PHILIPPINE BIDDING DOCUMENTS

SUPPLY, INSTALLATION, SUPPORT AND MAINTENANCE OF AUTOMATED BIOMETRIC IDENTIFICATION SYSTEMS (ABIS) FOR PHILIPPINE IDENTIFICATION SYSTEM (PHILSYS)

Government of the Republic of the Philippines

PHILIPPINE STATISTICS AUTHORITY
Quezon City, Philippines

PUBLIC BIDDING NO. 2019-08

October 2019

Fifth Edition
October 2016

TABLE OF CONTENTS

Section I. Invitation to Bid

INVITATION TO BID FOR SUPPLY, INSTALLATION, SUPPORT AND MAINTENANCE OF AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS) FOR PHILIPPINE IDENTIFICATION SYSTEM (PHILSYS)

1. The **Philippine Statistics Authority (PSA)**, through the **General Appropriations Act (GAA) 2019** intends to apply the sum of **One Billion Seven Hundred Million Pesos (PhP1,700,000,000.00)**, being the Approved Budget for the Contract (ABC) to payments to the above-named contract. Bids received in excess of the ABC shall be automatically rejected at bid opening.

2. The Philippine Statistics Authority (PSA) now invites bids for the **Supply, installation, support and maintenance of Automated Biometric Identification System (ABIS) for Philippine Identification System (PhilSys).** Delivery of the Goods is required **within ninety (90) calendar days upon receipt of Notice to Proceed.** Bidders should have completed, **within ten (10) years** from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II. Instructions to Bidders.

3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary "pass/fail" criterion as specified in the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (RA) 9184, otherwise known as the "Government Procurement Reform Act".

   Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA 5183.

4. Interested bidders may obtain further information from **Philippine Statistics Authority (PSA)** and inspect the Bidding Documents at the address given below during working hours.

   PSA BAC Secretariat
   11th Floor, Cyberpod Centris One, Eton Centris
   EDSA corner Quezon Avenue, Quezon City

5. A complete set of Bidding Documents may be acquired by interested Bidders starting **07 October 2019** from the address below and upon payment of the applicable fee for Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the amount of **Seventy-Five Thousand Philippine Peso (PhP75,000.00).** The Bidding Documents shall be received personally by the prospective bidder or his duly authorized representative upon presentation of proper identification documents.

It may also be downloaded free of charge from the website of the Philippine Government Electronic Procurement System (PhilGEPS) and the website of the Procuring Entity, provided that Bidders shall pay the applicable fee for the Bidding Documents not later than the submission of their bids.

6. The PSA-BAC will hold a **Pre-Bid Conference** on **15 October 2019, 1:30 P.M.** at **17th Floor, Cyberpod Centris Three, Eton Centris, EDSA corner Quezon Avenue, Quezon City**, which shall be open to prospective bidders.

7. Bids must be duly received by the BAC Secretariat at the address below on or before **29 October 2019, on or before 1:30 PM.** All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in **ITB** Clause 18.

   Bid opening shall be on **29 October 2019, 2:00 P.M.** at **17th Floor, Cyberpod Centris Three, Eton Centris, EDSA corner Quezon Avenue, Quezon City**. Bids will be opened in the presence of the bidders' representatives who choose to attend at the address below. Late bids shall not be accepted.

8. The PSA reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Section 41 of RA 9184 and its IRR, without thereby incurring any liability to the affected bidder or bidders.

9. For further information, please refer to:

   Atty. Revelyn C. Cayetano-Abduhalim
   Head, BAC Secretariat
   PSA Bids and Awards Committee
   11th Floor, Cyberpod Centris One, Eton Centris
   EDSA corner Quezon Avenue, Quezon City
   Tel. No. : (02) 374-8281
   Email : r.abduhalim@psa.gov.ph
   Web : **www.psa.gov.ph** or https://procurement.psa.gov.ph/

(SGD)
CANDIDO J. ASTROLOGO JR.
OIC-Deputy National Statistician, CTCO
Chairperson, PSA Bids and Awards Committee

Section II. Instructions to Bidders

TABLE OF CONTENTS

A. General

1. Scope of Bid

i. The Procuring Entity named in the **BDS** invites bids for the supply and delivery of the Goods as described in Section VII. Technical Specifications.

ii. The name, identification, and number of lots specific to this bidding are provided in the **BDS**. The contracting strategy and basis of evaluation of lots is described in **ITB** Clause 28.

2. Source of Funds

The Procuring Entity has a budget or has received funds from the Funding Source named in the **BDS**, and in the amount indicated in the **BDS**. It intends to apply part of the funds received for the Project, as defined in the **BDS**, to cover eligible payments under the contract.

3. Corrupt, Fraudulent, Collusive, and Coercive Practices

i. Unless otherwise specified in the **BDS**, the Procuring Entity as well as the bidders and suppliers shall observe the highest standard of ethics during the procurement and execution of the contract. In pursuance of this policy, the Procuring Entity:

(a) defines, for purposes of this provision, the terms set forth below as follows:

(i) "corrupt practice" means behavior on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves, others, or induce others to do so, by misusing the position in which they are placed, and includes the offering, giving, receiving, or soliciting of anything of value to influence the action of any such official in the procurement process or in contract execution; entering, on behalf of the government, into any contract or transaction manifestly and grossly disadvantageous to the same, whether or not the public officer profited or will profit thereby, and similar acts as provided in RA 3019.

(ii) "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Procuring Entity, and includes collusive practices among Bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the Procuring Entity of the benefits of free and open competition.

(iii) "collusive practices" means a scheme or arrangement between two or more Bidders, with or without the knowledge of the Procuring Entity, designed to establish bid prices at artificial, non-competitive levels.

