QUESTIONS & ANSWERS
as of 17 June 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	**Page 41, Point 8** **Benchmarking, Commission, Acceptance and Go-Live** Undertake benchmark exercise before Go-live. 1. Please share the Benchmarking Script in-terms of No. of Records, Scope of Benchmarking, No. of days, Hardware Availability at DR locations etc.	Benchmarking parameters and metrics should be jointly developed by PSA and the winning bidder during project initiation/kickoff.
2	**Page 42, 5.4 Exclusion:** **ABIS software and hardware for deduplication, Manual Adjudication System and biometric SDKs** 1. Kindly provide specification and BOM of ABIS hardware proposed by the vendor ? 2. The SI has to do interface with ABIS system hence it is important to know IT infra details which is provided by the ABIS supplier.	1. The necessary information will be provided to the winning SI bidder. 2. The interfacing with Automated Biometric Identification System (ABIS) system will be via API.
3	**Page 75, 6.3.4.5** **Manual Demographic Verification** The SI MUST provide an interface for an operator to manually compare results of demographic deduplication performed by IDMS and biometric matching scores from the ABIS provided as part of a registration packet to candidate matches identified by the automated demographic 1: N matching process. 1. We understand the MOSIP IDMS application and ABIS Manual Verification Suite will be used for the same. what is the expectation from SI on this by means of Interface for an Operator	The SI MUST provide the MV module. The Manual Adjudication (MA) and the Manual Verification (MV) modules are not used for the same purpose. The MA module allows a human operator to compare biometric images of candidates sent back by the ABIS after an inconclusive 1:N search (deduplication). The MA module is provided by the BioSP. The MV module allows a human operator to review all exceptions raised by ABIS and/or MA. The interface for the operator represents a suite of applications to facilitate the requirements in table 24 of 6.3.4.5 to be developed by the SI.

		Please refer to https://procurement.psa.gov.ph/sites/default/files/ABIS%20Bid%20Docs_compressed.pdf page 43 of Volume II (page 140 of the PDF)
4	**1.12 Collaboration with Civil Registration** **In line with best practices on the harmonization of civil registration and identification services, the PhilSys will collaborate with the Civil Registration Service to authenticate vital events such as births, deaths and marriages, in order to coordinate up-to-date authentic information with use case relying parties in compliance with existing laws, rules and regulations** Kindly confirm how the integration will be done with Civil Registration System. Does Civil Registration System have any API or manifest files which need to be connected to receive information from Civil Registration System.	We confirm that there will be collaboration with the CRS. The details of this collaboration will be discussed with the winning bidder.
5	**5 High-Level Scope of Work** **Table 12. Overview of the scope of work (software development) Integration with BioSP Solution** Please confirm that BioSP will provide the required SDK and license for the Registration Kits (for Mobile and Permanent centers) for Fingerprint, Face, and Iris 1:1 matching. The SDK component expected to be provided by the BioSP are: - Fingerprint Quality Check - Face Quality Check as per ICAO - Iris Image Quality Check - 1:1 Verification so confirm that the duplicate fingerprint is not captured. To avoid enrollment packet rejection in Backend ABIS because of Quality Threshold, the BioSP SDK for the Client System must provide the same Quality Check SDK which is used at the Backend ABIS.	This is to confirm that BioSP will provide the required SDK and its licenses for both the front end for the registration system, and back end systems for registration and authentication.

