plans for detailed wireless design.	37. Please refer to Question No. 14 response. 38. No. Please refer to Section 5.4, Vol. 2. 39. The PSA will provide the internet link for PFRCs, but the SI shall design how the PFRCs will connect to the DC/DR sites. 40. Please refer to Section 9.3 and Section 5 for the Required Equipment for PFRC sites. 41. PoE is preferred. 42. The SI will provide networking devices at PFRCs as specified in Section 8.3.6, Vol. 2. The SI shall include in their proposal whether to use wired/wireless connectivity at PFRCs.
24	Data Center **Compute** 43. Can the SI provide sizing on the workload that they will run?	43. The SI may propose the sizing of workload that they will run as long as the SLAs are complied with. 44. The SI may include in their technical proposal the number of servers (physical and virtual) and their corresponding specifications to meet the SLAs.

Query	Queries	Answers
	44. How many servers are needed and what are their individual specification requirements? 45. Can their application run on Hyperconverged infrastructure? **Network** 46. What are their network design requirements? 47. Can they provide details on the individual switches (# of ports, throughout, etc.)? 48. What are the DC interconnect requirements? **Software Defined Storage (SDS):** 49. What is the required capacity? 50. What fie system do they require? 51. What type of storage do they require (Block, file or Object)?	45. Yes, hyperconverged infrastructure can be proposed as long as static data is stored only in the PDC, SDC and DRDC, and all SLAs are met. 46. The SI shall provide the indicative network design and propose an overall network solution for PhilSys. Also, please refer to Section 8.3, Vol. 2. 47. Same response as No. 46. 48. Please refer to Question Nos. 12 to 17 responses. 49. The SI is shall provide the indicative storage design and propose an overall storage solution for PhilSys. Also, please refer to Section 4 on Demand Capacity and Section 9.8.4, Vol. 2, for guidance on estimation of storage capacity. 50. Same response as No. 49 51. The SI may propose block, file or object interfaces.
25	SOC & NOC Manpower 52. Is the NOC/SOC be operated on a 24x7x365? If yes, the number of analysts stated in the bidding documents looks insufficient.	Yes, the NOC/SOC is expected to run 24x7x365. The estimated manpower in Section 4 is provided as reference. The SI should conduct its manpower assessment and propose its solution that is responsive to the requirements.
26	Desktops, Printers, UPS, Videowall Display 53. Please provide detailed technical specifications for the Specs of the videowall display. 54. What programs / applications will be used in the desktops?	53. Video Wall Minimum Specifications Video Wall System - can be switched to any NOC workstations at any time and display the information from an NOC workstation - Video wall pixel pitch of 1.5 or lower - must be able to input at least 12 sources to the video wall - with video wall controller 54. The desktops for PFRCs shall be used in providing other PhilSys Services such as releasing PhilID cards, authentication, inquiries, and client services.
27	Clarifications 55. Can we still submit clarifications until July 10 2020 since the bid submission has been moved to July 22 2020?	No.
28	NOC/ SOC 56. In the scenario that the SI will be the one to provide Manpower for the NOC and SOC, will it be acceptable if we provide a single manpower team that will handle NOC and SOC?	The NOC and SOC should be distinct from each other by principle of check and balance.
29	HIGH LEVEL NETWORK SIZING PHYSICAL SITES 57. Please use the table below to specify the sites which are part of the network to be	Please refer to Question No. 6 response.

Query	Queries	Answers
	protected (example data below): Site name (or Codename) 1 (HQ) #1 (HQ) Number of Endpoints (Workstations|Servers) | 300 Intersite WAN Connections #2, #3, #4 Internet Gateway/Exit Local Network Flat or Segmented? Only Data Center is Segmented Site name (or Codename) 1 (HQ) #2 Number of Endpoints (Workstations|Servers) 500 | 5 Intersite WAN Connections ---- Internet Gateway/Exit Via HQ Network Flat or Segmented? Flat Site name (or Codename) 1 (HQ) #3 Number of Endpoints (Workstations|Servers) 500 | 5 Intersite WAN Connections ---- Internet Gateway/Exit Via #2 Network Flat or Segmented? Flat	
30	LAN – Local Area Network 58. Please use the table below to specify the throughput of the organization (example data below): Site Name (or codename) #1 (HQ) Bandwidth/Maximum Throughput (bps) 0.5Gbp/s Average Utilization (bps) 250Mbp Site Name (or codename) #2 Bandwidth/Maximum Throughput (bps) 2Gbp/s Average Utilization (bps) 1.5Gbp/s Site Name (or codename) #3 Bandwidth/Maximum Throughput (bps) 100 Mbps Average Utilization (bps) 80Mbps	The SI should propose a network solution that is responsive to the requirements.
31	Internet Gateways 59. Please use the table below to specify the internet gateways / exists of the organization (example data below):	59. The SI should propose a network solution that is responsive to the requirements. Please note that the sizing estimation for internet and network connectivity are included in Section 4.6, Vol. 2. Also, please refer to Question Nos. 8 to 12 responses.

Query	Queries	Answers
	Gateway Site #1 (HQ) Bandwidth/Maximum Throughput (bps) 0.5Gbp/s Average Utilization (bps) 250Mbps Gateway Site #4 Bandwidth/Maximum Throughput (bps) 100Mbps Average Utilization (bps) 50Mbps	
32	Operating Systems 60. What type of operating systems are most commonly in use (example data below)?	The 5,000 Registration Kits laptops are pre-installed with Windows 10. The SI is responsible for proposing the OS for the central sites and PFRC devices that is responsive to the requirements.
33	Security Tools 61. For possible integration purposes, what Security tools are already/scheduled to be implemented in the network and the TPS need to integrate with (example data below)? Operating System Windows 7 Approximate Number of Endpoints 3,000 Operating System Windows 10 Approximate Number of Endpoints 500 Operating System Windows 2012 R2 Approximate Number of Endpoints 350 Operating System Linux/MAC (specific versions) Approximate Number of Endpoints Ubuntu 18.04-40, MacOS High Sierra-20..	The SI should propose the Security Tools to be implemented in the network which are responsive to the requirements. Also, please refer to Section 9.7.1, Vol. 2.
34	Bid Bulletin 5 Section 2.4 PSA is hereby revising its requirement for the IT infrastructure. PSA will require the SI to propose a solution using a hybrid cloud system architecture. All in-scope core and support applications must be on Philippine government cloud while databases, data storage, and hardware security module must be on	Government thru DICT has an agreement with an existing commercial provider, which allows other government agencies to use its services.

Query	Queries	Answers
	premise. ABIS infrastructure, which are provided by the BioSP and is out of scope for the SI tender, will also be on premise. Will this mean that we will use an existing government subscription in the concerned government cloud providers (e.g. AWS, Azure, etc.)? Or should we create a new subscription instance for this project?	
35	Page 183 Virtualization Specifications Will you require applications to run in an intelligent virtualization software that manages every device inside the data centers?	The SI shall ensure that the application deployment is managed centrally. This may include that the server components including additional memory, I/O (input/output) capacity and optional factory-integrated hypervisors to help deliver the performance and manageability they need.
36	Page 189, Firewalls and Storage Security Ensure that no client or application should have connectivity / access to the storage server or cluster other than what it is permitted to. Will you require applications to run on a dedicated cluster?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
37	Page 183, Network Specification Will you require a network connection of 10Gb and above network interfaces?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
38	Page 183, Network Specification Will you require network connection for HBA with 16/32Gb and above?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
39	Page 182, Server Specification Will you require server components to have a high-availability or a feature that can support failover switching per site?	Yes, all components should be in high-availability configuration. Please refer to the following sections in Vol. 2: Sections 9.6.3.b.5 and 9.6.4.a.5; Section 9.6.5.1 for application and data center high-availability and failover configuration; and Section 9.6.7.2 for failover strategy.
40	Page 182, Server Specification Will you require the server components to have a maximum system capacity to cater high performance and throughput or load on a server, server farm and other devices connected?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
41	Page 182, Server Specification	Yes.

Query	Queries	Answers
	Will you require the server components to include OS like Windows, Linux and other flavors? **Also Govt. Cloud will provide the OS as per Bidder's requirement? Or we need to provide the same?**	Refer to DICT website on Government Cloud specifications.
42	Page 182, Server Specification Will you require the server components to have the capability or feature for rapid OS recovery in case of corruption which allows us to boot a trusted backup OS image from a hidden boot device?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
43	Page 182, Server Specification Will you require the server components to have the feature that locks down configuration and firmware, protecting it from inadvertent or malicious changes?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
44	Page 182, Server Specification Will you require the server components to have a Unified Management Console that can monitor other server vendor brands / models?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
45	Page 182, Server Specification Will you require the server components to have the feature wherein it can be managed using an Android and/or IOS mobile application?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
46	Page 182, Server Specification Will you require the server components to have the feature for phone-home support and technical incidents?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
47	Page 182, Storage Specification Based on the requirement in section 8.4.a Storage Specification on Vol 2 □ Will you require Unified Storage solution that deal with both block data (SAN) and	The SI shall propose a solution to easily manage and operate the storage system. Enterprise platform solutions can be considered.

Query	Queries	Answers
	unstructured data (NAS) in single system as part of the required technology?	
48	Page 182, Storage Specification Based on the requirement in section 8.4.b Storage Specification on Vol 2 □ Will you require the proposed Unified storage solution support these usage □- Bare Metal hosts, hypervisors, virtual machines & containers, leading database technologies, operating systems, data stores used by PhilSys and MOSIP applications	The SI shall propose a solution for deploying different workloads, applications, databases in a unified storage system. SAN or Unified Storage Solution can be considered.
49	Page 182, Storage Specification Based on the requirement in section 8.4.1 Storage Specification on Vol 2 □ Will you require the proposed storage solution standards to be open in nature (SAN & NAS) so that it can be connected all industry leading technologies that may be in use at PhilSys	The SI shall ensure that regardless of storage technology, their proposed solution must be integrated by a unified storage system. It is preferred that both the enterprise storage and enterprise backup are integrated and implemented by one technology provider to ensure seamless compatibility.
50	Page 182, Storage Specification Based on the requirement in section 8.4.3 Storage Specification on Vol 2 □ Will you need the proposed solution to be able to deal with performance & Capacity scalability needs within the Unified (SAN, NAS) solution that is supported by MOSIP and PhilSys systems. □ Will you need automated data tiering features whereby, frequently accessed data to be automatically promoted and stored on SSD (165TB on SSD, the rest of the block data on SAS disks). Also, Will you need non-disruptive LUN migration features?	The SI, as part of its managed services for PSA, must be able to eliminate bottlenecks in a storage system. This is to ensure that performance & capacity required are automatically managed by the system, regardless of storage tiers.
51	Section 9.6.6 on Vol 2 Based on the requirement in section 9.6.6 on Vol 2 □ Will you require the RPO and RTO needs to be on the application level?	The SI should propose solutions that are responsive to the KPI and SLA requirements.