(iv) "coercive practices" means harming or threatening to harm, directly or indirectly, persons, or their property to influence their participation in a procurement process, or affect the execution of a contract;

(v) "obstructive practice" is

(aa) deliberately destroying, falsifying, altering or concealing of evidence material to an administrative proceedings or investigation or making false statements to investigators in order to materially impede an administrative proceedings or investigation of the Procuring Entity or any foreign government/foreign or international financing institution into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the administrative proceedings or investigation or from pursuing such proceedings or investigation; or

(bb) acts intended to materially impede the exercise of the inspection and audit rights of the Procuring Entity or any foreign government/foreign or international financing institution herein.

(b) will reject a proposal for award if it determines that the Bidder recommended for award has engaged in any of the practices mentioned in this Clause for purposes of competing for the contract.

ii. Further, the Procuring Entity will seek to impose the maximum civil, administrative, and/or criminal penalties available under applicable laws on individuals and organizations deemed to be involved in any of the practices mentioned in **ITB** Clause i(a).

iii. Furthermore, the Funding Source and the Procuring Entity reserve the right to inspect and audit records and accounts of a bidder or supplier in the bidding for and performance of a contract themselves or through independent auditors as reflected in the **GCC** Clause3.

4. Conflict of Interest

i. All Bidders found to have conflicting interests shall be disqualified to participate in the procurement at hand, without prejudice to the imposition of appropriate administrative, civil, and criminal sanctions. A Bidder may be considered to have conflicting interests with another

Bidder in any of the events described in paragraphs (a) through (c) below and a general conflict of interest in any of the circumstances set out in paragraphs (d) through (g) below:

(a) A Bidder has controlling shareholders in common with another Bidder;

(b) A Bidder receives or has received any direct or indirect subsidy from any other Bidder;

(c) A Bidder has the same legal representative as that of another Bidder for purposes of this bid;

(d) A Bidder has a relationship, directly or through third parties, that puts them in a position to have access to information about or influence on the bid of another Bidder or influence the decisions of the Procuring Entity regarding this bidding process;

(e) A Bidder submits more than one bid in this bidding process. However, this does not limit the participation of subcontractors in more than one bid;

(f) A Bidder who participated as a consultant in the preparation of the design or technical specifications of the Goods and related services that are the subject of the bid; or

(g) A Bidder who lends, or temporarily seconds, its personnel to firms or organizations which are engaged in consulting services for the preparation related to procurement for or implementation of the project, if the personnel would be involved in any capacity on the same project.

ii. In accordance with Section 47 of the IRR of RA 9184, all Bidding Documents shall be accompanied by a sworn affidavit of the Bidder that it is not related to the Head of the Procuring Entity (HoPE), members of the Bids and Awards Committee (BAC), members of the Technical Working Group (TWG), members of the BAC Secretariat, the head of the Project Management Office (PMO) or the end-user unit, and the project consultants, by consanguinity or affinity up to the third civil degree. On the part of the Bidder, this Clause shall apply to the following persons:

(a) If the Bidder is an individual or a sole proprietorship, to the Bidder himself;

(b) If the Bidder is a partnership, to all its officers and members;

(c) If the Bidder is a corporation, to all its officers, directors, and controlling stockholders;

(d) If the Bidder is a cooperative, to all its officers, directors, and controlling shareholders or members; and

(e) If the Bidder is a joint venture (JV), the provisions of items (a), (b), (c), or (d) of this Clause shall correspondingly apply to each of the members of the said JV, as may be appropriate.

Relationship of the nature described above or failure to comply with this Clause will result in the automatic disqualification of a Bidder.

5. Eligible Bidders

i. Unless otherwise provided in the **BDS**, the following persons shall be eligible to participate in this bidding:

(a) Duly licensed Filipino citizens/sole proprietorships;

(b) Partnerships duly organized under the laws of the Philippines and of which at least sixty percent (60%) of the interest belongs to citizens of the Philippines;

(c) Corporations duly organized under the laws of the Philippines, and of which at least sixty percent (60%) of the outstanding capital stock belongs to citizens of the Philippines;

(d) Cooperatives duly organized under the laws of the Philippines; and

(e) Persons/entities forming themselves into a Joint Venture (JV), *i.e.*, a group of two (2) or more persons/entities that intend to be jointly and severally responsible or liable for a particular contract: Provided, however, that Filipino ownership or interest of the JV concerned shall be at least sixty percent(60%).

ii. Foreign bidders may be eligible to participate when any of the following circumstances exist, as specified in the **BDS**:

(a) When a Treaty or International or Executive Agreement as provided in Section 4 of RA 9184 and its IRR allow foreign bidders to participate;

(b) Citizens, corporations, or associations of a country, the laws or regulations of which grant reciprocal rights or privileges to citizens, corporations, or associations of the Philippines;

(c) When the Goods sought to be procured are not available from local suppliers; or

(d) When there is a need to prevent situations that defeat competition or restrain trade.

iii. Government owned or –controlled corporations (GOCCs) may be eligible to participate only if they can establish that they (a) are legally and financially autonomous, (b) operate under commercial law, and (c) are not attached agencies of the Procuring Entity.

iv. Unless otherwise provided in the **BDS**, the Bidder must have completed a Single Largest Completed Contract (SLCC)similar to the Project and the value of which, adjusted, if necessary, by the Bidder to current prices using the Philippine Statistics Authority (PSA)consumer price index, must be at least equivalent to a percentage of the ABC stated in the **BDS**.

For this purpose, contracts similar to the Project shall be those described in the **BDS**, and completed within the relevant period stated in the Invitation to Bid and **ITB** Clause 12.1(a)(ii).

v. The Bidder must submit a computation of its Net Financial Contracting Capacity (NFCC), which must be at least equal to the ABC to be bid, calculated as follows:

NFCC = [(Current assets minus current liabilities) (15)] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started, coinciding with the contract to be bid.