6	**Table 14. Overview of scope of work (other services)** Technical Services Periodic (Monthly) accuracy test of the automated matching for all biometric modalities of both the ABIS (1:N) and the ABAS (1:1). About Benchmarking of the ABIS, please confirm that the Speed and Accuracy of the ABIS will be the responsibility of BioSP provider.	Yes, the speed and accuracy will be the responsibility of the BioSP. The automated functionality to benchmark will be provided by the SI.
7	**6.1.2.4.1 Automated Biometric Authentication System (ABAS)** The ABAS will process requests to authenticate individuals against fingerprints, irises or facial images held by the PhilID Registry (see Authentication Services). Please confirm that the BioSP provider will provide the essential API Documentation for integration with ABIS.	The BioSP is expected to comply with the MOSIP API specification for ABIS interfacing with the PhilSys platform. Please refer to this link. https://docs.mosip.io/platform/biometrics/automated-biometric-identification-system-abis Please note that the SI MUST design, develop, deploy and maintain the ABAS by integrating the 1:1 biometric matching SDKs (fingerprint, iris and face) provided by the BioSP. ABAS MUST have its own reference database of biometric templates and is unrelated to ABIS. ABAS and ABIS are two completely separate systems sharing no resources.
8	**6.1.2.6 Manual Verification** The manual verification module is provided to enable authorized PSA staff to review: b. Potentially fraudulent cases raised by the fraud detection system. Kindly Elaborate Fraud Detection System and does it require Integration with 3rd party systems. If yes, please provide scope and integration requirements.	It is the scope of the SI to propose and implement a fraud detection system encompassing various PhilSys processes (e.g. registration, adjudication, authentication). The SI must be able to articulate how the fraud detection system will be implemented in the technical design documents, as part of their proposal. The

		Fraud Detection System must be able to account for PhilSys internal and external actors.
9	**Page 42, 5.4 Exclusions** PhilID cards personalization systems (card printers, QA workstations, etc.), services and consumables (pre-personalized blank cards, inks, overlays, etc.)	
	1. Who will be providing Card Printer SDK for integration with Card Printer?	1. The BSP will provide personalization printers and kitting/enveloping machines with corresponding drivers and bundled personalization software.
	2. Does it mean Printer, QA Workstation and other required hardware and environment maintenance and services?	2. Yes, personalization printers, QA Workstation and other required hardware and environment maintenance and services are not included in the scope of work of the SI.
	3. Card Inventory and Tracking of Card availability and re-order levels will also be out of scope for SI?	3. Card inventory and tracking of card will be provided by the SI. These are features of the CPMS.
	4. Does Card Design come under SI’s scope or out of scope for SI?	4. Card design of the PhilID is not included in the scope of work of the SI.
	5. Do we have Pre-personalized card design available?	5. Yes, pre-personalized card design is available.
10	**Page No: 53, 6.1.2.9 PhilID Card Management** the actual personalization of the PhilID Cards will be carried out by PSA	
	Is there any targets on no. of cards to be produced within the specified timelines? How many printers will be stationed for printing and what is the average no. of cards expected to be produced in a day?	The target production, personalization, and enveloping targets for PhilIDs can be computed based on the estimated average daily output of 144,000 PhilID cards.

11	**Page No: 94, 6.4.1.2.8 Request for a new PhilID Card** A reason for reissue should be provided by the individual and proof of payment before a new card can be issued. Is it only a proof of payment to be captured and no payment integration required at this stage?	The minimum requirement is prescribed in 6.4.1.2.8. The bidder can propose other optimal solutions such as a payment gateway.
12	**Page No: 103, 6.4.2.5.2 Generate Print Files for Card Personalization** b. The SI shall provide a system for tracking and monitoring the delivery of all PhilID cards. Does it mean the option to be given at PFRC to confirm the delivery of cards after receiving?	Please refer to 6.4.2.5.3 Track Personalization Orders. PFRC personnel must be able to log all received PhilIDs through a system to be developed by the SI. This is a feature of the CMS.
13	**Page No: 113, 6.4.3.9.5.1 Personalize PhilID** b. The CPMS sends requests for batches of records for card printing. Are these records grouped as a batch based on PFRC?	Yes, records for personalization can be grouped as a batch based on PFRC.
14	**Page No: 114, 6.4.3.9.6 Card Shipment** The CPMS prepares for the packaging or kitting of the PhilID and other communication materials into individual envelopes. What are other communication materials?	Other communication materials include transmittal letters, list of enveloped PhilIDs, etc. that will be used to turn over the cards to the delivery partner.
15	**Page No: 114, 6.4.3.9.6 Card Shipment** Card Shipment status of the envelopes are updated through the CPMS. Shipment status means whether shipped or not and also through which delivery partner and tracking number?	Yes, the shipment status means whether the PhilID was shipped or not. The status of all PhilIDs for turnover to the delivery partner will be updated through the