Query	Queries	Answers
52	Page 182, Storage Specification

Based on the requirement in section 9.8.4.2 on Vol 2 ☐ Will you require ☐ Useable capacity of Packet Archival @ 200TB + Pre-registration que buffer @200TB, Log files @10TB on NAS file system technology asynchronously replicating to near DC and as well as DR site too ☐ Useable capacity of authentication (50TB) , analytics/reporting (50TB), CRM(30TB), Management (20TB), Application data stores (20TB), Miscellaneous (dev, QAT) @ 100TB, virtual machines & containers @ 20TB on high performance block storage technology, enabled as active-active between DC and near DC, any asynchronously replicated to DR site too. | The SI must propose a solution to manage the capacity of data in a storage system and to ensure there is enough buffer of useable capacity. |
| 53 | section 8.3.2 on Vol 2

Based on the requirement in section 8.3.2 on Vol 2 ☐

Will you also need:

☐-highly available SAN network at each of Data centers with two fabric each towards a resilient architecture supporting the needs of the PhilSys systems? Each Fibre switch must come with 24 ports activated and must have 16Gbps SFPS for PhilSys use

-High performance, low latency, secure, redundant data replications between data centers, leveraging IP technology links for delivering RTT<5ms for DC to near DC, and another high performance required connectivity to DR DC site as well? ☐ -These inter-site replications to leverage Fibre Channel over IP extension solutions, delivering dynamically adjusting bandwidth utilizations ☐ -A comprehensive SAN network management & monitoring framework with end-to-end visibility with ability to monitor and analyze | The SI must be able to provide 100% Data Availability by having data replication and connectivity to DR and DC. The proposed solution must enable PSA to use multiple service types of Fibre Switch, FC/IP across multiple connection and manage them in a single dashboard. |

Query	Queries	Answers
	performance in real-time and historical fashion to ensure PHilSys systems are at the peak of its health and availability.	
54	Based on the requirements detailed in 8.4.2.2 Data Encryption □ Will you require the storage system to be the capability of utilizing an encryption feature internal to the platform or integrating with a 3rd-party key management platform? **How this will affect post Govt. Cloud Approach now?**	Regardless of the hosting strategy, all data in motion, in use and at rest must be encrypted.
55	Based on the requirements detailed in section 9.6.7.2 Disaster Recover Strategy and Procedures □ Will you require the storage system to have the capability to protect critical data from logical corruption? **Can we use Govt. Cloud to do backup also?**	The SI may propose backup and recovery strategy that may include government cloud as long as the backup SLAs and Backup and Restore System requirements are complied with.
56	Will you require a containerization platform that is an enterprise grade open source that includes bug fixes, security fixes, software patches and enhancements?	In addition to response in Question No. 21, the SI shall propose the appropriate containerization solution it sees fit for the requirements of PSA.
57	Will you require the containerization platform that allows self-service to deploy code on compiled and source formats?	This is necessary to allow developers to quickly and easily create applications on demand.
58	Will you require the containerization platform that must have a built-in with load balancer?	This is necessary for PSA to deploy clusters to manage PSA's virtual private network or virtual private cloud connection.
59	Will you require the containerization platform to be deployed on virtualization platform, private and public cloud?	The SI's proposed solution must be able to ensure having enough flexibilities in future deployment strategies of PSA, regardless if virtualized, private, or public cloud.
60	Will you require the containerization platform to secure all applications and or log files in a centralized location?	Yes
61	Will you require the containerization platform to have an upgrade feature without affecting other services?	The SI must be able to ensure that any modifications in containerized components shall not result in massive disruptions to the system.
62	Will you require other systems or middleware tools aside from departments like health etc. to	The PhilSys Information System Architecture adopted API-first approach for data integration.

Query	Queries	Answers
	be integrated and what interfaces will be used?	
63	For the applications that will run on PSA what are their respective deployment languages, frameworks, technologies, and data set requirements for integration?	The SI must propose the appropriate languages, frameworks, technologies, and data integrations as part of its solution presentation.
64	For MOSIP modules what are the integrations required?	Please refer to https://docs.mosip.io/platform/build-and-deploy/customisations-for-a-country, if the query is related to customizations.
65	BPM Which of the workflows defined in the specifications are to be implemented with Business Process Management? How many concurrent users will you require or should be expected?	a. Please refer to Section 6.3.6, Vol. 2, para h, Vol. 2. b. Please refer to Section 4, Vol. 2 on Demand Capacity for estimating concurrent users.
66	DevOPS and Deployment What is the development and deployment process for custom applications and integrations? (i.e. DevOps Agile Scrum etc.) Please confirm how this can be achieve using Hybrid Cloud? Govt. Cloud has any tools already which can be used for Cloud Deployment and automation?	a. The SI can adopt its preferred development and deployment process for custom applications and integrations as long as the deliverables are responsive to the PhilSys requirements. b. Please refer to DICT website on Government Cloud.
67	Case Management Will you require to handle case management?	The Fraud and Detection Management System (FDMS) requires case management functions. Please refer to Sec. 7.4.8, para. i, item 1, Vol. 2.
68	Will you require the backup and recovery solution to support a data growth plan for 3 years and above?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
69	Will you require the backup and recovery solution on data centers to have a dedicated network?	The SI must be able to design and propose the appropriate backup and recovery solution, consistent with the required SLAs.
70	Will you require backing up more than hundreds of Clients per site?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
71	Will you require the backup and recovery solution to support backup and restore of a relational database management system that requires processing of massive amounts of real time data in a short time?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
72	Will you require the backup and recovery solution to support a pure software-defined storage that has a	The SI must be able to design and implement a backup and recovery solution that can be leveraged on any storage hardware, backup software, virtualization platform and/or cloud provider. The solution must also deliver long-term retention and disaster recovery through optimized processes, such

Query	Queries	Answers
	feature of deduplication and replication?	as but not limited to replicating only the unique data, reducing replication window and lowering network bandwidth.
73	In terms of remote replication on DR will you require to replicate only the unique data to remote site? Or all data on sites?	The SI should propose solutions that are responsive to the KPI and SLA requirements.
74	Data Management and Fraud Management Will you require seamless integration of the Data Management platform to Data Governance applications such as stewardship and catalog?	Yes, this is to provide and enable PSA in automating data discovery processes.
75	Data Management and Fraud Management Will you require the data management platform to run standard ETL, big data jobs, API services all in one platform?	Yes, this is necessary to significantly reduce points for sensitive data leakages in the data processing pipeline.
76	Data Management and Fraud Management Will you require that data can be managed and processed on on-prem or hybrid deployment architecture?	SI must be able to propose the appropriate implementation design for Data Management and Fraud Management, aligned with the required SLAs
77	Data Management and Fraud Management Will you require a platform that can automate the sharing of data to external/internal groups/customers?	Please refer to Question No. 76 response.
78	Data Lake Will you require a data lake or data warehouse platform that will process and transform data with management capabilities?	SI must be able to propose the appropriate implementation design for an overall Data Management Strategy supporting an Enterprise Data Model and Master Data for PhilSys.
79	Data Lake Will you require the Data Lake or Data Warehouse platform to scale structured, unstructured, and semi-structured data?	SI must be able to propose the appropriate implementation design for an overall Data Management Strategy supporting an Enterprise Data Model and Master Data for PhilSys.
80	Data Lake Will you require the Data Lake or Data Warehouse to be on-premise, on-cloud or hybrid?	SI must be able to propose the appropriate implementation design for an overall Data Management Strategy supporting an Enterprise Data Model and Master Data for PhilSys
81	Data Lake Will you require the Data Lake or Data Warehouse solution to have a feature of data security, governance, and control policies that you can	SI must be able to propose the appropriate implementation design for an overall Data Management Strategy supporting an Enterprise Data Model and Master Data for PhilSys.

Query	Queries	Answers
	enforce anywhere in the data centers?	
82	Data Lake Will you require the Data Lake or Data Warehouse solution to capture real-time insights with support on IoT with processing and management?	SI must be able to propose the appropriate implementation design for an overall Data Management Strategy supporting an Enterprise Data Model and Master Data for PhilSys.
83	Data Lake Will you require the Data Lake or Data Warehouse solution to support high concurrency with more than 10 users?	SI must be able to propose the appropriate implementation design for an overall Data Management Strategy supporting an Enterprise Data Model and Master Data for PhilSys.
84	Firewall Tier 2 Scoping 1. What are the required security services or functionality of the appliance? **Is there any change in Firewall specs now post Hybrid Cloud approach? Please provide the revised information if Govt Cloud need to be considered for Authentication Ecosystem and Web Portal etc.** 2. Throughput required ex. threat prevention, IPS throughput? 3. How many systems/users will be protected by the firewall? 4. Any throughput and maximum sessions required? 5. Number of ports and type required (10 GE, 1 GE, Fiber, Copper)? 6. What are the WAN link throughput? 7. Number of years for subscription 8. What is the throughput needed for internal traffic? 9. "The SI using HSM will digitally encrypt the data / file to be sent to BSP Service Provider. The Digital Certificate / HSM required for data encryption will be procured by the SI and its public key shared with PSA. Please confirm if we need to provide Digital Certificate or HSM? If yes, how many numbers of HSM to be provided. 10. What is Testing Environment and Staging Environment for Registration	The SI must be able to propose a comprehensive solution for security. At the very least, the firewall component must enable PSA to do the following: (i) to perform stream-based, bi-directional traffic analysis, without proxying or buffering, (ii) to uncover intrusion attempts and malware and (iii) to identify application traffic regardless of port.

Query	Queries	Answers
85	Firewall Branches 1. What are the required security services or functionality of the appliance? 2. Throughput required ex. threat prevention, IPS, VPN throughput? 3. How many systems/users will be protected by the firewall? 4. Any throughput and maximum sessions required? 5. Number of ports and type required (10 GE, 1 GE, Fiber, Copper)? 6. What are the WAN link throughput? 7. Number of years for subscription	The SI must be able to propose a comprehensive solution for security. At the very least, the firewall component must enable PSA to do the following: (i) to perform stream-based, bi-directional traffic analysis, without proxying or buffering, (ii) to uncover intrusion attempts and malware and (iii) to identify application traffic regardless of port.
86	Antivirus/Endpoint Protection 1. What are the OS of the endpoints to be protected? Technical Questions for National ID Project v1.0 2. Should the solution have a proprietary remediation engine with insights on suspicious activities for zero-day malware removal? 3. Should the solution support the following exclusion types: File, Folder, File Extension, MD5 Hash, Registry Key, Website/IP address? 4. Should the solution be able to do rollback encrypted files with a minimum size of 80Mb (per file) and a minimum time of 72 hours to its original state after a ransomware attack happened? 5. Would you need an endpoint isolation feature? 6. Do you need a process graph of an attack for visualization? 7. Should the solution need to be able to scan inside the archives and compressed files? 8. Should the proposed Web Isolation Platform be able to preserve native end user web browsing experience? 9. Should the solution need to provide 100% malware-free Internet Isolation? 10. How many endpoints are going to be monitored/protected? Can we have a breakdown of the endpoints per site? 11. How many servers are going to be monitored/protected? Can we have a breakdown of the servers per site?	In addition to response in Question No. 84, the antivirus/endpoint protection should have multiple methodologies of endpoint isolation to restrict running and communicating process on the endpoint. This is necessary to stop users from interaction with the endpoint and to prevent malware from escalating. Furthermore, the solution should include process graph that will provide graphical visualization of suspicious activity occurring on the endpoint.

Query	Queries	Answers
	12. How many users are allowed to browse the internet? Can we have a breakdown of the internet users per site?	
87	Switches and Routers Border Router 1. What is the minimum switching and forwarding capacity of the Border Router? 2. What are the minimum routes for both IPv4 and IPv6 for the Border Router in a 1RU form factor? 3. What is the minimum number of 10/1 Gbe transceiver ports? 4. What is the minimum number of 40/100 Gbe transceiver ports? 5. What is the minimum packet buffer allowed in the Border Router? 6. Does the Border router require to have redundancy for both power supplies and fans? 7. How can the Border Router be managed and configured?	The SI should propose a security solution that is responsive to the requirements.
88	Switches and Routers Distribution Switch 1. What is the minimum number of 40/100 Gigabit interface in a 1RU form factor? 2. What is the minimum switching and forwarding capacity of the switch? 3. What is the maximum latency allotted for the switch? 4. What is the minimum packet buffer allotted for the switch? 5. How can the switch be managed and configured? 6. What are QoS Policies do the switch support?	The SI should propose a security solution that is responsive to the requirements.
89	Switches and Routers TOR Switch 1. What is the minimum number of 1/10 Gigabit Ethernet SFP-based ports in a 1RU form factor? 2. What is the minimum number of 40/100 GbE uplink ports? 3. What is the minimum switching capacity of the switch? 4. What are QoS Policies do the switch support? 5. How can the switch be managed and configured?	The SI should propose a security solution that is responsive to the requirements.
90	Switches and Routers Border Leaf 1. What is the minimum	The SI should propose a security solution that is responsive to the requirements.