The values of the domestic bidder's current assets and current liabilities shall be based on the latest Audited Financial Statements submitted to the BIR.

For purposes of computing the foreign bidders' NFCC, the value of the current assets and current liabilities shall be based on their audited financial statements prepared in accordance with international financial reporting standards.

If the prospective bidder opts to submit a committed Line of Credit, it must be at least equal to ten percent (10%) of the ABC to be bid. If issued by a foreign universal or commercial bank, it shall be confirmed or authenticated by a local universal or commercial bank.

6. Bidder's Responsibilities

i. The Bidder or its duly authorized representative shall submit a sworn statement in the form prescribed in Section VIII. Bidding Forms as required in **ITB** Clause 12.i(b)(iii).

ii. The Bidder is responsible for the following:

(a) Having taken steps to carefully examine all of the Bidding Documents;

(b) Having acknowledged all conditions, local or otherwise, affecting the implementation of the contract;

(c) Having made an estimate of the facilities available and needed for the contract to be bid, if any;

(d) Having complied with its responsibility to inquire or secure Supplemental/Bid Bulletin(s) as provided under **ITB** Clause 10.iv.

(e) Ensuring that it is not “blacklisted” or barred from bidding by the GOP or any of its agencies, offices, corporations, or LGUs, including foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the GPPB;

(f) Ensuring that each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

(g) Authorizing the HoPE or its duly authorized representative/s to verify all the documents submitted;

(h) Ensuring that the signatory is the duly authorized representative of the Bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the Bidder in the bidding, with the duly notarized Secretary’s Certificate attesting to such fact, if the Bidder is a corporation, partnership, cooperative, or joint venture;

(i) Complying with the disclosure provision under Section 47 of RA 9184 and its IRR in relation to other provisions of RA 3019;

(j) Complying with existing labor laws and standards, in the case of procurement of services; Moreover, bidder undertakes to:

> (i) Ensure the entitlement of workers to wages, hours of work, safety and health and other prevailing conditions of work as established by national laws, rules and regulations; or collective bargaining agreement; or arbitration award, if and when applicable.
>
> In case there is a finding by the Procuring Entity or the DOLE of underpayment or non-payment of workers’ wage and wage-related benefits, bidder agrees that the performance security or portion of the contract amount shall be withheld in favor of the complaining workers pursuant to appropriate provisions of Republic Act No. 9184 without prejudice to the institution of appropriate actions under the Labor Code, as amended, and other social legislations.
>
> (ii) Comply with occupational safety and health standards and to correct deficiencies, if any.
>
> In case of imminent danger, injury or death of the worker, bidder undertakes to suspend contract implementation pending

clearance to proceed from the DOLE Regional Office and to comply with Work Stoppage Order; and

(iii) Inform the workers of their conditions of work, labor clauses under the contract specifying wages, hours of work and other benefits under prevailing national laws, rules and regulations; or collective bargaining agreement; or arbitration award, if and when applicable, through posting in two (2) conspicuous places in the establishment’s premises; and

(k) Ensuring that it did not give or pay, directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

Failure to observe any of the above responsibilities shall be at the risk of the Bidder concerned.

iii. The Bidder is expected to examine all instructions, forms, terms, and specifications in the Bidding Documents.

iv. It shall be the sole responsibility of the Bidder to determine and to satisfy itself by such means as it considers necessary or desirable as to all matters pertaining to the contract to be bid, including: (a) the location and the nature of this Project; (b) climatic conditions; (c) transportation facilities; and (d) other factors that may affect the cost, duration, and execution or implementation of this Project.

v. The Procuring Entity shall not assume any responsibility regarding erroneous interpretations or conclusions by the prospective or eligible bidder out of the data furnished by the procuring entity. However, the Procuring Entity shall ensure that all information in the Bidding Documents, including bid/supplemental bid bulletin/s issued, are correct and consistent.

vi. Before submitting their bids, the Bidder is deemed to have become familiar with all existing laws, decrees, ordinances, acts and regulations of the Philippines which may affect this Project in any way.

vii. The Bidder shall bear all costs associated with the preparation and submission of his bid, and the Procuring Entity will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

viii. The Bidder should note that the Procuring Entity will accept bids only from those that have paid the applicable fee for the Bidding Documents at the office indicated in the Invitation to Bid.

7. Origin of Goods

Unless otherwise indicated in the **BDS**, there is no restriction on the origin of goods other than those prohibited by a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, subject to **ITB** Clause 27.i.

8. Subcontracts

i. Unless otherwise specified in the **BDS**, the Bidder may subcontract portions of the Goods to an extent as may be approved by the Procuring Entity and stated in the **BDS**. However, subcontracting of any portion shall not relieve the Bidder from any liability or obligation that may arise from the contract for this Project.

ii. Subcontractors must submit the documentary requirements under **ITB** Clause 12 and comply with the eligibility criteria specified in the **BDS.** In the event that any subcontractor is found by the Procuring Entity to be ineligible, the subcontracting of such portion of the Goods shall be disallowed.

iii. The Bidder may identify the subcontractor to whom a portion of the Goods will be subcontracted at any stage of the bidding process or during contract implementation. If the Bidder opts to disclose the name of the subcontractor during bid submission, the Bidder shall include the required documents as part of the technical component of its bid.

B. Contents of Bidding Documents

9. Pre-Bid Conference

i. (a) If so specified in the **BDS**, a pre-bid conference shall be held at the venue and on the date indicated therein, to clarify and address the Bidders' questions on the technical and financial components of this Project.