		CPMS by PSA employees. The tracking number for each envelope is the transaction number of the data subject. The transaction number is also printed in their transaction slip, sent to them via SMS message and/or email after their successful registration in the PhilSys.
16	**Page No: 114, 6.4.3.9.6.2 Card Release Status** When the Registered Person comes to the PFRC to claim his/her PhilID, the PFRC Registration Officer/Staff releases the envelope and PhilID after a successful authentication. Is it going to be Biometric Authentication? Will there be any provision to release the card without authentication in case if the applicant is not in a position to come to collect his / her card?	All PhilIDs released in the PFRCs will be biometrically authenticated. Details of the provision to release the card without authentication in case if the applicant is not in a position to come to collect his/her card will be shared to the SI.
17	**Page No: 166, 7.4.11 Card Personalization and Management System (CPMS) c. The CPMS MUST generate, forward and follow up on PhilID Cards personalization orders.** What is forward card personalization orders? Forward to whom?	The CPMS interfaces with the Card Personalisation System (the bundled personalization system of the printers) for actual printing, therefore requests will need to be forwarded to this system by the CPMS. See 6.1.2.10 PhilID Card Management. The CPMS automatically prepares and forwards PhilID card personalization orders (in batches) to the card personalization system procured by BSP.
18	**Page No: 166, 7.4.11 Card Personalization and Management System (CPMS)** i. The data transfer shall be on SFTP (Secure File Transfer Protocol). The SFTP download / upload client shall be provided or specified, as the case may be, by SI to the BSP Service Provider and the SI shall install the server with the same SFTP client at BSP printing premises and use it for download / upload of data from / to PSA.	

	Will the Server be provided by BSP?	No, the SI will provide the server for which the CPMS will run and data for personalization will be stored. A firewall will also be required from the SI.
19	**Page No: 166, 7.4.11 Card Personalization and Management System (CPMS)** I. The SI is expected to validate the data file structure, verify the mandatory fields as specified by PSA and print only unique records. How to identify whether it's a unique record or not? It was expected to delete the record after successful printing.	The unique identifier of an individual record is the transaction number.
20	**Page 224, 9.8.1.1 Benchmarking** 3) Provide the tools (load generator), scripts for etc. for benchmarking. Performance tool to be procured by SI?	Yes.
21	**Page 224, Table 54. ABIS Test Scenarios** Gallery Size 10 million 1. Who is responsible for providing the gallery? 2. Does it mean that 10 million Biometric records having Fingerprints, Face and IRIS templates or 10 million Fingerprint records?	1. The BioSP provider is responsible to provide the gallery. 2. This is to confirm that the gallery will have 10 million Biometric records having Fingerprints, Face and IRIS templates.
22	**Page 202, 9.4.6 Migration of Pilot Registration Data** The SI shall migrate pilot registration data (approximately one million records including demographic and biometric data) into the PhilSys Registry. 1. Is it a full blown Registration System? 2. What is the current status of the Pilot Registration? Is it completed or still on going? 3. Is it only the registration completed during Pilot or Cards also issued? 4. Is Pilot application source code available?	1. Yes. It is a full blown registration system. 2. The status of the pilot registration is completed. 3. Only the registration is completed. 4. Yes, the pilot application source code is available.

23	**Page 109: 6.4.3.3 Customer Relationship Management System (CRMS) sub-Clause 5 (b): Letters sent via postal services (including handwritten ones)** 1. will the contents of the physical letters need to be typed and entered into the system? 2. will the physical letters need to scanned, digitised and archived? 3. since this process is initiated outside of the system - we presume it will be the responsibility of PhilSys to track incoming letters and be registered on the system	1 and 2. Yes, to facilitate ease of indexing and retrieval as well input for analytics. 3. It will be PSA who will initiate the tracking of incoming letters to be registered on the system.
24	**Page 110: 6.4.3.3** Customer Relationship Management System (CRMS) sub- Clause 5 (c): The CRMS also retrieves the list of current incidents detected at the infrastructure level and inform CRMS operators accordingly. This requires an interface between CRMS and EMS. The CRMS also produces and disseminates activity reports on a regular basis. Kindly confirm if the CRMS need to have two logical sections - one which is citizen facing, two which is internal facing; is the CRMS expected to be the default incident reporting, tracking and management system as well?	We confirm. CRMS is designed for receive complaints and feedback from the general public. PhilSys officers will have access to such complaints and will be able to facilitate and/or resolve the concerns submbitted via the CRMS. The CRMS serves as the de-facto incident reporting, tracking and management system for PhilSys applicants, registered persons and stakeholders.
25	**Page 112: 6.4.3.9.2 Technical Help Desk / Incident Management System sub- Clause (a):** What is the expected number of ports required for the call center operations?	The SI is expected to estimate this based on their experience and the requirements stated in the document.
26	**Page 150: 7.4.4.2.1 Clause 7.4.4.2.1 Deployment of Infrastructure for Call Center Operations sub-Clause (b) (1)** Does PhilSys have any guidance on the actual physical location of the Call center?	The deployment of infrastructure for call center operations must be within the Philippines.