Query	Queries	Answers
	switching capacity of the border leaf? 2. What is the minimum forwarding capacity of the border leaf? Technical Questions for National ID Project v1.0 3. What are the minimum routes for both IPv4 and IPv6 for the Border Router in a 1RU form factor? 4. What is the minimum interface requirement of the border leaf? 5. What is the minimum packet buffer for lossless forwarding allotted for the switch? 6. How can the switch be managed and configured?	
91	Switches and Routers Access Switch 1. What is the minimum port configuration of the switch? 2. What is the minimum switching bandwidth and forwarding rate of the switch? 3. What capability should the switch have for automated connectivity? 4. How can the switch be managed and configured?	The SI should propose a security solution that is responsive to the requirements.
92	Switches and Routers Central Network Management System (NOC) 1. What is the minimum capability of the Central Management System? 2. What is the minimum content of the Central Management System? 3. What is the minimum capability of the system with regards to policy creation? 4. What is the minimum requirement with regards to user/device auditing? 5. What can PSA utilize in the Central Management System? 6. Can the system fully integrate with the proposed network switches from campus network to data center network? 7. Can the CMS be able to monitor layer 7 application? 8. What are the minimum system support notifications the CMS should support?	The SI should propose a security solution that is responsive to the requirements.
93	Switches and Routers Wireless Router for PFRCs 1. What are the minimum specifications should the wireless router have? 2. What are the features should the wireless router	The SI should propose a solution that is responsive to the requirements.

Query	Queries	Answers
	have? 3. What type of deployments should the wireless router have? 4. What is the minimum number of SSIDs could the wireless router support? 5. What security features should wireless router have? 6. What is the minimum data rate supported by the wireless router? 7. What segment of the Gartner☐s Wired and Wireless LAN Magic Quadrant last 2019 should the wireless router brand placed?	
94	Distributed Denial of Service (DDoS) Protection 1. What is the internet bandwidth and network throughput? 2. What functionalities of DDoS are you requiring for this solution?	The solution must be a Full Proxy appliance that should not allow Fail-open or traffic bypass at all times. This is necessary to ensure the application infrastructure is protected using advanced capabilities to mitigate DoS and DDoS attacks.
95	Web Application Firewall (WAF) 1. How many web applications are going to be protected? 2. What are the web applications? Please provide a list. 3. What functionalities of WAF are you requiring for this solution?	Q1 and Q2: Please refer to Section 7.4.18.1, Vol. 2 PhilSys Web Portal and Mobile Applications for the list of applications integrated with PhilSys Web Portal. Q3: SI must refer to Table 53 of Section 9.7.1. for the functionalities of WAF, which reads: It should protect the web infrastructure of PhilSys from any kind of web attacks like defacement, injection, broken authentication etc. It can also function as a load balancer. The solution must protect credentials from theft and abuse, and secures any parameter from client-side manipulation by validating login parameters and application flow to prevent forceful browsing and logical flaws.
96	Data Governance 1. What actions do you need to be detected to protect files? 2. What other functionalities do you require for this solution? 3. What platforms are your files & folders and user data (Active Directory, LDAP, etc.) stored in and how many? ☐-Directory Services / How many users? ☐-Windows Filer Server / How many? ☐-NAS Storage, please indicate _____ ☐-Unix/Redhat (Samba) ☐-SharePoint ☐-Exchange ☐-Office 365 platforms (SharePoint Online, Exchange Online, OneDrive for Business) 4. What type of data will be stored? ☐-Database/Structured Data? E.g. SQL, etc. ☐-Unstructured Data? E.g. xls,	The SI must be able to implement the following Data Governance functional requirements: - Manage Permission Visibility - Remove excessive permissions - Full Audit log - Provide Alerts on modifications to file in sensitive file in transit - Provide Alerts on access to sensitive content - Manage and Configure alerts based on threats - Identify/assign data owners (stewardship) - Identify Stale Data - Identify and classify sensitive content - Secure sensitive data

Query	Queries	Answers
	doc, zip, txt, pdf, etc. ☐-Are there any PII (Personally Identifiable Information)? If yes, what are those? E.g. passport, driver☐s license etc.☐ ☐-Need to prove Data Privacy Compliance or other compliance? 5. Is Threat Detection required? -Provide real time alert on threat on-premise? E.g. on AD, Servers, etc.	
97	Security Will you consider following components to the Phase 3 project to ensure governance, risk management, and compliance requirements are met? ☐-Security Information and Event Management (SIEM) ☐-Security Orchestration, Automation and Response (SOAR) ☐-IAM (Identity Access Management) ☐-GRC (Governance, Risk and Compliance) ☐-F2F (Dual / 2 Factor Authentication) ☐-UBA (User Behavior Analytics)	The SI should propose a security solution that is responsive to the requirements.
98	Security Operations Center 1. Number of Assets 2. How many servers and VMs? 3. How many endpoints? 4. Total number of IP address? 5. Locations of sites to be monitored 6. Can you provide network architecture? 7. Do you require a backup offshore SOC?	The SI should propose a solution that is responsive to the requirements.
99	Security Information and Events Management (SIEM) **1.** Do we need to provide SIEM and other Security Tools for Govt. Cloud or that will be provided by PSA free of cost under Govt. Cloud Services? What are the log sources to be integrated to SIEM? 2. Please specify what are the solutions. 3. Does the solution need a built-in Threat Intel? 4. Do you require connectors developed by the vendor for the applications?	In addition to response in Question No. 84, the SI must provide an SIEM solutions that have built in Threat Intelligence with regular updates. The solution is capable of integrating with 3rd party open source and/or subscribed services for threat intel. Furthermore, the proposed solution should have ready-made connectors for most popular/common vendors applications. If the need arises, the connectors can be customized for any new application as needed.

Query	Queries	Answers
	5. How would you calculate or rate for offense prioritization?	
100	Security Orchestration Automation and Response (SOAR) 1. How many analysts are deployed in SOC? 2. Please share the list of Servers (Web, APP, DB, R&D) which will be integrated to SIEM or any other log aggregator such as AV server, AD, patch management etc. 3. How many incidents does the SOC observe daily? 4. What are the different compliances which the SOC must comply with? (Aside from DPA) 5. How many Planned SOP's are there? can you elaborate on these. 6. Do you require in-product script editor with run buttons to facilitates debug and perform tests on scripts for the incident response? 7. Do you need playbooks that automatically adapt to real-time incident conditions? 8. How many threat intelligence feed providers do you require?	The SI should propose a security solution that is responsive to PhilSys requirements. Estimated number of internal users is provided under Section 4, Vol. 2, for reference. The SI, however, should conduct its own estimation.
101	Identity and Access Management 1. How many end-users will there be? What are the classifications of end-users you are expected to consider? 2. Where will the information be coming from? Can this be the trusted source? 3. How many endpoints/systems will be integrated in IAMS? What are those? 4. Is the IAMS expected to be the central source of access request, approval & granting and rights provisioning/de-provisioning (which will be automatically reflected in the corresponding endpoints)? 5. What are the other features expected that of the proposed IAMS? Single Sign- On? Multiple Factor Authentication? 6. What form of MFA is expected? (Email verification, Security Questions, OTP). a. For OTP, does the organization have provision for SMS gateway? 7. Will the system be expected to log transactional information? 8. How long should the data	The IAM and PAM should be accessed in a single, integrated portal.

Query	Queries	Answers
	be retained? 9. For archiving, what are the information expected to be kept? 10. Are you considering an integrated Identity and Access Management solution with a Privileged Access Management solution? 11. How many users will be connected on IAM	
102	Privileged Access Management (PAM) 1. How many privileged users/ super users will there be? 2. Will you allow non-employees to have special privileged access? 3. What are the target systems or endpoints that will be considered for privileged sessions? 4. Will there be a need to do Video Recording? 5. Will there be a need to log keystrokes? 6. Will there be a need to monitor remote sessions in real time? Technical Questions for National ID Project v1.0 7. Will there be a need to have the capability of terminating remote sessions? 8. Will there be a need to use password vault or check-out feature in accessing systems for the administrators?	The SI should propose a network and security solution that is responsive to the requirements. Estimated number of internal users is provided under Section 4, Vol. 2, for reference. The SI, however, should conduct its own estimation. It is recommended that the solution should support password vault for handling the systems' credentials and a password-less function that would be given by the PAM administrator to the requestor to be able to access a specific system for a precise period of time only.
103	Document Management System 1. What kind of volume is the solution expected to handle? We understand we will only consider POA, POI and Application Form which are part of Registration Packets. Any other document which are outside core system will be handled under KMS or LMS, please confirm. 2. Number of documents that will be processed daily 3. Can you provide samples of the kind of documents to be scanned and stored?	1. DMS will only handle documents as part of the registration packet. Other documents will be managed through the KMS/LMS. Please refer to Section 4.4, Vol. 2 on Data Size for estimate on registration packet size for reference. The SI is expected to conduct its own estimation as part of its proposal. 2. Daily registration throughput is estimated at 200,000 per day at its peak. 3. Documents to be scanned and stored would be credentials from the registrant (e.g., registration forms, birth certificate, passport, UMID, etc.).
104	TPF 3. Comments and Suggestions of Consultant on the Terms of Reference Please confirm if we need to use this format for providing compliance to RFP specification and TOR? If yes please provide the Template	Please refer to Bid Bulletin No. 6.

Query	Queries	Answers
	for the same. TPF 3 is an open format, we request PSA to provide format for providing TOR Compliance Table.	
105	TPF 3 Comment and suggestions on Data, Services, and Facilities to be Provided by the Procuring Entity TPF 3 is an open format, we request PSA to provide format for providing data, service and facilities to be provided by procurement entity.	Please enumerate the data, services and facilities you would need from the procurement entity. There is no need to provide a standard format as this list varies depending on the SI's proposal.
106	TPF 5 Where applicable, indicate relationships among the Consultant and any partner and/or subconsultant, and relationship to the Procuring Entity, the Funding Source and other parties or stakeholders, if any, involved in the project. Please explain what is required to submit against this clause and how?	This section refers to requirement for disclosures of relationship, if any, between the Bidder and the PSA, as Procuring entity, the Philippine Government, as funding source, and other parties or stakeholders involved in the project.
107	TPF 6. Format of Curriculum Vitae (CV) for Proposed Professional Staff NAME OF NOTARY PUBLIC Serial No. of Commission _____ Notary Public for _____ until _____ Roll of Attorneys No. _____ PTR No. __, [date issued], [place issued] IBP No. __, [date issued], [place issued] Doc. No. ___ Page No. ___ Book No. ___ Series of ____. Please confirm if we can change this NOTARY statement as per our country rules and regulation? There will be ONLINE OFFSITE resource for them we need to notarize in respective countries. We don□t see any response on this query in your Bulletin no 4	Yes, please use notary statement prescribed by country where notarization is made. Please note, however, that per Government Procurement Policy Board Resolution No. 9-2020, submission of unnotarized documents are acceptable subject to verification during post-qualification and submission of notarized document after award of contract but before payment.
108	TPF 7. Time Schedule for Professional Personnel Months (in the Form of a Bar Chart) Please confirm if we can	Bidders may use any Project Management Tool to show bar or Gantt chart as long as the information required in TPF 7 are included.