(b) The pre-bid conference shall be held at least twelve (12) calendar days before the deadline for the submission and receipt of bids, but not earlier than seven (7) calendar days from the posting of the invitation to bid/bidding documents in the PhilGEPS website. If the Procuring Entity determines that, by reason of the method, nature, or complexity of the contract to be bid, or when international participation will be more advantageous to the GOP, a longer period for the preparation of bids is necessary, the pre-bid conference shall be held at least thirty (30) calendar days before the deadline for the submission and receipt of bids, as specified in the **BDS**.

ii. Bidders are encouraged to attend the pre-bid conference to ensure that they fully understand the Procuring Entity's requirements. Non-attendance of the Bidder will in no way prejudice its bid; however, the Bidder is expected to know the changes and/or amendments to the

Bidding Documents as recorded in the minutes of the pre-bid conference and the Supplemental/Bid Bulletin. The minutes of the pre-bid conference shall be recorded and prepared not later than five (5) calendar days after the pre-bid conference. The minutes shall be made available to prospective bidders not later than five (5) days upon written request.

9.3 Decisions of the BAC amending any provision of the bidding documents shall be issued in writing through a Supplemental/Bid Bulletin at least seven (7) calendar days before the deadline for the submission and receipt of bids.

10. Clarification and Amendment of Bidding Documents

i. Prospective bidders may request for clarification on and/or interpretation of any part of the Bidding Documents. Such request must be in writing and submitted to the Procuring Entity at the address indicated in the **BDS** at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

ii. The BAC shall respond to the said request by issuing a Supplemental/Bid Bulletin, to be made available to all those who have properly secured the Bidding Documents, at least seven (7) calendar days before the deadline for the submission and receipt of Bids.

iii. Supplemental/Bid Bulletins may also be issued upon the Procuring Entity's initiative for purposes of clarifying or modifying any provision of the Bidding Documents not later than seven (7) calendar days before the deadline for the submission and receipt of Bids. Any modification to the Bidding Documents shall be identified as an amendment.

iv. Any Supplemental/Bid Bulletin issued by the BAC shall also be posted in the PhilGEPS and the website of the Procuring Entity concerned, if available, and at any conspicuous place in the premises of the Procuring Entity concerned. It shall be the responsibility of all Bidders who have properly secured the Bidding Documents to inquire and secure Supplemental/Bid Bulletins that may be issued by the BAC. However, Bidders who have submitted bids before the issuance of the Supplemental/Bid Bulletin must be informed and allowed to modify or withdraw their bids in accordance with **ITB** Clause 23.

C. Preparation of Bids

11. Language of Bids

The eligibility requirements or statements, the bids, and all other documents to be submitted to the BAC must be in English. If the eligibility requirements or statements, the bids, and all other documents submitted to the BAC are in foreign language other than English, it must be accompanied by a translation of the documents in English. The documents shall be translated by the relevant foreign government agency, the foreign government agency authorized to translate documents, or a registered translator in the foreign bidder’s country; and shall be authenticated by the appropriate Philippine foreign service establishment/post or the equivalent office having jurisdiction over the foreign bidder’s affairs in the Philippines. The English translation shall govern, for purposes of interpretation of the bid.

12. Documents Comprising the Bid: Eligibility and Technical Components

i. Unless otherwise indicated in the **BDS**, the first envelope shall contain the following eligibility and technical documents:

(a) Eligibility Documents –

Class “A” Documents:

(i) PhilGEPS Certificate of Registration and Membership in accordance with Section 8.5.2 of the IRR. For procurement to be performed overseas, it shall be subject to the Guidelines to be issued by the GPPB.

(ii) Statement of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid; and

Statement of the Bidder’s SLCC similar to the contract to be bid, in accordance with ITB Clause 5.4, within the relevant period as provided in the **BDS.**

The two statements required shall indicate for each contract the following:

(ii.1) name of the contract;

(ii.2) date of the contract;

(ii.3) contract duration;

(ii.4) owner’s name and address;

(ii.5) kinds of Goods;

(ii.6) For Statement of Ongoing Contracts - amount of contract and value of outstanding contracts;

(ii.7) For Statement of SLCC - amount of completed contracts, adjusted by the Bidder to current prices using PSA’s consumer price index, if necessary for the purpose of meeting the SLCC requirement;

(ii.8) date of delivery; and

(ii.9) end user's acceptance or official receipt(s) or sales invoice issued for the contract, if completed, which shall be attached to the statements.

(iii) NFCC computation in accordance with ITB Clause 5.5 or a committed Line of Credit from a universal or commercial bank.

<u>Class "B" Document</u>:

(iv) If applicable, the Joint Venture Agreement (JVA) in case the joint venture is already in existence, or duly notarized statements from all the potential joint venture partners in accordance with Section 23.1(b) of the IRR.

(b) Technical Documents –

(i) Bid security in accordance with **ITB** Clause 18. If the Bidder opts to submit the bid security in the form of:

(i.1) a bank draft/guarantee or an irrevocable letter of credit issued by a foreign bank, it shall be accompanied by a confirmation from a Universal or Commercial Bank; or

(i.2) a surety bond, it shall be accompanied by a certification by the Insurance Commission that the surety or insurance company is authorized to issue such instruments;

(ii) Conformity with technical specifications, as enumerated and specified in Sections VI and VII of the Bidding Documents; and

(iii) Sworn statement in accordance with Section 25.3 of the IRR of RA 9184 and using the form prescribed in Section VIII. Bidding Forms.

(iv) For foreign bidders claiming eligibility by reason of their country's extension of reciprocal rights to Filipinos, a certification from the relevant government office of their country stating that Filipinos are allowed to participate in their government procurement activities for the same item or product.

13. Documents Comprising the Bid: Financial Component

i. The financial component of the bid shall contain the following:

(a) Financial Bid Form, which includes bid prices and the applicable Price Schedules, in accordance with **ITB** Clauses 15.i and 15.iv;

(b) If the Bidder claims preference as a Domestic Bidder, a certification from the DTI issued in accordance with **ITB** Clause 27, unless otherwise provided in the **BDS**; and

(c) Any other document related to the financial component of the bid as stated in the **BDS**.

ii. (a) Unless otherwise stated in the **BDS,** all bids that exceed the ABC shall not be accepted.