27	**LDAP Server** Please confirm if you have an LDAP server already which can be used ?	There are no LDAP servers that we can use at this time. The SI is expected to propose a corresponding solution.
28	**Email Server** Please confirm if you have an Email server already which can be used ?	A separate email server must be established for PhilSys by the SI
29	**Connectivity** For Permanent Registration Location : Do we need to provide LAN connectivity ? How many Switch to be provided for these 250 Locations ? Do we also need to provide the Firewall and IPS for these locations ?	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.
30	**Connectivity** What connectivity is present at these 250 Locations	Connectivity is a mixture of Broadband, 4G, or Fiber.
31	**Fraud Management System** Please confirm if there is a Government policy framework already present in regard to this ?	The SI must be able to define, propose, and implement a framework for Fraud Management as part of its services to PhilSys.We are not aware of any existing government policy framework at this time.
32	**Environment** Please confirm how many environments to be provided for the same ?	The SI must be able to define, propose, and implement the number of environments to be provided as part of its services to PhilSys.

33	**1.2.2 Procurement of Main Components of the PhilSys** The main components of the PhilSys have been or will be procured separately, namely: 1. Supply, Delivery and Managed Services of 5,000 Registration Kits for the Philippine Identification System (PhilSys) (awarded in August 2019); 2. Supply, installation, support and maintenance of Automated Biometric Identification Systems (ABIS) for Philippine Identification System (PhilSys) (awarded in April 2020); 3. Consultancy Services as System Integrator for the Philippine Identification System (PhilSys) (this procurement); and 4. PhilID card production and personalization, to be procured by the Bangko Sentral ng Pilipinas (BSP). PSA to reconfirm that these are not under this Tender Scope of Work and these are already procured and available. If its out of scope, PSA to provide complete details and specifications of Registration Kits, ABIS, PhilD Card and Personalization Software. This information is required for the SI to design, develop software application, Integration with hardwares, etc.	This is to reconfirm that the following are outside of the SI scope of work 1. Reg Kit procurement bid docs at https://procurement.psa.gov.ph/node/3938, 2. ABIS procurement bid docs at https://procurement.psa.gov.ph/node/4220. 3. PhilID card production and personalization
34	**Software to be deployed at Relying Parties (except for the pilot application to be deployed at PSA and DSWD)** Kindly provide details of the location, space (no. of workstations that can be accommodated) for development of software application that shall be provided by PSA	PSA will not provide the space necessary to develop the software for pilot applications. PSA will not provide any piece of software. The SI MUST design, develop, deploy and support a pilot client application that will be used at PSA and DSWD to showcase all forms of online authentication. Regarding full scale deployment, please note that the Relying Parties will implement their own

		client software (or integrate with existing business software) based on the API to be developed by the SI.
35	**Central sites (Primary DC, secondary DC, DR) and utilities. The PSA shall provide the physical space for hosting IT Infrastructure in a Primary Data Center and Disaster Recovery site as well as Secondary DC.** Kindly provide the proposed location where the Primary DC, Secondary DC and DR is to be setup	Please refer to page 204, Section 9.6.1 (Data Center Strategy of Project) of the SI Bidding Documents volume II.
36	**The SI MUST integrate all back-end PhilSys applications including the design and implementation of final workflows.** Kindly confirm that PSA shall be responsible to provide API of back-end PhilSys applications and other third party appliction for Integration.	The SI must be the one providing the APIs of the components that are part of their solution. Only third party apps that are not part of the SI scope should be provided by PSA.
37	**Integration with BioSP Solution** Provide integration with biometric SDKs provided by the BioSP for PhilSys front-end systems (registration client) and back-end services (e.g. biometric 1:1 matching SDKs for fingerprint, iris and face). PSA to get biometric SDKs from BioSP and provide free of cost to SI for integration. Kindly confirm.	Biometric SDKs will be provided by the BioSP to the PSA and will be available to the SI for integration to the PhilSys platform. For purposes of integration, corresponding licenses are to be provided by the BioSP without cost to the SI.
38	**Other Business Services** Migrate registration pilot data (approximately one million records including demographic and biometric data) Is this data already available or is this the one the SI captures during the Pilot project. If already developed, PSA to provide complete details about the data and the database structure	The pilot registration data is available. The data structure and its storage follows that of the MOSIP data structure and data store specifications.