Query	Queries	Answers
	submit MS Project Plan or any other Project Management Tool to show Bar Chart or Gantt chart? Please clarify what is the Bar Chart required? Is it required in the same template under TPF 7?	
110	Query 2: IT Infra Architecture What is the "Philippines Govt. Cloud"?	Please refer to the link http://i.gov.ph/govcloud/ for an overview of the Government Cloud.
111	Query 2: IT Infra Architecture Please confirm if Govt. Cloud is Private or Public Cloud? or combination of Both.	The government cloud mentioned is a commissioned commercial cloud service provider.
112	Query 2: IT Infra Architecture Please confirm if Govt. Cloud is only Infra as a Service? if yes, what are the infra services that will be provided to bidders.	The government cloud mentioned is Infrastructure as a Service.
113	Query 2: IT Infra Architecture In the situation if Govt. Cloud are CSP providers like AWS, Azure, Google what are the "private/public cloud tenancy" being provided by these CSPs.	This will be discussed with the winning SI bidder.
114	Query 2: IT Infra Architecture All in-scope core and support applications must be on Philippine government cloud **MOSIP Application** Is MOSIP providing their core component on Cloud or it is the responsibility of SI to host MOSIP application stack on Govt. Cloud ? Please provide details on how MOSIP Compute and desired Dockers will be distributed over Govt. Cloud?	MOSIP can run both on cloud and on premise. The SI is responsible to deploy the MOSIP application stack onto the PH Gov cloud.
115	Query 2: IT Infra Architecture □ All in-scope core and support applications must be on Philippine government cloud **Privacy and Data Protection Guideline & technical Specification on Govt. Cloud** Core System, CPMS Application, Web Portal, Pre-Registration Portal, FDMS, Authentication Packets In Memory, Registration Packets In memory	Please refer to the National Privacy Commission Circular 16-01 https://www.privacy.gov.ph/memorandum-circulars/npc-circular-16-01-security-of-personal-data-in-government-agencies/

Query	Queries	Answers
	These applications contains information related to the Resident and Citizen☐s Privacy. Kindly advise what is the provision to secure this information on Govt. Cloud ? We also request PSA to please provide data security and data protection compliance guideline and procedures while on Public or Private Cloud. As per response from PSA it seems these application data, in memory biometric information will have to be on Govt. Cloud, which raise serious concern and requirement of adherence to the privacy and data protection policy.	
116	Query 2: IT Infra Architecture ☐ **PDC, SDC and DR and Backup Sites** Kindly explain if we there will no need for SDC and DR for all Application Deployment IT Infra ? SI will only be responsible for Data Storage and Database Replication when it comes to RTO and RPO requirement. With this change now, Govt. Cloud provider has to comply on the RTO and RPO as per project requirement & specification.	This will be discussed with the winning bidder.
117	Query 2: IT Infra Architecture ☐ **Data Retention Policy** Kindly clarify on the data retention policy and guideline on Govt. Cloud. This arrangement should be directly between Govt. of Philippines and CSP provider if applicable based on the response of our query number 2 & 3.	The data retention policy of the Philippines is governed by NAP General Circular No. 1 (http://nationalarchives.gov.ph/wp-content/uploads/2015/04/NAP-Gen.-Circular-1-2-and-GRDS-2009.pdf).
118	Query 2: IT Infra Architecture ☐ **Accredited CSP** Please provide Accredited Cloud Services Providers by the Govt. of Philippines? If applicable based on the response of our query number 2 & 3.	There are no accredited cloud service providers by the Philippine Government.

Query	Queries	Answers
119	Query 2: IT Infra Architecture □ **Data Classification – Categories for Core and Non- Core Applications** With reference to putting core and support applications on Philippine government cloud in Bid Bulletin No. 5, may we request PSA to provide the classification of the personal data collected under PhilSys. Are these data classified as Sensitive Government Data, Above-Sensitive Government Data, or do they fall under another classification?	Please refer to the National Privacy Commission Circular 16-01 https://www.privacy.gov.ph/memorandum-circulars/npc-circular-16-01-security-of-personal-data-in-government-agencies/"
120	Query 2: IT Infra Architecture □ **SLA, Throughput & Performance Requirements** We believe there is a need to look and revise overall SLA, Throughput and Performance Matrix for this overall program. There will be huge dependencies to meet and comply currently mentioned specs in the RFP, which will now differ, and need amendments based on Govt. Cloud and Hybrid Cloud Deployment Approach.	SLA targets for the PhilSys will remain, however, penalties will be imposed on the SI only if the SLA breach is caused by any application, services and/or infrastructure that the SI are responsible and accountable for.
121	Query 2: IT Infra Architecture □ **Govt. Cloud Hosting Services & Costing** It is assumed that now with this change overall cost for Govt. Cloud Hosting & Services will also be under PSA□s responsibility including connectivity cost between Govt. Cloud and PSA Datacenters and BSP Data Center.	Yes.
122	Against your Response : Query 74 as published on 25 June, 2020. Please refer to https://docs.mosip.io/platform/build- and-deploy/hardware-sizing for the hardware compute and storage requirements for MOSIP core platform The SI should propose an overall deployment diagram which is responsive to meet the KPI and SLA requirements. Please confirm if MOSIP HW sizing will be on Govt. Cloud	Hardware sizing is provided for commodity hardware with certain specification. If the hardware on cloud/on-premise has different specs, the sizing may be worked out accordingly by SI in consultation with MOSIP team.

Query	Queries	Answers
	or we need to cater this under PSA premise, this is important national id data and should be in compliance of the national data protection guidelines.	
123	Hybrid Cloud a) Please confirm the location of the NOC for Govt. Cloud? b) Please confirm the ABIS ☐ BIOSP ☐ Engine if that is also shifted on Govt. Cloud? c) As per project requirement we will have to design the network topology between PSA, Govt. Cloud, BSP, ABIS, SDC, DR, 250 PFRC and Backup Site please provide details and connectivity architecture between all these NOC.	The SI is responsible for the selection of the location for the NOC. PSA will require the SI to propose a solution using a hybrid cloud system architecture. All in-scope core and support applications must be on Philippine government cloud while databases, data storage, and hardware security module must be on premise. ABIS infrastructure, which are provided by the BioSP and is out of scope for the SI tender, will also be on premise. PSA / DICT to provide details re: network connectivity between the sites (central sites, PFRCs, NOC/SOC, PH Gov cloud, etc.)
124	Staging Server, Development Environment, Testing Environment, Training and Benchmarking Environment Please confirm if we can provide this on Govt. Cloud? Can we use Automation Tool from your Govt. Cloud CSP to manage Benchmarking and Testing?	The SI should propose a solution that is responsive to the requirements.
125	Page 182, Server Specification At the time of bid submission, SI shall propose the latest (within the last 1 year) server model with proof from OEM. We have checked with all reputed OEMs for Server Make / Series, it is not launched every year. This has to be changed to (within 2 years criteria) to comply.	The requirement is for the SI to propose the latest model/series within the last 1 year. If there has been no updated model /series within the last year then the prevailing latest model should be acceptable.
126	Query Response ☐ 127 The SI must propose Software Defined Storage (SDS) or any other compatible storage system along with enterprise support for the duration of the contract, which is responsive to meet the KPI and SLA requirements. 1. Can we use an appliance-based OEM to provide the Software Defined Storage requirements of the infrastructure? 2.) If the infrastructure will be hosted on the Government Cloud / Certified Cloud Provider, in this situation PSA☐s CSP to guarantee the	The SI should propose a storage solution that is responsive to the requirements.

Query	Queries	Answers
	availability of the storage requirement of the applications.	
127	Backup Software

Section 7.5.6. Given that the SI is required to put core and support applications on Philippine government cloud, and given the various types of databases and storage required by the core and support applications in the PhilSys project -- software defined storage, distributed file system, data lake, etc.

Will the bidder be allowed to propose a combination of more than one backup software and/or Backup-as-a-Service in order to provide comprehensive, MOSIP centric data protection for all PhilSys systems? | The SI should propose a backup and recovery solution that is responsive to the requirements. |
| 128 | Registration Processor and Authentication□

Do we need to have replica in SDC and DR?

Can we use PSA Govt. Cloud for application as SDC and DR will not be required now due to Hybrid Cloud Deployment.
As per MOSIP document and registration processor we need to provide 180 Servers in total.

Can we put this on Govt. Cloud? | The SI should propose a backup and recovery solution that is responsive to the requirements. |
| 129 | BIAS

Will you require automation of deduplication processes using built-in machine learning algorithms? | Machine Learning/AI/Neural Networks is not and should not be a mandatory requirement for biometric deduplication (traditional, NIST-certified algorithms perform well enough). We see no need for ML/AI/NN technology for "deduplication automation" either. SI MUST develop the central workflow supporting registration and let the ABIS carry out the full biometric deduplication. |
| 130 | BIAS - FDMS

Will you require built-in components that can leverage machine learning to aid in fraud detection? | The SI should propose a DM and FM solution that is responsive to the requirements. |
| 131 | Should the solution require User Behavior Analytics as a best practice? To be able to have the visibility or monitoring on the ff; DHCP traffic monitoring, DNS traffic monitoring, Email traffic monitoring, MS SQL monitoring, SMB/CIF traffic monitoring, VOP traffic monitoring, and HTTP traffic monitoring? | The SI must propose and implement a solution for layer 7 monitoring in support of troubleshooting and SLA management. |

Query	Queries	Answers
132	Do you require the User Behavior Analytics to identify which users are doing an attack in the network? Should the system be capable of detecting the following anomalies: port scanning, dictionary attack, Denial of Service attacks, attack on network protocols SSH, RDP, Telnet, and other services?	The SI must propose and implement a solution capable of network behavior analysis.
133	Is it necessary to identify the application's access by users in application performance monitoring? Like the communication between application servers and database servers, Oracle, MSSQL, Postgre SQL, MySQL, MariaDB.	The SI must propose and implement a solution for application and database monitoring.
134	Should the solution need to be capable of doing a network delay analysis or reporting of a round-trip time, server response time, delay, jitter, retransmission, and out-of-order packets?	The SI must be able to propose a comprehensive solution for network monitoring. These components must be used as the basis for monitoring network SLAs.
135	To avoid additional load on the server, does the tool be non-intrusive or agentless application monitoring? Does the tool needs to agentless?	The SI must be able to propose a comprehensive solution for network monitoring. These components must be used as the basis for monitoring network SLAs.
136	Do you require to have network visibility on the remote branches?	The SI must be able to propose a comprehensive solution for network monitoring. These components must be used as the basis for monitoring network SLAs.
137	Does the tool need to support Internet service provider bandwidth monitoring to identify its performance and alert if the ISP provider is not efficient?	The SI must be able to propose a comprehensive solution for network monitoring. These components must be used as the basis for monitoring network SLAs.
138	How long is your data retention requirement?	The data retention policy of the Philippines is governed by NAP General Circular No. 1 (http://nationalarchives.gov.ph/wp-content/uploads/2015/04/NAP-Gen.-Circular-1-2-and-GRDS-2009.pdf). PSA shall share the retention period for PhilSys data to the winning bidder.
139	Should the tool support a graphical user interface or chart to display the performance of the network?	The SI must be able to propose a comprehensive solution for network monitoring. These components must be used as the basis for monitoring network SLAs.
140	Does the network monitoring have the capability to alert or set an SLA in case network devices or servers experience some issues?	The SI should propose a network solution that is responsive to the requirements.
141	Machine Learning & Artificial Intelligence 1. How many devices expected to be monitored? 2. What are the ports on the core switch? (copper or fiber) 3. Can we use any Govt. Cloud Service or any	In addition to response in Question No. 134, the solution must be able to support both copper and fiber-based components. The solution must have unsupervised capability of detecting network patterns autonomously.

Query	Queries	Answers
	application as available with your CSP?	
142	3.3 Page 34 Furthermore, the Funding Source and the Procuring Entity reserve the right to inspect and audit records and accounts of a Consultant in the bidding for and performance of a contract themselves or through independent auditors as reflected in the GCC Clause 51. Please confirm funding source for this project. What is this process and its applicability?	Please refer to Clause 1.2, Bid Data Sheet, Vol 1. Funding Source is the Gov of the Philippines.
143	Document Screener 1. Please confirm if PSA operator will do screening manually or electronically? 2. What are the documents which need to be screened and verify by PSA officer before sending person to the registration counter?	1. Document screening is done manually. 2. Any two (2) valid IDs (Document-based Registration) or thru Introducer-based Registration More details on this will be shared with the winning bidder.
144	Project Kick Start: Deliverable after 30 Days post Contract Signing Approved project initiation document including risk analysis, project organization, and deployment and delivery plan, training plan and project control. Please also include SRS and FRS under this phase. Phase wise – version wise SRS and FRS will have to be approved PSA before any development and customization to kick-start.	Current deliverables include approved functional and technical specifications (Vol 1) which is what the FRS and SRS will address. This must include FRS and SRS. Functional and Tech Specs are approved at each Phase, as there may be revisions for these resulting from the ongoing development. Please refer to Question No. 171 (25 June 2020) response relating to new functionalities and change request.
145	Query 68 response published on 25th June 2020. The SI shall discuss with all the stakeholders and confirm the actual storage capacity and type of storage (block, file, object) and create a detailed design for each of the clusters as follows: Log Cluster =120 TB + 2 Replica Copy = 240 TB = 360 TB; but as per the clause it says 120 + 264 TB? The SI is responsible for making a final assessment of the storage requirement as part of "Requirements Gathering.	Please refer to Section 8.C of the IRR of RA11055 https://psa.gov.ph/system/files/kmcd/IRR%20of%20the%20RA%2011055%20or%20PhilSys%20Law.pdf regarding the documentary requirements to be presented during registration. At most three documents will be scanned in the process. A gray scale copy of the POA/POI is required.