(b) Unless otherwise indicated in the **BDS**, for foreign-funded procurement, a ceiling may be applied to bid prices provided the following conditions are met:

(i) Bidding Documents are obtainable free of charge on a freely accessible website. If payment of Bidding Documents is required by the procuring entity, payment could be made upon the submission of bids.

(ii) The procuring entity has procedures in place to ensure that the ABC is based on recent estimates made by the responsible unit of the procuring entity and that the estimates reflect the quality, supervision and risk and inflationary factors, as well as prevailing market prices, associated with the types of works or goods to be procured.

(iii) The procuring entity has trained cost estimators on estimating prices and analyzing bid variances.

(iv) The procuring entity has established a system to monitor and report bid prices relative to ABC and engineer's/procuring entity's estimate.

(v) The procuring entity has established a monitoring and evaluation system for contract implementation to provide a feedback on actual total costs of goods and works.

14. Alternative Bids

14.1 Alternative Bids shall be rejected. For this purpose, alternative bid is an offer made by a Bidder in addition or as a substitute to its original bid which may be included as part of its original bid or submitted separately therewith for purposes of bidding. A bid with options is considered an alternative bid regardless of whether said bid proposal is contained in a single envelope or submitted in two (2) or more separate bid envelopes.

14.2 Each Bidder shall submit only one Bid, either individually or as a partner in a JV. A Bidder who submits or participates in more than one bid (other than as a subcontractor if a subcontractor is permitted to participate in more than one bid) will cause all the proposals with the Bidder's participation to be disqualified. This shall be without prejudice to any applicable criminal, civil and administrative penalties that may be imposed upon the persons and entities concerned.

15. Bid Prices

i. The Bidder shall complete the appropriate Schedule of Prices included herein, stating the unit prices, total price per item, the total amount and the expected countries of origin of the Goods to be supplied under this Project.

ii. The Bidder shall fill in rates and prices for all items of the Goods described in the Schedule of Prices. Bids not addressing or providing all of the required items in the Bidding Documents including, where applicable, Schedule of Prices, shall be considered non-responsive and, thus, automatically disqualified. In this regard, where a required item is provided, but no price is indicated, the same shall be considered as non-responsive, but specifying a zero (0)or a dash (-) for the said item would mean that it is being offered for free to the Government, except those required by law or regulations to be accomplished.

iii. The terms Ex Works (EXW), Cost, Insurance and Freight (CIF), Cost and Insurance Paid to (CIP), Delivered Duty Paid (DDP),and other trade terms used to describe the obligations of the parties, shall be governed by the rules prescribed in the current edition of the International Commercial Terms (INCOTERMS) published by the International Chamber of Commerce, Paris.

iv. Prices indicated on the Price Schedule shall be entered separately in the following manner:

(a) For Goods offered from within the Procuring Entity's country:

(i) The price of the Goods quoted EXW (ex works, ex factory, ex warehouse, ex showroom, or off-the-shelf, as applicable);

(ii) The cost of all customs duties and sales and other taxes already paid or payable;

(iii) The cost of transportation, insurance, and other costs incidental to delivery of the Goods to their final destination; and

(iv) The price of other (incidental) services, if any, listed in the **BDS**.

(b) For Goods offered from abroad:

(i) Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted DDP with the place of destination in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.

(ii) The price of other (incidental) services, if any, listed in the **BDS**.

(c) For Services, based on the form which may be prescribed by the Procuring Entity, in accordance with existing laws, rules and regulations

v. Prices quoted by the Bidder shall be fixed during the Bidder’s performance of the contract and not subject to variation or price escalation on any account. A bid submitted with an adjustable price quotation shall be treated as non-responsive and shall be rejected, pursuant to **ITB** Clause 24.

All bid prices for the given scope of work in the contract as awarded shall be considered as fixed prices, and therefore not subject to price escalation during contract implementation, except under extraordinary circumstances. Upon the recommendation of the Procuring Entity, price escalation may be allowed in extraordinary circumstances as may be determined by the National Economic and Development Authority in accordance with the Civil Code of the Philippines, and upon approval by the GPPB. Nevertheless, in cases where the cost of the awarded contract is affected by any applicable new laws, ordinances, regulations, or other acts of the GOP, promulgated after the date of bid opening, a contract price adjustment shall be made or appropriate relief shall be applied on a no loss-no gain basis.

16. Bid Currencies

i. Prices shall be quoted in the following currencies:

(a) For Goods that the Bidder will supply from within the Philippines, the prices shall be quoted in Philippine Pesos.

(b) For Goods that the Bidder will supply from outside the Philippines, the prices may be quoted in the currency(ies) stated in the **BDS**. However, for purposes of bid evaluation, bids denominated in foreign currencies shall be converted to Philippine currency based on the exchange rate as published in the *Bangko Sentral ng Pilipinas* (BSP) reference rate bulletin on the day of the bid opening.

ii. If so allowed in accordance with **ITB** Clause i, the Procuring Entity for purposes of bid evaluation and comparing the bid prices will convert the amounts in various currencies in which the bid price is expressed to Philippine Pesos at the foregoing exchange rates.

iii. Unless otherwise specified in the **BDS**, payment of the contract price shall be made in Philippine Pesos.

17. Bid Validity

i. Bids shall remain valid for the period specified in the **BDS** which shall not exceed one hundred twenty (120) calendar days from the date of the opening of bids.

ii. In exceptional circumstances, prior to the expiration of the bid validity period, the Procuring Entity may request Bidders to extend the period of validity of their bids. The request and the responses shall be made in writing. The bid security described in **ITB** Clause 18 should also be extended corresponding tothe extension of the bid validity period at the least. A Bidder may refuse the request without forfeiting its bid security, but his bid shall no longer be considered for further evaluation and award. A Bidder granting the request shall not be required or permitted to modify its bid.