39	**Other Business Services** Publish and maintain mobile application(s) on the mobile app store(s). PSA to register in the Mobile app store(s) and pay for any charges incurred. SI shall take responsibility to publish and maintain the mobile app on the mobile app store. Kindly confirm	SI to shoulder any charges in publishing to a mobile app store. Please refer to section 6.1.1.3 PhilSys Mobile Application (PMA), page 46 of SI Bidding Documents Volume II.
40	**Primary Data Center, Secondary Data Center, Disaster Recovery Site** The SI shall be required to take over the sites for hosting IT infrastructure PSA to kindly confirm whose scope of work shall be laying of cables for LAN	The setting up of LAN for all SI-provided hardware will be done by the SI.
41	**Information Security** The SI shall be responsible for ensuring information security Does PSA recommend any Guidelines for security processes and procedures?	The SI shall recommend and implement Information Security best practices. SI must submit preliminary recommendations on Information Security for PhilSys must be part of the technical proposal to be submitted as part of the bid evaluation.
42	**5.4 Exclusions** Site preparation for PFRCs (location, contracts, payments, and fit out) PSA to confirm whose scope shall be on supply of work stations/furnitures, laying cables for LAN, any civil works, etc. apart from the ones listed in the tender	PSA is responsible for the site preparation and any kinds of civil works for PFRCs.
43	**6.1.2.11 Post and Courier Services** Courier Cost PSA to confirm who bears the courier cost for distribution of PhilID Cards and PhilSys Numbers to PhilSys Fixed Registration Centers	PSA to shoulder the courier cost for distribution of PhilID Cards and PhilSys Numbers to PhilSys Fixed Registration Centers.

44	**Call Center** PSA to confirm whose scope is to set up the Call Center. Space, Workstation, Manpower, etc. Kindly provide clarity.	Please refer to Section 7.4.4.1 Customer Relationship Management – (page 149 of the SI Bidding Documents Volume II).
45	This project requires lots of underlying components and sub-systems. Not one of your eligibility bidders have all the required expertise. Kindly define what are the services that can not be subcontracted. However, please allow subcontracting on non-core components like ICT equipment/ services, COTS SW integration and other manpower requirements for operation centers and help desks, etc.	Sub-contacting is not allowed.
46	The PSA has stated that the proposed solution must support the standard set by MOSIP. However, MOSIP limits the supported file system to the Gluster File System. Could the PSA open the requirement to support other file systems available in the market today? If PSA will not allow bidders to use other open source platform, it will restrict PSA to the following provisions: a. application development language that could be supported by PhilSys b. technology components which could be used to service the requirements of PSA c. portability and support for other application development languages and types of data that could be stored	The MOSIP documentation actually notes the file system as CEPH and not GlusterFS. The PSA is to maintain the recommendations of the MOSIP documentation.
47	How can PSA ensure the timelines of this project using an OPEN SOURCE platform with restrictive proven installations? We just want to highlight the huge risk which was also raised by many proponents during many meetings with PSA. To add to the risk, the delivery timeline stated by PSA is exceptionally tight. Can we therefore request PSA to allow an alternate proven Identity Management platform based on open standards to meet all the PSA's requirements and still deliver on time with minimal risks?	PSA maintains its position to use the MOSIP framework.
48	Can bidders submit proposals using an identity management platform based on any open standards? We feel that PSA and this project should benefit from other technology platforms and not limit itself with a single platform. This will also avoid any possible lock-in that will be detrimental to the government.	No. Non MOSIP proposals will not be entertained.