Query	Queries	Answers
	This is fixed price bid and there is a provision of change management for any new scope and cost escalation. Should be assume that if our sizing assumptions are not as per PSA business flow that will be treated as additional cost to System Integrator. We would like to request PSA to confirm for example mandatory and options documents captured during registration process. Also please confirm if there will be a need of Color or Gray Scale Copy for POA AND POI documents?	
146	Change Management Process What is Change Management Process for the RFP, please provide details for the same.	There is no Change Management Process relating to the RFP. The requirements under the Bidding Documents, including the supplemental bid bulletins, are final.
147	Benchmarking for Registration and Authentication 10 to 25 Million for Benchmarking Please confirm if we can use PDC & SDC infrastructure for benchmarking or we need to supply separate hardware. Please note that the MOSIP component itself need multiple VCPU in total.	Please refer to page 41 of Vol 2. Setup of benchmark environment should be in DR site.
148	ABIS System Benchmarking Please confirm how Benchmarking SLA and throughput to be measured as we are now using Govt. Cloud. Please confirm ABIS system is on Govt. Cloud too?	ABIS infrastructure, which is provided by the BioSP and is out of scope for the SI tender, will be on premise. ABIS benchmarking requirement will remain as-is.
149	Please confirm PhilSys users who will access all the systems for all applications. How many users are considered for IAM including Registration kits operators. Do we need to consider Operators + Supervisors + PSA officers at PFRC + Manual Verification + SOC + NOC + Call Center + IT HelpDesk + Other Govt officials. Do we need to consider devices	Please refer to Section 4, Vol. 2 for reference data relating to the project. The SI should conduct its own estimation and provide a solution that is responsive to the requirements.

Query	Queries	Answers
150	Please confirm if SI need to consider for providing Space, Meals, Projector, Mic, or LCD during the Training to Master. Can we use Conference Room at PSA?	The SI is responsible for the logistics relating to training. PSA conference room can be used, subject to availability.
151	Please confirm the specification of the Mobile Phone and Tablet which PSA will use at PFRC for card issuance using QR code – offline transaction. We would like to know if those are Android or IOS Devices? How many persons from PSA will be involved in the Offline Dispatch Process across 250 PFRC?	The OS is Android. At least one PSA staff will be involved in this process per PFRC
152	SSL AND DIGITAL CERTIFICATES Please confirm if we can provide solution on Firefox as preferred browser as it works well with Java, which is needed to run the digital certificates. Google Chrome, on the other hand, usually can't recognize Java.	The SI should provide a solution that is responsive to the requirements.
153	No of Digital Certificates Please confirm the number of Digital Certificates required for this project.	Please refer to Section 4, Vol. 2 for reference data relating to the project. The SI should conduct its own estimation and provide a solution that is responsive to the requirements.
154	No of SSL Certificates Please confirm the number of SSL Certificates required for this project. Can we use Govt. Cloud CSP SSL Certificates? Or any other out of box solution?	Please refer to Section 4, Vol. 2 for reference data relating to the project. The SI should conduct its own estimation and provide a solution that is responsive to the requirements.
155	Bid Bulletin 5 - replies as of 25th June 2020 Clarification number 2, Page 1 PSA is hereby revising its requirement for the IT Infrastructure. PSA will require the SI to propose a solution using a hybrid cloud system architecture. All in-scope core and support applications must be on Philippine government cloud while databases, data storage, and hardware security module must be on premise. ABIS infrastructure, which are provided by the BioSP and is out of scope for the SI tender, will also be on premise. 1. Need more information on Govt. Cloud. Is the cloud setup	1. The government cloud mentioned is a commissioned commercial cloud service provider. 2. MOSIP scalability is not exclusively based on kubernetes. SI may opt to provide their own scalability solution. 3. SLA targets for the PhilSys will remain, however, penalties will be imposed on the SI only if the SLA breach is caused by any application, services and/or infrastructure that the SI are responsible and accountable for. 4. Please refer to Question no. 121 response. 5. Connectivity will be out of scope for SI.

Query	Queries	Answers
	in association with existing service providers like AWS, Azure, Google etc.? Or is it a cloud with Philippines specific setup? What are the provisions of cloud? How do we source resources from them? Do they publish rate card? Does SI need to procure the resources on cloud or these will be paid by PSA? 2. MOSIP scalability is based on Kubernetes. Will Gov't. Cloud provide for these features or SI has to provision for it separately? 3. Connectivity between DC, Secondary DC and DR with cloud. Since data is expected to be in PSA DC and compute on cloud, quality of connectivity between these sites is extremely important. Will the latency of this connectivity be equivalent to latency on high speed LAN? If no, what will it be? Please note this will have direct impact on performance of the system and thus SLA. 4. There is provision of Primary DC, Secondary DC, DR and Cloud. Request PSA to clarify their expectation on solution with regards to earlier provisions of the TOR. E.g. Authentication was expected to be active - active - between primary and secondary. Are these still valid? If so, does PSA expect SI to renting some infrastructure from cloud and buy some infrastructure for on premise? If not, then will cloud have near site for active - active working? Or it is expected that cloud will provide necessary redundancies and thus provision of active - active setup no longer exist? Overall clarification from PSA will be highly appreciated and will enable SI to optimize. 5. Will PSA provision for connectivity between cloud and primary / secondary as well as DR? Is there any requirement for SI to purchase any compute for secondary or DR other than those required to data store?	
156	Bid Bulletin 5 - replies as of 25th June 2020 Clarification number 2, Page 1	External connectivity is out scope for the SI. The SI should propose a solution which is responsive to meet the KPI and SLA requirements.

Query	Queries	Answers
	PSA is hereby revising its requirement for the IT Infrastructure. PSA will require the SI to propose a solution using a hybrid cloud system architecture. All in-scope core and support applications must be on Philippine government cloud while databases, data storage, and hardware security module must be on premise. ABIS infrastructure, which are provided by the BioSP and is out of scope for the SI tender, will also be on premise.6. Specific Queries with regards to network and security infrastructure provision in cloud: a. Internet Router i. Will this be dedicated router or this will be software defined router? ii. If this is Software defined Router then who will manage this? iii. Routing and Switching configuration, uptime etc., will be managed by SI or Cloud Service Provider? b. MPLS Link i. Does PSA Government Cloud will provide the MPLS Connectivity Links? ii. Please provide the details of the connectivity of MPLS Connectivity to PSA government cloud Service. Who will manage and uptime of these MPLS Links? c. MPLS Router i. Will this be dedicated router or this will be software defined router? ii. If this is Software defined Router then who will manage this? iii. Routing and Switching configuration, uptime etc., will be managed by SI or Cloud Service Provider? d. PhilSys Aggregation Router i. Will this be dedicated router or this will be software defined router? ii. If this is Software defined Router then who will manage this? iii. Routing and Switching configuration, uptime etc., will be managed by SI or Cloud Service Provider? iv. Does PSA Government Cloud will provide the MPLS Connectivity Links?	SLA targets for the PhilSys will remain, however, penalties will be imposed on the SI only if the SLA breach is caused by any application, services and/or infrastructure that the SI are responsible and accountable for.

Query	Queries	Answers
	e. PhilSys WAN P2P Link i. Does PSA Government Cloud will provide the P2Plink Connectivity? ii. Please provide the details of the connectivity of P2Plink Connectivity to PSA government cloud Service. iii. Who will manage and uptime of these P2Plink Links? f. Perimeter Firewall i. Will this be dedicated perimeter firewall or this will be software defined? ii. If this is Software defined firewall then who will manage this? iii. Perimeter Firewall configuration, uptime etc., will be managed by SI or Cloud Service Provider? iv. The Management Server of the Perimeter firewall will be at PSA Based Government Cloud based Service or this will be in in premise? g. SSL/ LB/ WAF i. Will this be dedicated SSL/ WAF/ Load Balancer or this will be software defined? ii. If this is Software defined SSL/ WAF/ Load Balancer then who will manage this? iii. SSL/ WAF/ Load Balancer configuration, uptime etc., will be managed by SI or Cloud Service Provider? iv. The Management Server of the SSL/ WAF/Load Balancer will be at PSA Cloud based Service or this will be in in premise? v. Please Clarify if SSL certificate will be on PSA based Government Cloud service? h. NIPS i. Will this be dedicated NIPS appliance or this will be software defined? ii. If this is Software defined NIPS then who will manage this? iii. NIPS configuration, uptime, updates and upgrades etc., will be managed by SI or Cloud Service Provider? iv. The Management Server of the NIPS will be at PSA based government Cloud Service or this will be in in premise? i. SIEM, SOAR & Security Feed i. Considering criticality hence please clarify that do we need to host the SIEM, SOAR and	

Query	Queries	Answers
	Security Feed in In premise or Cloud Based Model? ii. Can we deploy Security as Service model for SIEM, SOAR and Security Feed for OEM based Cloud Service?	
157	Volume 2 Section 4.6, Page 29 Table 9: Technical Parameters 7. It is our understanding that there would be a dedicate 1 Gbps for point to point replication link Primary DC and DR DC but no information is mentioned for replication between Primary and Secondary DC, Please Clarify	External connectivity is out scope for the SI. SLA targets for the PhilSys will remain, however, penalties will be imposed on the SI only if the SLA breach is caused by any application, services and/or infrastructure that the SI are responsible and accountable for.
158	Volume 2 Section 4.5, Pages 27 & 28 Table 8: estimation of users 8. It is our understanding that SI is required to secure following end points: □ 5000 machine in PFRC □ 250 desktops that would be supplied by SI □ IT operations in PhilSys WAN – NOC,SOC, call center, IT help desk, Dashboard users, Internal PSA users as defined in volume 2. Kindly confirm.	Confirmed.
159	Volume 2 Section 4.5, Pages 27 & 28 Table 8: estimation of users 9. It is our understanding that SI has to procure desktops for the following: □ One desktop each for 250 PFRC □ Internal operations will NOC,SOC, Call center, IT helpdesk etc. For the 5000 registration kits, SI is not obligated to provided desktop machines. Kindly confirm.	Confirmed.
160	Volume 2.1 5.2 Hardware and consumables , Page 37 Table 13 - Overview of the scope of work (hardware) #2 Setting Up of Fixed Registration Centers The SI shall perform the following activities: Provide 250 sets of Wi-Fi ready desktop computer with UPS, authentication devices (Iris, Fingerprint and Facial), Printer and peripherals for the handling of non-registration transactions. Desktop systems	The winning SI may propose a different brand for the authentication devices as long as it complies with the MOSIP Device Specification requirement.

Query	Queries	Answers
	must be delivered complete with the necessary office productivity tools and remote desktop capabilities. Annex C 10. For the Authentication Devices, do we have to provide the exact make and model or we can propose a different brand?	
161	Vol.01, Pg. 64, clause 31.4. f. Confidentiality Agreement/NDA is required to be signed IT is requested to please share the template for NDA / Confidentiality agreement to be signed with successful bidder.	NDA/Confidentiality agreement will be discussed during contract negotiations.
162	001 Vol1 SI BID DOCS_0.pdf (Section 10.2 (c)(vi) of the ITB) Pg. 39 Section 10.2 (c)(vi) of the ITB states: "...In addition, the expert should submit a signed written commitment stating that the expert shall work for the Project once awarded the contract." There is already a "Commitment" statement like this in the CV. Is a separate document/statement still necessary?	No.
163	Technical Proposal 001 Vol1 SI BID DOCS_0.pdf and June 15, 2020 Q&A In the Q&A as of June 15, 2020, the PSA BAC clarified in Q&A No. 29 that as regards the Bid Securing Declarations (BSD): "If bidders submitted an intent to form a joint venture agreement, then it should be in the name of the joint venture members." We would like further clarification on this because in our situation, the consortium members are in different countries - one in the Philippines, and another in India. a. Should two separate BSDs be prepared, one for each consortium member? b. If two separate BSDs will be prepared, who would be considered by the PSA as the	Joint venture members have the option of submitting BSDs either in one or more than one separate documents. Hence: a) Joint venture may execute two separate BSDs, one for each consortium member; b) If two separate BSDs are executed, signatory should be the one authorized by the joint venture member executing the BSD; (c) Joint venture may also submit only one BSD for all joint venture members; (d) If only one BSD is submitted for all joint venture members, signatories may be as follows: (i) signatories authorized by each joint venture member, or (ii) one signatory authorized by the consortium.