18. Bid Security

i. The Bidder shall submit a Bid Securing Declaration or any form of Bid Security in the amount stated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the following schedule:

Form of Bid Security	Amount of Bid Security (Not Less than the Percentage of the ABC)
(a) Cash or cashier's/manager's check issued by a Universal or Commercial Bank. *For biddings conducted by LGUs, the Cashier's/Manager's Check may be issued by other banks certified by the BSP as authorized to issue such financial instrument.*	Two percent (2%)
(b) Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank. *For biddings conducted by LGUs, Bank Draft/Guarantee, or Irrevocable Letter of Credit may*	

be issued by other banks certified by the BSP as authorized to issue such financial instrument.	
(c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	Five percent (5%)

The Bid Securing Declaration mentioned above is an undertaking which states, among others, that the Bidder shall enter into contract with the procuring entity and furnish the performance security required under ITB Clause 33.2, within ten (10) calendar days from receipt of the Notice of Award, and commits to pay the corresponding amount as fine, and be suspended for a period of time from being qualified to participate in any government procurement activity in the event it violates any of the conditions stated therein as provided in the guidelines issued by the GPPB.

ii. The bid security should be valid for the period specified in the **BDS**. Any bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

iii. No bid securities shall be returned to Bidders after the opening of bids and before contract signing, except to those that failed or declared as post-disqualified, upon submission of a written waiver of their right to file a request for reconsideration and/or protest, or upon the lapse of the reglementary period to file a request for reconsideration or protest. Without prejudice on its forfeiture, bid securities shall be returned only after the Bidder with the Lowest Calculated Responsive Bid (LCRB) has signed the contract and furnished the performance security, but in no case later than the expiration of the bid security validity period indicated in **ITB** Clause ii.

iv. Upon signing and execution of the contract pursuant to **ITB** Clause 32, and the posting of the performance security pursuant to **ITB** Clause 33, the successful Bidder’s bid security will be discharged, but in no case later than the bid security validity period as indicated in the **ITB** Clause ii.

v. The bid security may be forfeited:

(a) if a Bidder:

(i) withdraws its bid during the period of bid validity specified in **ITB** Clause 17;

(ii) does not accept the correction of errors pursuant to **ITB** Clause 28.iii(b);

(iii) has a finding against the veracity of any of the documents submitted as stated in **ITB** Clause 29.2;

(iv) submission of eligibility requirements containing false information or falsified documents;

(v) submission of bids that contain false information or falsified documents, or the concealment of such information in the bids in order to influence the outcome of eligibility screening or any other stage of the public bidding;

(vi) allowing the use of one’s name, or using the name of another for purposes of public bidding;

(vii) withdrawal of a bid, or refusal to accept an award, or enter into contract with the Government without justifiable cause, after the Bidder had been adjudged as having submitted the LCRB;

(viii) refusal or failure to post the required performance security within the prescribed time;

(ix) refusal to clarify or validate in writing its bid during post-qualification within a period of seven (7) calendar days from receipt of the request for clarification;

(x) any documented attempt by a Bidder to unduly influence the outcome of the bidding in his favor;

(xi) failure of the potential joint venture partners to enter into the joint venture after the bid is declared successful; or

(xii) all other acts that tend to defeat the purpose of the competitive bidding, such as habitually withdrawing from bidding, submitting late Bids or patently insufficient bid, for at least three (3) times within a year, except for valid reasons.

(b) if the successful Bidder:

(i) fails to sign the contract in accordance with **ITB** Clause 32; or

(ii) fails to furnish performance security in accordance with **ITB** Clause 33.

19. Format and Signing of Bids

i. Bidders shall submit their bids through their duly authorized representative using the appropriate forms provided in Section VIII. Bidding Forms on or before the deadline specified in the **ITB** Clauses21 in two (2) separate sealed bid envelopes, and which shall be submitted simultaneously. The first shall contain the technical component of the bid, including the eligibility requirements under **ITB** Clause i, and the second shall contain the financial component of the bid. This shall also be observed for each lot in the case of lot procurement.

ii. Forms as mentioned in **ITB** Clause imust be completed without any alterations to their format, and no substitute form shall be accepted. All blank spaces shall be filled in with the information requested.

iii. The Bidder shall prepare and submit an original of the first and second envelopes as described in **ITB** Clauses 12 and13. In addition, the Bidder shall submit copies of the first and second envelopes. In the event of any discrepancy between the original and the copies, the original shall prevail.

iv. Each and every page of the Bid Form, including the Schedule of Prices, under Section VIII hereof, shall be signed by the duly authorized representative/s of the Bidder. Failure to do so shall be a ground for the rejection of the bid.

v. Any interlineations, erasures, or overwriting shall be valid only if they are signed or initialed by the duly authorized representative/s of the Bidder.

20. Sealing and Marking of Bids

i. Bidders shall enclose their original eligibility and technical documents described in **ITB** Clause 12 in one sealed envelope marked "ORIGINAL - TECHNICAL COMPONENT", and the original of their financial component in another sealed envelope marked "ORIGINAL - FINANCIAL COMPONENT", sealing them all in an outer envelope marked "ORIGINAL BID".

ii. Each copy of the first and second envelopes shall be similarly sealed duly marking the inner envelopes as "COPY NO. ___ - TECHNICAL COMPONENT" and "COPY NO. ___ – FINANCIAL COMPONENT" and the outer envelope as "COPY NO. ___", respectively. These envelopes containing the original and the copies shall then be enclosed in one single envelope.

iii. The original and the number of copies of the Bid as indicated in the **BDS** shall be typed or written in ink and shall be signed by the Bidder or its duly authorized representative/s.

iv. All envelopes shall:

(a) contain the name of the contract to be bid in capital letters;

(b) bear the name and address of the Bidder in capital letters;

(c) be addressed to the Procuring Entity's BAC in accordance with **ITB** Clause 1.i;

(d) bear the specific identification of this bidding process indicated in the **ITB** Clause **Error! Reference source not found.**; and

(e) bear a warning “DO NOT OPEN BEFORE…” the date and time for the opening of bids, in accordance with **ITB** Clause21.

v. Bid envelopes that are not properly sealed and marked, as required in the bidding documents, shall not be rejected, but the Bidder or its duly authorized representative shall acknowledge such condition of the bid as submitted. The BAC or the Procuring Entity shall assume no responsibility for the misplacement of the contents of the improperly sealed or marked bid, or for its premature opening.