49	Is the winning bidder required to provide existing or ready APIs to interface with PSA Civil Registration and Vital Statistics (CRVS) solution as it is of top priority for the government to ensure successful and timely roll-out the National ID project	Yes. Interfacing to PSA Civil Registration System will be done via API.
50	Can PSA also include other payment portals?	The SI will provide a solution that will interface with payment portals.
51	On Queuing Solution: Will PSA require only the system or the infra as well?	PSA will require both the hardware and software for the queuing solution..
52	Please confirm our understanding that the personalization system is not part of the scope of work of the SI. This shall be provided by the card personalization system provider.	This is to confirm that the bundled personalization software and printer drivers of the personalization machines will be provided by BSP.
53	May we clarify on the definition of Relying Parties (RP)? What will be the connection of the Relying Parties (RP) going to the Data Center? Broadband (DSL), Leased Line (MPLS), 4G/LTE? What will be the Bandwidth of each Connectivity?	A Relying Party is a service dependent on authentication against PhilSys Registry in order to verify the identity of the registered person when accessing a service. Please refer to Section 1.7 (Stakeholders), page 7 of the SI Bidding Documents Volume 2 The SI must be responsible in proposing/ designing the bandwidth of the network connectivity between RPs and Data Center based on the Number of Authentication Request and Number of eKYC Request stated in Table 6 of 002 SI PBD Vol. 2 and at the same time, based on the size of an authentication packet and eKYC packet stated in Table 7 of 002 SI PBD Vol. 2.
54	Please confirm our understanding that the 250 Philsys Fixed Registration Centers is where the Registrations Kits will be deployed. Will there be a dedicated Server Room per Fixed Registration Center? Does the Server Room in each Fixed Registration Center have enough Rack, Power and Cooling? How many Internet Connections are required per Fixed Registration Center? What is the Connectivity available from the Fixed Registration Center to each Data Center? What is the Internet Bandwidth Required?	This is to confirm that the Registration Kits will be deployed to the 250 PFRCs. There is no dedicated server room per PFRC. SI shall design the network connectivity from PFRC to Data Center (See Section 9.3 Setting up of Fixed Registration Centers in the PBD Volume II)

55	On Access Points: What is the use case of the Access Point? Is there a requirement for Indoor and Outdoor Access Point? How many Users that will connect to the Access Point per Fixed Registration Center? In terms of deployment of the Access Point, may we please request floor plan for proper sizing and heat map?	The use for the Access Points would focus on providing connectivity to wireless devices such as registration kits and other wifi enabled devices necessary in the operations of the registration center. Access points will be for indoor use by the registration clients to connect to the data center.
56	On Mobile Registration Center: Is Mobile Registration Device and Mobile Registration Center the same? Is Mobile Registration Device referring to a kiosk? Is the setup here will be same as PFRD - registration kits will also be deployed here? Will there be an IT infrastructure required here such as Router, Firewall, Switch, Access Points? Will there be a dedicated Server Room per Mobile Registration Center? Does the Server Room in each Mobile Registration Center have enough Rack, Power and Cooling? How will the connectivity of the Mobile Registration Device to the Data Center? How many Internet connections Required? What is the Internet Bandwidth Required?	Mobile registration centers are temporary locations where registration will take place. The mobile registration device pertains to the registration kits. Registration kits will be deployed to Mobile registration centers, where the registration kits can be used in an offline manner (when there is no internet connectivity in the area). The registration kits can be connected to the PhilSys backend (if internet connectivity is available in the area) by means of a dedicated mobile internet device that is to be provided by PSA.
57	On Document Management System: Will there be any legal or compliance requirements on document retention and purging policy on different types of documents? If so, how many numbers of record administrators will administer these policies?	The PhilSys is still in the process of identifying the retention period for documents that are in line with document retention policies of the National Archives. The SI, however, is expected to provide a feature for PhilSys Administrators to define this parameter in the Document Management System.
58	On Warranty: When will the Warranty start? When will the Maintenance Agreement start?	Warranty will start after acceptance of the specific deliverables. On maintenance agreement: Please refer to Section VIII (Appendices) starting on page 131 of the Bidding Docs Volume I