Query	Queries	Answers
	authorized signatory to these documents? c. In contrast, should only one BSD be prepared for both members together? d. If only 1 BSD, who should be the authorized signatory to this - (A) should there be two signatories, one for the Indian company and one for the Philippine company, together in the same document, or (B) only the representative of the consortium	
164	Financial Proposal 001 Vol1 SI BID DOCS_0.pdf Page 125 Regarding Financial Proposal Forms (FPF) 3 onwards Should the "Activity No." fields correspond to the Activities to be listed in Technical Proposal Form (TPF) 8?	Yes.
165	Technical and Financial Proposals 001 Vol1 SI BID DOCS_0.pdf Page 116, 120 Some of the forms, including the Bid Securing Declaration and Summary of Costs require us to indicate the "Invitation to Bid Reference No." Do we assume that this is the same as the Request for Expression of Interest Reference No. 6997462 on PhilGEPS and PSA's procurement website?	Invitation to Bid Reference No is Public Bidding No. PRO-005.
166	Financial Proposal001 Vol1 SI BID DOCS_0.pdf FPF 4. Breakdown of Remuneration per Activity Please interpret allowing terms Regular staff, Local staff and Consultants	Question vague.
167	Technical Proposal 001 Vol1 SI BID DOCS_0.pdf TPF 8. Activity (Work) Schedule Please elaborate on how this is different from a workplan and how should the consultant respond to the activity table.	This is the same as a workplan. Please note response in Question No. 108.
168	002 Vol2 SI BID DOCS_1 page 25 Department of Information and Communications Technology (DICT) Provides technical assistance to the PhilSys and shared government ICT	The SI should provide anti-DDOS solution on top of what is provided by the Government.

Query	Queries	Answers
	including data center space and hosting, and WAN connections We understand provisioning the WAN connectivity (both Intranet and Internet) at any location is not under the scope of the SI. Please confirm. RFP also has a requirement of Anti DDOS solution from the ISP. Please suggest which ISP should we contact for the DDOS solution as ISP is selected by the PSA. Whom (in DICT or ISP) should we contact for the DDoS solution.	
169	IT Infrastructure 002 Vol2 SI BID DOCS_1 Page 29 1. Network Connectivity (DC-DR Replication Link): Dual links of 1 Gbps capacity provided by PSA 2, Network Connectivity (Internet) at the Data Center: Initially 200 Mbps internet connectivity 3. Network Connectivity (Data Validation) at the Data Center: Initially, 200 Mbps leased line We understand it is estimated bandwidth is provided by PSA. The bidder can propose as per their solution requirement if required additional bandwidth can be provided by PSA.	PSA should be able to provide the required bandwidth as soon as it has independently confirmed that the bandwidth is insufficient.
170	IT Infrastructure 002 Vol2 SI BID DOCS_1 Page 29 Network Connectivity (TSPs) at the Data Center: To be provisioned by respective TSP and other external entities, based on their transaction projections. 1. Please confirm whether TSP connectivity need to be provisioned at PDC & DR only as per the network architecture in section 8.3.4. or at all three DCs. 2. Kindly provide the no. of port and port capacity need to be provisioned at respective data centers	1. TSP connectivity is to be provisioned at PDC only. 2. The SI shall include in their proposal the number of ports and port capacity needed to be provisioned at respective Data Centers. Please refer to Network Connectivity Diagram in Bid Bulletin No. 6.
171	002 Vol2 SI BID DOCS_1 Page 31 Re. Online authentication: Fingerprint, iris or facial image biometric authentication Demographic authentication One Time Password (OTP) by SMS: Electronic Know Your Customer (eKYC)	External connectivity is out scope for the SI. However, the SI should provide end-to-end data encryption regardless of connectivity Please refer to Network Connectivity Diagram in Bid Bulletin No. 6.

Query	Queries	Answers
	Is SI responsible to procure and implement the secured connections to PhilSYS (inward requests & outbound replies)? It is recommended that SI is responsible for network and bandwidth connectivity to Fixed Registration Center to "wholly" investigate & resolve secured data transmission for authentication purposes	
172	002 Vol2 SI BID DOCS_1 Re. Online authentication: Fingerprint, iris or facial image biometric authentication Demographic authentication One Time Password (OTP) by SMS: Electronic Know Your Customer (eKYC) Is SI responsible to procure and implement the secured connections to PhilSYS (inward requests & outbound replies)?	External connectivity is out scope for the SI. However, the SI should provide end-to-end data encryption regardless of connectivity Please refer to Network Connectivity Diagram in Bid Bulletin No. 6.
173	002 Vol2 SI BID DOCS_1 page 37 Table 14 Overview of scope of work (other services) Point # 2 says "The SI shall perform the following activities: Set-up of network connectivity at Fixed Registration Centers" On the other hand Table 6 point # 9 on page 42 provides: Bandwidth at each Fixed Registration Center to be provided by PSA or its nominated agency: 4Mbps Please clarify what is meant and difference in network connectivity vis-à-vis network links and/or bandwidth connectivity? It is recommended that SI is responsible for network and bandwidth connectivity to Fixed Registration Center to "wholly" investigate & resolve secure data transmission issues	External connectivity is out scope for the SI. However, the SI should provide end-to-end data encryption regardless of connectivity Please refer to Network Connectivity Diagram in Bid Bulletin No. 6.
174	General 002 Vol2 SI BID DOCS_1, Section 1 Page 1 RFP describes under Purpose of this Terms of Reference. The PSA is committed to selecting a Bidder for a 5-year contract from the issuance of Notice to Proceed(NTP) and conducting this procurement in	This project is a 5-year contract from the issuance of NTP. This includes operation, maintenance and support for the duration of the contact.

Query	Queries	Answers
	an open and competitive manner in full compliance with appropriate regulations and policies We request you to confirm that the timeline for this project will be 5 years from the NTP with PSA. This includes implementation and support duration.	
175	002 Vol2 SI BID DOCS_3 Page 85 6.3.6.2.1 Offline Authentication: User / Actor: Registered Person Role: A person registered with the PhilSys and in possession (or issued with) a valid PSN or Alyas PSN. Clarification: In this use case is the person within PSA premises or not? Or is this being done via call/video con? a. Contact Management / CRMS	In this use case, the person is not within the PSA premises. The relying party is offline and not connected to PhilSys via the TSP and uses only the PhilID card to perform some form of authentication of the person transacting business.
176	002 Vol2 SI BID DOCS_3 Page 112 6.4.3.9.2 Technical Help Desk / Incident Management System e. Escalation – capability to route specific issues to specific expert staff or managers in order to resolve pressing issues or reduce the effect of bottlenecks. Clarifications: 1. Does this mean we have to integrate to PSA's communications systems? 2. Please provide inventory of existing communication systems	This should refer to the SI's expert staff and/or managers who should be alerted and expected to provide solution to the escalated issue. PSA point persons should be alerted and involved depending on the severity of the issue through email, SMS or phone call.
177	002 Vol2 SI BID DOCS_3 Page 112 e. Escalation – capability to route specific issues to specific expert staff or managers in order to resolve pressing issues or reduce the effect of bottlenecks. How many supervisors are needed?	SI to provide optimum number to meet the PhilSys SLA.
178	002 Vol2 SI BID DOCS_3 Page 112 g. Analytics Clarifications: 1. Is cloud based analytics acceptable? 2. Will voice and screen recording be required?	Cloud-based analytics is acceptable provided no data is stored in the cloud and there is strong access management system in place like 2-factor authentication, limited specific devices and IDs that are allowed access, etc. to prevent unauthorized access.

Query	Queries	Answers
179	002 Vol2 SI BID DOCS_4 Page 150 7.4.4.2.1 Deployment of Infrastructure for Call Center Operations a. The SI shall provide PRI lines and a toll-free number for the Call Center and will bear the operational costs of these items. Please explain further the process on how this will be supported by the contact center since this is one the channels specified that they must support 1. How many PRI lines? Will you require lines from two different telco's (e.g. PLDT & Globe)? 2. How many SIM cards for the SMS gateways?	The SI should provide a solution that is responsive to the requirements on call center operations. Also, please refer to Bid Bulletin No. 6.
180	002 Vol2 SI BID DOCS_4 Page 165 The SI MUST test, install and maintain the EMS. What is the current Enterprise Management System (EMS) being considered? Can vendor also provide the following capabilities in each product/solution and is able to integrate with the EMS a. Network Management (LAN, WAN) b. Server Management, Hypervisor, VM Management c. Storage Management d. Asset Management e. Patch Management f. Backup and Recovery h. DevOps, Release Management j. Application Performance Management k. Log File Management l. Infrastructure Service Management	The SI should provide all the necessary products/features into EMS to meet the requirements in Section 6.4.3.4, Vol 2.
181	IT Infrastructure 002 Vol2 SI BID DOCS_4 Page 179 Synchronous replication can be assessed based on the distance between two data centers and the physical link availability. Asynchronous replication will be followed for non-critical applications. Please clarify if the proposed replication should support 3-way data replication i.e. (1) Synchronous Data replication between DC-1 to	Replication should be synchronous between PDC and SDC and asynchronous between SDC and DR. Please refer to Network Connectivity Diagram in Bid Bulletin No. 6.

Query	Queries	Answers
	DC-2 (2) Asynchronous Data replications between DC-1 to DR and DC-2 DR.	
182	002 Vol2 SI BID DOCS_4 Page 152 Key Features of the Proposed Call Center The key features of the proposed Call Center are given in the table below: Key Features of the Proposed Call Center (a) Phase 1: 10 Seats (b) Phase 2: 20 Seats Clarifications: 1. Does this mean that there will be a total of 30 Seats? 2. Are these the maximum concurrent users per shift? 3. Please specify if the agents will be using handphone or softphone? 4. How many supervisors are needed? 5. What are the channels that must be supported per agent (e.g. voice, SMS, email)	For Phase 1, the Call center shall have 10 seats and in Phase 2, the Call Center shall have 20 seats The SI shall propose the technology or number of supervisors needed for the Call Center. The "Remarks" entry for row item "Offsite/Onsite" of Table 43 Key Features of Call Center is hereby revised as follows: Description/ Activity: Offsite/Onsite Remarks: "The SI is responsible for selecting the location of the contact center."
183	IT Infrastructure 002 Vol2 SI BID DOCS_4 and "002 Vol2 SI BID DOCS_5, Section 7.5.2 and 9.8.3 Page 178, 234 As per Section 7.5.2, under Backup Architecture, RFP Describes, "Data will be backed up in disks for a defined duration, as per the backup policy and then data will be moved to backup media for longer storage duration", but as per section 9.8.3 under Data backup table of "Types of Data to be Backed-up" describes that every backup needs to be taken to tapes and stored at offsite media. provided statement is contradictory, Please confirm if each backup for disk based and media/tape solution has similar retention (including offsite backup), except monthly Full backup (listed as "Grandfather"). If not Please share the retention of Tape solution and Disk solution separately below: Monthly Tape Backup: Monthly Disk Backup: Weekly Tape Backup: Weekly Disk Backup: Daily Tape Backup:	There is no mention of "tapes" in Section 9.8.3, Vol. 2. The SI shall propose the type of media for its backup solution. The SI shall propose and finalize the backup strategy as per Section 9.8.3

Query	Queries	Answers
	Daily Disk Backup: This information is needed, so that SI can cater the Disk based solution capacity and no. of required media's throughout the engagement accordingly	
184	IT Infrastructure 002 Vol2 SI BID DOCS_4, Section 7.5.2 Page 178 RFP Describes under Replication Solution for Secondary DC Key applications for which Secondary DC will be leveraged are: 1) EKYC 2) Authentication 3) CRMS 4) Portal 5) ESM and ITSM DB We understand that provided application data needs to be replicated to Secondary DC. Please confirm if these application data need to be replicated to DR site as well	All PhilSys data and application data must be replicated to the DR site The SI shall perform back up of all types of PhilSys data. Please refer to Sec 9.8.3, Vol. 2.
185	IT Infrastructure 002 Vol2 SI BID DOCS_4, Section 7.7 Page 177 RFP describes under section PhilSys Registry Backup Solution Please confirm, if the Data Backup (not Data replication) is only required at PDC site only, not from the SDC and DR site.	Please refer to Section 9.8.3 for Data Backup
186	IT Infrastructure 002 Vol2 SI BID DOCS_5 Page 204 The Primary DC and DR sites will be configured in an Active-Passive Mode while the Primary DC and Secondary DC will be configured Active-Active Mode (For Front-End applications) In case of Primary DC and secondary DC will be configured Active-Active, however in network architecture there is no WAN and internet link at secondary DC. Kindly elaborate how will front end application be accessed at secondary DC.	Please refer to Network Connectivity Diagram in Bid Bulletin No. 6.
187	002 Vol2 SI BID DOCS_5 Page 204 Table 47. Hosting sites in	DCs will have a perimeter firewall. It is suggested that the winning SI bidder to provide its own internal firewall.