D. Submission and Opening of Bids

21. Deadline for Submission of Bids

Bids must be received by the Procuring Entity’s BAC at the address and on or before the date and time indicated in the **BDS**. In case the deadline for submission of bids fall on a non-working day duly declared by the president, governor or mayor or other government official authorized to make such declaration, the deadline shall be the next working day.

22. Late Bids

Any bid submitted after the deadline for submission and receipt of bids prescribed by the Procuring Entity, pursuant to **ITB** Clause 21, shall be declared “Late” and shall not be accepted by the Procuring Entity. The BAC shall record in the minutes of bid submission and opening, the Bidder’s name, its representative and the time the late bid was submitted.

23. Modification and Withdrawal of Bids

23.1 The Bidder may modify its bid after it has been submitted; provided that the modification is received by the Procuring Entity prior to the deadline prescribed for submission and receipt of bids. The Bidder shall not be allowed to retrieve its original bid, but shall be allowed to submit another bid equally sealed and properly identified in accordance with ITB Clause 20, linked to its original bid marked as “TECHNICAL MODIFICATION” or “FINANCIAL MODIFICATION” and stamped “received” by the BAC. Bid modifications received after the applicable deadline shall not be considered and shall be returned to the Bidder unopened.

23.2 A Bidder may, through a Letter of Withdrawal, withdraw its bid after it has been submitted, for valid and justifiable reason; provided that the Letter of Withdrawal is received by the Procuring Entity prior to the deadline prescribed for submission and receipt of bids. The Letter of Withdrawal must be executed by the duly authorized representative of the Bidder identified in the Omnibus Sworn Statement, a copy of which should be attached to the letter.

23.3 Bids requested to be withdrawn in accordance with **ITB** Clause 0 shall be returned unopened to the Bidders. A Bidder, who has acquired the bidding documents, may also express its intention not to participate in the bidding through a letter which should reach and be stamped by the BAC before the deadline for submission and receipt of bids. A Bidder that withdraws its bid shall not be permitted to submit another bid, directly or indirectly, for the same contract.

23.4 No bid may be modified after the deadline for submission of bids. No bid may be withdrawn in the interval between the deadline for submission of bids and the expiration of the period of bid validity specified by the Bidder on the Financial Bid Form. Withdrawal of a bid during this interval shall result in the forfeiture of the Bidder's bid security, pursuant to **ITB** Clause18.v, and the imposition of administrative, civil and criminal sanctions as prescribed by RA 9184 and its IRR.

24. Opening and Preliminary Examination of Bids

i. The BAC shall open the bids in public, immediately after the deadline for the submission and receipt of bids, as specified in the **BDS**. In case the Bids cannot be opened as scheduled due to justifiable reasons, the BAC shall take custody of the Bids submitted and reschedule the opening of Bids on the next working day or at the soonest possible time through the issuance of a Notice of Postponement to be posted in the PhilGEPS website and the website of the Procuring Entity concerned.

ii. Unless otherwise specified in the **BDS**, the BAC shall open the first bid envelopes and determine each Bidder's compliance with the documents prescribed in **ITB** Clause 12, using a non-discretionary "pass/fail" criterion. If a Bidder submits the required document, it shall be rated "passed" for that particular requirement. In this regard, bids that fail to include any requirement or are incomplete or patently insufficient shall be considered as "failed". Otherwise, the BAC shall rate the said first bid envelope as "passed".

iii. Unless otherwise specified in the **BDS**, immediately after determining compliance with the requirements in the first envelope, the BAC shall forthwith open the second bid envelope of each remaining eligible bidder whose first bid envelope was rated "passed". The second envelope of each complying bidder shall be opened within the same day. In case one or more of the requirements in the second envelope of a particular bid is missing, incomplete or patently insufficient, and/or if the submitted total bid price exceeds the ABC unless otherwise provided in **ITB** Clause 13.ii, the BAC shall rate the bid concerned as "failed". Only bids that are determined to contain all the bid requirements for both components shall be rated "passed" and shall immediately be considered for evaluation and comparison.

iv. Letters of Withdrawal shall be read out and recorded during bid opening, and the envelope containing the corresponding withdrawn bid shall be returned to the Bidder unopened.

v. All members of the BAC who are present during bid opening shall initial every page of the original copies of all bids received and opened.

vi. In the case of an eligible foreign bidder as described in **ITB** Clause 5, the following Class "A" Documents may be substituted with the appropriate equivalent documents, if any, issued by the country of the foreign Bidder concerned, which shall likewise be uploaded and maintained in the PhilGEPS in accordance with Section 8.5.2 of the IRR:

(a) Registration certificate from the Securities and Exchange Commission (SEC), Department of Trade and Industry (DTI) for sole proprietorship, or CDA for cooperatives;

(b) Mayor's/Business permit issued by the local government where the principal place of business of the bidder is located; and

(c) Audited Financial Statements showing, among others, the prospective bidder's total and current assets and liabilities stamped "received" by the Bureau of Internal Revenue or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two years from the date of bid submission.

vii. Each partner of a joint venture agreement shall likewise submit the requirements in **ITB** Clause 12.1(a)(i). Submission of documents required under **ITB** Clauses 12.1(a)(ii) to 12.1(a)(iii)by any of the joint venture partners constitutes compliance.

viii. The Procuring Entity shall prepare the minutes of the proceedings of the bid opening that shall include, as a minimum: (a) names of Bidders, their bid price (per lot, if applicable, and/or including discount, if any), bid security, findings of preliminary examination, and whether there is a withdrawal or modification; and (b) attendance sheet. The BAC members shall sign the abstract of bids as read.