59	**Servers** On Servers a. Will you require the server components to have the capability for rapid OS recovery? b. Will you require the server components to have a “System Lockdown” feature? c. Will you require the server components to have a Unified Management Console? d. Will you require the server components to have the feature of OpenManage Mobile? e. Will you require the server components to have the feature for Support Assist Integration?	PSA will not be requiring the mentioned features. The SI is free to propose such features.
60	**Network** On Network a. Can PSA provide a Distributed Software Defined Network (SDN) in PSA Spine and Leaf Data Center Deployment?	PSA maintains its position that it is up to the SI to propose a MOSIP centric solution and for the SI to maintain its KPIs and SLAs.
61	**Storage** On Storage a. Based on the requirements detailed in section 9.6.7.2 Disaster Recovery Strategy and Procedures and 8.4.3 Capacity, Performance, and Scalability, Will you require that the storage system have a design for an active-active storage architecture? b. Based on the requirements detailed in section 8.4.3 Capacity, Performance, and Scalability, will you require the storage system to have the ability to support scale-up and scale-out approach when expanding capacity and performance? c. Based on the requirements detailed in section 9.8.6.3 Storage Management, will you require the storage system to have an Application Programming Interface (API) feature? d. 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? e. Based on the requirements detailed in section 9.6.7.2 Disaster Recovery Strategy and Procedures, will you require the storage system to have the capability to protect critical data from logical corruption? f. Based on the requirements detailed in section	PSA maintains its position that it is up to the SI to propose a MOSIP centric solution and for the SI to maintain its KPIs and SLAs.

	9.6.1 Data Center Strategy of Project, will you require the storage system to have the capability of dynamically supporting synchronous and asynchronous replication? g. Based on the requirements detailed in section 9.6.1 Data Center Strategy of Project, will you require the storage system to have support for Fan-In and Fan-Out replication strategies? h. Based on the requirements detailed in section 9.6.6 Recovery Time Objective (RTO) and Recovery Point Objective (RPO), will you require the storage system to have a phone-home feature for support and technical incidents? i. Will you require the storage system to have the capability to support multiple protocols on the same system? j. Based on the requirements detailed in section 9.8.4.8 Storage Monitoring and Management, will you require the storage system to have a cloud-based management portal? k. How will the PSA manage the identity records of citizens that have been declared deceased? Will we maintain the identity records and the associated transaction files of each citizen regardless of whether they are deceased or alive? In what manner must we store the identity records when it is not pulled out for a long time? How do we dispose of data which has been qualified for deletion? l. How will PSA require the system to handle the information and documents identity records found to be duplicates of an existing valid record? Does the PSA want to keep these identity records which were found to be irregular for purposes of re-vetting or litigation? What process should be followed in the disposal process of these falsified or duplication identity records? m. Will the PSA require separate systems or infrastructure to be built for each agency or 3rd party organization which will be allowed to connect to the PhilSys Platform?Will agencies or organizations with their existing identity records of a segment of the Philippine population be enabled by the PSA to stream identity information? If yes, how will this be done? If 3rd parties will be allowed to access the identity records in PSA, who will be responsible for securing these connections?	

	n. Is PSA amenable to using Traditional Storage (Enterprise Class Storage - SAN, NAS, etc)?	
62	On Backup and Recovery a. Based on the requirements detailed in section 9.6.7.2 Disaster Recover Strategy and Procedures and 9.8.6.6.5 Recovery and Restore, will you require the backup and recovery solution to include a backup to disk platform? b. Based on the requirements detailed in section 9.8.6.6 Backup and Restore System, will you require the backup and recovery solution to have the ability to deliver a high level of data efficiency when storing backup data? c. Based on the requirements detailed in section 9.8.6.6.5 Recovery and Restore, will you require the backup and recovery solution to support the capability to perform long term retention by shipping the backup data sets to an object storage platform? d. Based on the requirements detailed in section 9.8.6.6.1 Backup, will you require the backup and recovery solution to have the capability to perform backups of virtual machine (VM) server without the need for agents to be installed directly unto each VM server? e. Based on the requirements detailed in section 9.6.6 Recovery Time Objective (RTO) and Recovery Point Objective (RPO), will you require the backup and recovery solution to have the feature that will enable searching of a specific backup data set across the entire archive? f. Based on the requirements detailed in section 9.8.6.6.4 Automation Support, will you require the backup and recovery solution to have an Application Programming Interface (API) feature? g. Based on the requirements detailed in section 9.6.6 Recovery Time Objective (RTO) and Recovery Point Objective (RPO), will you require the backup and recovery solution to have a phone-home feature for support and technical incidents? h. Can we propose disk storage and not VTL or can we propose alternative solution other than tape? i. Do they require that the backup be replicated on the DR? j. Are there workloads that are running on all 3 site that need to be backup? k. What will be the required retention?	