Query	Queries	Answers
	Long Run Do all hosting sites, Primary DC, Secondary DC and DR all have 2 sets of Firewall? 1st set as the perimeter; 2nd set as internal.	
188	002 Vol2 SI BID DOCS_5 Page 209 VPN Access VPN access, do you need a dedicated appliance for VPN gateway? How many remote users can we assume?	SI to provide optimum solution to meet performance and load requirements based on the estimated number of users in Section 4.5, Vol 2.
189	002 Vol2 SI BID DOCS_5 Page 211 Information Security Can the Firewall and the IPS be on the same appliance? For the web gateway, for how many users? Does the DR need to have an appliance as well? Is a physical separation required for the infrastructure resources to be used for internal endpoints (data from FRC) and externally facing APIs (northbound services i.e. Authentication from banks, etc.), aside from a logical separation available in a software defined computing/storage or hyper converged set up? Such considerations have twice cost impact in overall design across 2 DCs and DR.	The SI should propose a solution which is responsive to meet the KPI and SLA requirements.
190	002 Vol2 SI BID DOCS_5 Page 251 9.8.6.10.2 Dashboard and Reporting a. Provide a visual dashboard to display call graphs of multiple applications/instances b. Allow multiple users to track and analyze their applications concurrently in the dashboard c. Provide role-based access to applications We request you to elaborate on this requirement	The SI should provide a solution that is responsive to the Dashboard and Reporting requirements.
191	002 Vol2 SI BID DOCS_5 Component Specifications Aside from defined DC sites, would you be proposing utilizing public cloud in this application? Will the solution be integrated to public clouds? Dashboard and Reporting	No. Only Government-provided cloud services should be used.
192	002 Vol2 SI BID DOCS_5 Network Operations Center	As an alternative to a landline solution, the SI can propose VOIP or similar solutions to the NOC/SOC.

Query	Queries	Answers
	(NOC) and Security Operation Center (SOC) We understand that the physical space for the SOC, NOC will be provided by the PSA. Please confirm if the non- IT work related to Civil work, Furniture etc. for the SOC/NOC is under the responsibility of the SI or will be provided by PSA. Please confirm if Phone connection for the NOC/SOC is also under the scope of the SI or will be provided by PSA.	
193	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.8.3 Page 233 RFP describes under Types of Data to be Backed-up For a 5-day working week, there are 4 son backup media, 3 father backup media, and a new grandfather backup media every month. Our understanding from this statement is that PSA requires retention of monthly backup of 1 week, weekly backup of 3 weeks and daily incremental of 4 days. Please confirm the requirements	In a month, the number of backups are as follows: a. 4 daily incremental backups for one week, 16 incremental backups for a month b. 3 weekly full backups c. 1 monthly full backup
194	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.8.3 Page 233 RFP describes under Data Backup: Table 56. Types of Data to be Backed up We understand that data backup needs to be taken as per schedule listed by PSA and to be stored at offsite location. Please confirm that offsite location and transfer of tapes from DC to offsite location would be taken care by PSA (including logistics)	The offsite location and transfer of tapes from DC to offsite location, including logistics, is still under the scope of work of the SI.
195	IT Infrastructure 002 Vol2 SI BID DOCS_5, Page No. 254, Section 9.8.7 Page 254 The SI shall provide up to One (1) Migration services for each of the PhilSys Data Centers, namely, Primary Data Center, Secondary Data Center and Disaster Recovery Site as part of this contract. The SI shall be responsible for the migration of the ICT	1. No existing DC needs to be migrated. 2. No. Please refer to the following locations: Primary DC: Metro Manila Secondary DC: Clark, Pampanga Disaster Recovery Site: Subic, Zambales

Query	Queries	Answers
	equipment/rack, including but not limited to transportation, coordination, manpower, from current location to a new data center location at no additional cost, with supervision from the PSA. to transportation, coordination, manpower, from current location to a new data center location at no additional cost, with supervision from the PSA. Kindly elaborate this section requirements, including below items: 1. Are there any existing DC's that needs to be migrated, if yes, please provide details of existing DC IT infrastructure. 2. Is PSA planning to migrate the PDC, SDC, DR after the installation by the SI to be selected as part of this RFP	
196	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 8.1.3 Page 182 RFP Describes under Server Specifications - At the time of bid submission, SI shall propose the latest (within the last 1 year) server model with proof from OEM. Please elaborate last 1 year requirement - Does that mean the product should have been launched within last 1 year or the product should have not declared End of Life or end of Support in last one year	Please refer to Section 8.1.3, as amended by Bid Bulletin No. 5, which reads: 8.1.3 Server Specifications a. At the time of bid submission, SI shall propose the latest (within the last 1 year) server model with proof from OEM. The OEM can be based on the server model or series. b. The proposed server models should support redundant power supplies.
197	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.6.3 Page 204 Primary Data Center and Secondary Data Center Set-up. The proposed solution should be optimized for power, rack space while ensuring high availability and no single point of failure We understand SI scope on DC Non-IT is limited to Racks Sizing, placement of IT Hardware/resources. The Unit DC facility components (Cooling, Power, Fire-Safety, etc.) will be arranged by PSA, please confirm	The Unit DC facility components (Cooling, Power, Fire-Safety, etc.) will be arranged by PSA.
198	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.6.5 Page 204	Please refer to Cloud Deployment Strategy Diagram in Bid Bulletin No. 6.

Query	Queries	Answers
	RFP describes under 9.6.5: Business Continuity and Disaster Recovery (BCP/DR) "The Primary DC and DR sites will be configured in an Active-Passive Mode while the Primary DC and Secondary DC will be configured Active-Active Mode (For Front-End applications)" and Under section 9.6.5.1, Table 48. Recovery Strategy describes: Authentication, PhilSys portal(s), Email, CRMS, SOC application requires · Active – Active (DC – DR), offline backup · 100% data backup in Secondary DC Provided clauses describes DR site should be active-active and active-passive both. Please clarify, if DR site should be designed as active - passive or active-active for all applications. Please also confirm whether the Secondary DC site is only a Data backup site or if PSA is also expecting to run critical applications from the Secondary DC.	
199	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.6.5.1 Page 206 Under Table 48. Recovery Strategy, item name Authentication, PhilSysportal(s), Email, CRMS, SOC Active – Active (DC – DR), offline backup is mentioned As per RFP, DR site has to be in Active-Passive Setup, so why the Active-Active requirement is listed	Please refer to Cloud Deployment Strategy Diagram in Bid Bulletin No. 6.
200	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.6.6 Page 207 RFP describes under Business Rationale for RPO and RTO for Other Portals RTO: It is understood that these portals are not public facing and criticality RPO (Logs databases and Registration, Authentication	Please refer to Bid Bulletin No. 5.

Query	Queries	Answers
	databases): It is a business requirement to ensure there is no data loss in case data other than logs is present. RPO of "Other Portals" application is defined as 5 minutes, which means this application will face 5 mins of data loss while recovery, so it is suggested to remove the contradictory line statement " It is a business requirement to ensure there is no data loss in case data other than logs is present" , as not data loss means Zero RPO. Also please specify the list of items categorized under "Critical Portals"	
201	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.6.6 Recovery Time Objective (RTO) and Recovery Point Objective (RPO) RTO for CRMS and SOC is defined as 5 minutes. We suggest to change the same to 30 minutes to align with the critical applications i.e. Authentication. "Other Portals" with Medium criticality is also defined with 5 minutes RTO and RFP. Please look into this and suggested to change the same as RPO: 24 hours, RTO: 30 minutes.	The RTO for CRMS and SOC is retained at 5 minutes.
202	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.6.7.3 Page 210 RFP describes under Testing of BCP/ DR: Power Source and UPS maintenance, Quarterly maintenance of Power Source and UPS as per manufacturer specifications We understand Supply and installation of DC/DR facility components i.e. Power, UPS, cooling is not under the scope of bidder. Thus, request you to remove the maintenance of these components from the SI scope	Please refer to Bid Bulletin No. 6.
203	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.8.4.2 Page 235 Storage Design, Policies and Procedures - Item a. 1) Archival Cluster - 700 TB, 2 replica copies, Raw Capacity – 1500 TB	Confirmed.

Query	Queries	Answers
	2) Log Cluster – 120 TB, 2 replica copies, Raw Capacity – 264 TB 3) ODS Store – 130 TB, 2 replica copies, Raw Capacity – 273 TB 4) Authentication Data Store – 20 TB, 3 replica copies, Raw Capacity – 66 TB 5) Test & Dev Store – 100 TB, 2 replica copies – Raw Capacity – 220 TB We understand, 2 replica means one replica copy at PDC and DR each. 3 replica means one replica copy mean PDC, SDC and DR each. Please confirm.	
204	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.8.3 Page 234 As per section 9.8.3 under Data backup, Item # 3) which describes "Daily incremental backup shall be done called the "son". Son backup media can be stored onsite or offsite depending on the volume of data changes. Onsite backup media shall be kept in fireproof cabinet." Please confirm if SI needs to provide fireproof cabinet at both primary Data center and Offsite locations.	The SI should provide a solution that is responsive to the requirements.
205	IT Infrastructure 002 Vol2 SI BID DOCS_5, Section 9.8.6.12.1 Page 252 As per Section Infrastructure Service Management, RFP describes "Support IaaS, PaaS and SaaS Services as required" We understand that SI would be providing on-premise solution and services. Please confirm. We also understand that PSA is not looking for any additional Cloud Services i.e. PaaS, SaaS from external cloud vendor. Please elaborate on the IaaS/PaaS and SaaS requirements. In case, PSA is looking for any additional Cloud Services i.e. PaaS, SaaS from external cloud vendor, please provide the list of applications that	Please refer to Bid Bulletin No. 5 on Hybrid Cloud System Architecture.

Query	Queries	Answers
	needs to be hosted on PaaS and SaaS.	
206	IV. Breakdown of Contract Price A. Payment Schedule Page 132 Supply, Implementation and Commissioning of IT Hardware at Primary Data Center, Secondary and Disaster Recovery Site for Version_1 Page 120: FPF 2. Summary of Costs: In this table we have observed 8 different line items under HARDWARE AND SOFTWARE category. However, there is NO line item to indicate "Secondary Data Center" cost. How the bidder will indicate the "Secondary Data Center" cost in this table? Request you, kindly review the "FPF 2. Summary of Costs table (Page 120)" and help us with proper input.	Please refer to Section 9.6.1, Vol. 2 on Data Center Strategy of Project. Item number 2 states that "The Primary Data Center will be replicated to Secondary Data Center on real-time basis for all critical application except raw registration packets whose replication frequency will be decided at the time of implementation." This implies that the costing for the secondary data center is the same with that of the primary data center.
208	Question and Answer as of 17 June 2020 Yes, LAN connectivity is part of the SI's scope. The SI needs to provide Firewall and IPS for all locations/sites. This project also needs enabling technologies for Network Performance Monitoring, Network Behavior Analysis, Network Management System, Threat Intelligence and Endpoint Detection and Response 1. We understand IPS is required to be provisioned at PDC, SDC and DR. Does SI need to provision NIPS device for FRCs as well? please confirm 2. We understand "Network Performance Monitoring, Network Behavior Analysis, Network Management System, Threat Intelligence and Endpoint Detection and Response" need to be provisioned for the PDC, DR and SDC only. Please confirm.	The SI should provide a solution that is responsive to the requirements and SLAs/KPIs.
209	Hardware and Consumables Section 5.2 Page 36 **Supply, Installation, Commissioning of IT infrastructure and Software System** The hardware and peripherals to be provided must be verifiable (appearing in an	Sec. 5.2, Vol. 2 is maintained.

Query	Queries	Answers
	international, reputable (bad or good) source i.e. Gartner, Forrester, G2 Crowd, PCMag, etc.). The RFP requires multiple hardware and software components and all of them may not be available in Gartner and Forrester reports. Thus, we request you to revise the clause as follows: The hardware and peripherals to be provided must be verifiable (appearing in an international, reputable (bad or good) source i.e. Gartner, Forrester, G2 Crowd, PCMag), wherever available.	
210	Section 9.4.1 Warranty & Annual Technical Support Page 197 It is mandatory for the SI to take enterprise level annual support over the entire contract duration, at a minimum, for the MOSIP underlying tools and components software(s). The SI should also refer to the MOSIP documentation at https://github.com/mosip/ on MOSIP underlying tools and technologies For MOSIP components: (a) is it mandatory to provide Enterprise Level Support? (b) If reply for (a) is "Yes", for software components for which the enterprise level annual support is not available, please confirm that we can propose a community edition support	The SI should provide a solution that is responsive to the requirements.
211	Section 9.4.1 Warranty & Annual Technical Support Page 197 The SI shall be responsible for providing annual technology support for the COTS/OTS products supplied by respective OEMs during the entire maintenance and management phase. It is mandatory for the SI to take enterprise level annual support over the entire contract duration, at a minimum, for the software(s) as mentioned in the Summary of Costs provided by the SI. For Non-MOSIP components: (a) is it mandatory to provide Enterprise Level Support? (b) If reply for (a) is "Yes", for software components for which the enterprise level	The SI should provide a solution that is responsive to the requirements and SLAs/KPIs.

Query	Queries	Answers
	annual support is not available, please confirm that we can propose a community edition support	
212	Technical TPF 8. Activity (Work) Schedule Page 112 A. Field Investigation and Study Items Request you, kindly elaborate the clause "Field investigation". What kind of activities are expected in this activity (work) schedule?	Field investigation refers to requirements gathering.
213	Technical Proposal Vol 2, section 7.4.15.2 Email Gateway: An authenticated SMTP mail service (also known as SMTP relay or smart host) is envisaged to be integrated with the solution for sending mail from the solution and delivered to the intended inbox. Support anti-spam features. The SI must consider this service and its integration in the proposal. The SI is required to propose email solution such that there is one email address per user. Additionally, the email address will be created for applications (e.g. authentication.notification@psa.gov.ph). For such cases, 100 email addresses will be required. Please confirm if the Supply and installation of Emailing solution is also under the scope of the system integrator or only integration with the application is in the scope. If SI need to provide the emailing solution, please confirm if a cloud based emailing solution can be provided as there is requirement of only 100 email accounts	This is to confirm that the SI scope of work includes the supply and installation of emailing solution that is responsive to the requirements, SLAs/KPIs of the project.
214	Technical Proposal Vol 2, section 9.6.1, 9.6.7.2 1) The Primary DC and DR sites will be in 1:1 configuration i.e. exact replica of each other. Table 51. Disaster Recovery Strategy and Procedures: 2. Redundancy at component level in DC, Redundancy for critical components in DR	Please refer to Cloud Deployment Strategy Diagram in Bid Bulletin No. 6.

Query	Queries	Answers
	As per the RFP clause in section 9.6.1 DC and DR should be exact replica with 1:1. We understand here exact replica is refereed for the availability of all applications and not for infrastructure. Please confirm As per the section 9.6.7.2 of the RFP DR needs to have redundancy for critical components in DR. We understand only critical components required to be in redundancy in DR and all DR hardware components are not required in Redundancy. Please confirm. Please also confirmed the components classified as critical to include in our solution accordingly. Please also confirm the redundancy requirements in Secondary DC infrastructure components.	
215	BIAS and FDMS Vol 2. section 13.3 Delivery and Acceptance of PhilSys Information System Application Version_4 Page 275 Delivery of application and hardware; and signed Certificate of Acceptance/Inspection for the following deliverables: a. BI and Data Analytics b. Dashboards c. Fraud engine set up Duration: 600 Calendar days after issuance of Notice to Proceed As per the timelines, all the BIAS and FDMS components duration is 600 calendar days. Please confirm if this assumption is correct, or are we required to share any deliverable related to BIAS/FDMS before 600 days	This is to confirm that the SI is required to share any deliverable related to BIAS/FDMS within 600 days after NTP.
216	VOL 2: Section - 4.6 Network Connectivity (DC-DR Replication Link). The link and / or including bandwidth connectivity shall be provided by PSA or its nominated agency : 1 Gbps Network Connectivity (Primary DC, Secondary DC and DR Site link) The link and / or including bandwidth connectivity shall be provided by PSA or its nominated agency : 500 Mbps Capacity As per the RFP section 4.6.	Please refer to Bid Bulletin No. 6. Note: provide the network connectivity diagram.

Query	Queries	Answers
	the DC-Dr capacity is different at two locations. Please confirm the capacity provided between: 1. PDC- DR 2. PDC- SDC 3. SDC - DR	
217	VOL 2: Section - 4.6 For Pilot, the DC-DR will be in the same city. Subsequently, the DC and DR will be more than 100 KMs apart 1. We understand for Pilot SDC is not required. Pls confirm 2. RFP has a mention of Migration requirement. IS the migration linked to after Pilot Migration requirements? 3. Please confirm if both DC-Dr locations will be changed after the Pilot or only DR will shift to another city. 4. Please confirm if the DR location used during the Pilot will be used for SDC after Pilot	1. Yes pilot SDC is not required. 2,3 & 4 Please refer to the following locations: Primary DC: Metro Manila Secondary DC: Clark, Pampanga Disaster Recovery Site: Subic, Zambales
218	VOL 2: Section - 7 Network equipment for priority use cases: Multi-Protocol Label Switching (MPLS) router for the pilot at first two RPs/TSPs (PSA and DSWD). 1. We understand the requirement form MPLS perspective is only that the Router should be capable to connect as CE router with the MPLS Cloud service provider. 2. Please confirm how many routers need to be provisioned at each Pilot location i.e. 1 or 2 (HA) 3. We understand any LAN components for these pilot sites are not under the scope, please confirm	The SI should provide a solution that is responsive to the requirements. This is to confirm that the LAN requirements within the pilot RPs/TSPs are not within the scope of work of the SI.
219	VOL 2: Technical Specifications Page 29 Section 4.6 Technical Parameters It is requested to confirm what is the external network throughput requirement of DC and DR sites?	External network throughput requirement is not part of the SI TOR. The SI will not be penalized for unmet SLAs caused by factors outside its control.
220	VOL 2: Technical Specifications Page 214 Section 9.7.1 Security Framework - The patch management	The SI should provide a solution that is responsive to the requirements.

Query	Queries	Answers
	solution should provide automated patches of the Operating System, Firmware, Virtual Machines, Hypervisors and Applications The Antivirus solution should be deployed on all endpoints It is requested to confirm if SI required to deploy the below mentioned endpoint security solutions on registration kits: 1. Endpoint Protection 2. Patch Management 3. DLP	
221	VOL 2: Technical Specifications Page 213 Section 9.7.1 Security Framework - Protection against attack like DDoS can be catered by ISP providers securing PhilSys network from such attacks at off-premises locations. It is requested to confirm if SI is responsible for procuring DDoS solution from ISP or will it be purchased by PSA	The SI shall provide the required number of licenses and subscriptions of the various information security products. Please refer to Sec. 9.7.3, Vol. 2 on Provide Information Security Products.
222	VOL 2: Technical Specifications Page 213 Section 9.7.1 Security Framework - All the incoming and outgoing mails should be scanned against the rules deployed at Mail Gateways. It should protect PhilSys from both Spam and phishing mails. It should integrate with advanced persistent threat solution. It is requested to confirm if SI is responsible for procuring Anti-APT solution or will it be purchased by PSA	The SI shall be responsible for procuring anti-APT solution for email gateway that is managed by the SI. Please refer to Sec 7.4.15.2, Vol. 2 on Email Gateway.
223	Training We understand that the training and certification of operators is required under this project. This certification may be awarded to the operates who successfully clears the certification examination after the training. As there may be restrictions in SI firm's policies around branding of certifications, we request you to confirm that the certification may be branded by PSA only	Participants to trainings will be provided with certificates that they have completed the training, and not necessarily certifications. Certificates will be issued by PSA.
224	Bid Submission date: 6th July Many of our technical	Bid submission date of July 22 is maintained.

Query	Queries	Answers
	questions are still not responded in the clarification issues on 15th June and 17th June. We understand that PSA is working on the same and will issue last bid queries response on 29th June. As there are many dependencies on technical queries for the final solution, we request you to extend the bid submission to at least for two weeks from the last clarifications to be issued by PSA.	
225	Core Switch 1. What is the minimum interface requirement of the stackable core switch? 2. What is the minimum switching capacity for line rate and minimum forwarding rate? 3. What is the average latency for the core switch? 4. What is the stacking capability required for the switch at full duplex? 5. What deployment should the switch have to not disrupt the forwarding traffic operation in the switch? 6. What can the switch do to manage the edge device? 7. How can the switch be managed and configured?	The SI should provide a solution that is responsive to the requirements.
226	Clarification on conflicting statements on pages 33 and 43 concerning SMS costs. Page 33 indicates SI is responsible while page 43 states otherwise (exclusions).	Please refer to Bid Bulletin No. 6.
227	Annex F 3.8 Registration and Update Manager ☐3.9 Authentication, e-KYC, APIs and Ecosystem Partnership Manager Experience: Registration and Update Manager has worked on at least one (1) project involving IT system rollout for large user bases (in excess of 100,000 users) and has prior experience of National ID, civil registration or public service delivery. 1. For the following resources, can the experience requirement "has worked on at least one (1) project involving IT system rollout for large user bases (in excess of 100,000 users) and has prior experience of National ID, civil registration or public service delivery" be removed or at least relaxed? We have been	Please refer to Bid Bulletin No. 6.

Query	Queries	Answers
	searching for weeks already and we have not found a candidate that meets this requirement. If the large user base one project (in excess of 100,000 users) will be eased or removed, then we would be able to comply.	
228	1. Required information under TPF 6. Format of Curriculum Vitae (CV) for Proposed Professional Staff Please confirm if the required professional staff are those under the Annex F - Profile of Key Personnel only and does not include other technical support team?	Annex F provides the minimum requirements. SI can propose other technical support team as it sees fit.
229	Section 7.4.16.2.2 Metering & Pricing Configurations Page 172 Support definition of different types of metering configurations in PhP, including uniform pricing, slab pricing, subsidized pricing for specific customers, premium pricing for specific customers, other types of differential pricing (time-based, service-based), pricing for packaging & bundling, etc. including periods of validity In our understanding the metering requirements in National Identity projects are quite standardized and simplified. Based on our understanding of National Identity projects, some of these features may not be required. Thus, we request you to review the requirement (especially around metering) and, if necessary, please revise the requirements.	The provision is there to provide clarity to all stakeholders regarding the PhilSys requirement to support various metering and pricing configurations for the PhilSys. The SI is encouraged to propose solutions that are responsive to the requirements.