	l. Please expound on the Backup policy adherence / violations from the Vol.2 Page 179 m. Please also confirm that the Replication and SAN solution should be from same OEM of per Vol.2 Page 179	
63	On Security a. Will you consider following components to the Phase 3 project to ensure governance, risk management, and compliance requirements are met? i. Based on the requirement detailed in section 9.7 Information Security, within table 53. Overview of Security Tools on item/level “F2” Will PSA be open to use MFA (Multi-Factor Authentication) instead of 2FA, and the capability to do Risk analytics / assessment on every authentication? b. Who will be considered users for authentication? PSA employees / internal users? External users (registering demographic)? c. On Identity and Access Management (IAMS): On item “d” – are you looking at challenging users with 2FA for all these local systems? d. On item “e” – Please confirm whether it is XAML or SAML? May you also elaborate further on item “f”? Are you referring to the user entitlements within PSA (as an Org) or just the access of a user to resources? e. On Public Key Infrastructure (PKI): DICT has PKI infrastructure. If DICT will mandate to use it, can it be a source of PKI? f. On Governance, risk management, and compliance (GRC): What is their primary use case why is there a need for a GRC platform? Are there any existing processes that needs to be migrated and automated? What is the objective of using GRC? Does PSA already have Policy or SI will provide? g. On HSM: What encryption algorithm and key size will be used? (RSA? 2048 bit?) Are all keys shared/replicated between Primary DC, Secondary DC and DR HSMs? Or each location has separate keys? Are backups required for	PSA maintains its position that it is up to the SI to propose a MOSIP centric solution and for the SI to maintain its KPIs and SLAs.

	only Primary DC HSM? Or does each location's HSM require backup? How about test/staging? Is multi-factor authentication into the HSM required? h. On Database Audit Manager: How many data centers will be protected? Will a disaster recovery site be protected? i. On Attack Surface Reduction (ASR): Please expound if this is a Service or a Function?	
64	Technical Help Desk a. Volume 2.5, Section 9.8.5 Technical Helpdesk, page 237 states that, "The PSA shall provide physical space for the Technical Helpdesk along with necessary Electrical and Physical Infrastructure…" It is also stated in Section 7.4.4.5 Key Features of the Proposed Call Center, page 152. Please confirm our understanding that SI will only provide the technical helpdesk system and its manpower requirement. b. Do we need to provide toll free number for Technical Help Desk, is there specific number required? c. Do we have available call flow for the Technical Help Desk? d. Do we have floor plan and dimensions for the facility that will be provided for the National Call Center? e. Can we locate the Technical Help Desk together with the NOC/SOC? f. What specific remote support is needed to be performed by the Help Desk? Phone support only or need to remote desktop support as well? g. Do we have recommended Internet bandwidth that needs to be provisioned for Technical Help Desk?	Please refer to Section 9.8.5
65	NOC/SOC a. Can we put the NOC and SOC in the same facility? This it to provide ease of collaboration between the network and security teams b. Can we have the dimensions for the NOC? c. Can we have the dimensions for the SOC? d. What collaborations tools are needed for the NOC? SOC? e. Do we have recommended Internet bandwidth that needs to be provisioned for the NOC? SOC?	a. Yes, the SOC and NOC can be placed in the same facility b. c. It is expected that the SI can best define the dimensions of the SOC and NOC based on their experiences. d. The SI is expected to propose collaboration tools for the SOC and NOC. e. SI is responsible for designing the network

		connectivity that includes the Internet bandwidth. The end-to-end connectivity must always be available and reliable (see Section 9.8.6.15 Network Operations Center letter 'e')