24.8 The bidders or their duly authorized representatives may attend the opening of bids. The BAC shall ensure the integrity, security, and confidentiality of all submitted bids. The Abstract of Bids as read and the minutes of the bid opening shall be made available to the public upon written request and payment of a specified fee to recover cost of materials.

24.9 To ensure transparency and accurate representation of the bid submission, the BAC Secretariat shall notify in writing all bidders whose bids it has received through its PhilGEPS-registered physical address or official e-mail address. The notice shall be issued within seven (7) calendar days from the date of the bid opening.

E. Evaluation and Comparison of Bids

25. Process to be Confidential

i. Members of the BAC, including its staff and personnel, as well as its Secretariat and TWG, are prohibited from making or accepting any kind of communication with any bidder regarding the evaluation of their bids until the issuance of the Notice of Award, unless otherwise allowed in the case of **ITB** Clause 26.

ii. Any effort by a bidder to influence the Procuring Entity in the Procuring Entity's decision in respect of bid evaluation, bid comparison or contract award will result in the rejection of the Bidder's bid.

26. Clarification of Bids

To assist in the evaluation, comparison, and post-qualification of the bids, the Procuring Entity may ask in writing any Bidder for a clarification of its bid. All responses to requests for clarification shall be in writing. Any clarification submitted by a Bidder in respect to its bid and that is not in response to a request by the Procuring Entity shall not be considered.

27. Domestic Preference

i. Unless otherwise stated in the **BDS**, the Procuring Entity will grant a margin of preference for the purpose of comparison of bids in accordance with the following:

(a) The preference shall be applied when the lowest Foreign Bid is lower than the lowest bid offered by a Domestic Bidder.

(b) For evaluation purposes, the lowest Foreign Bid shall be increased by fifteen percent (15%).

(c) In the event that the lowest bid offered by a Domestic Bidder does not exceed the lowest Foreign Bid as increased, then the Procuring Entity shall award the contract to the Domestic Bidder at the amount of the lowest Foreign Bid.

(d) If the Domestic Bidder refuses to accept the award of contract at the amount of the Foreign Bid within two (2) calendar days from receipt of written advice from the BAC, the Procuring Entity shall award to the bidder offering the Foreign Bid, subject to post-qualification and submission of all the documentary requirements under these Bidding Documents.

ii. A Bidder may be granted preference as a Domestic Bidder subject to the certification from the DTI that the Bidder is offering unmanufactured articles, materials or supplies of the growth or production of the Philippines, or manufactured articles, materials, or supplies manufactured or to be manufactured in the Philippines substantially from articles, materials, or supplies of the growth, production, or manufacture, as the case may be, of the Philippines.

28. Detailed Evaluation and Comparison of Bids

i. The Procuring Entity will undertake the detailed evaluation and comparison of bids which have passed the opening and preliminary examination of bids, pursuant to **ITB** Clause 24, in order to determine the Lowest Calculated Bid.

ii. The Lowest Calculated Bid shall be determined in two steps:

(a) The detailed evaluation of the financial component of the bids, to establish the correct calculated prices of the bids; and

(b) The ranking of the total bid prices as so calculated from the lowest to the highest. The bid with the lowest price shall be identified as the Lowest Calculated Bid.

iii. The Procuring Entity's BAC shall immediately conduct a detailed evaluation of all bids rated "passed," using non-discretionary pass/fail criteria. The BAC shall consider the following in the evaluation of bids:

(a) Completeness of the bid. Unless the **BDS** allows partial bids, bids not addressing or providing all of the required items in the Schedule of Requirements including, where applicable, Schedule of Prices, shall be considered non-responsive and, thus, automatically disqualified. In this regard, where a required item is provided, but no price is indicated, the same shall be considered as non-responsive, but specifying a zero (0)or a dash (-) for the said item would mean that it is being offered for free to the Procuring Entity, except those required by law or regulations to be provided for; and

(b) Arithmetical corrections. Consider computational errors and omissions to enable proper comparison of all eligible bids. It may also consider bid modifications. Any adjustment shall be calculated in monetary terms to determine the calculated prices.

iv. Based on the detailed evaluation of bids, those that comply with the above-mentioned requirements shall be ranked in the ascending order of their total calculated bid prices, as evaluated and corrected for computational errors, discounts and other modifications, to identify the Lowest Calculated Bid. Total calculated bid prices, as evaluated and corrected for computational errors, discounts and other modifications, which exceed the ABC shall not be considered, unless otherwise indicated in the **BDS**.

v. The Procuring Entity's evaluation of bids shall be based on the bid price quoted in the Bid Form, which includes the Schedule of Prices.

vi. Bids shall be evaluated on an equal footing to ensure fair competition. For this purpose, all bidders shall be required to include in their bids the cost of all taxes, such as, but not limited to, value added tax (VAT), income tax, local taxes, and other fiscal levies and duties which shall be itemized in the bid form and reflected in the detailed estimates. Such bids, including said taxes, shall be the basis for bid evaluation and comparison.

vii. If so indicated pursuant to **ITB** Clause 1.2, Bids are being invited for individual lots or for any combination thereof, provided that all Bids and combinations of Bids shall be received by the same deadline and opened and evaluated simultaneously so as to determine the Bid or combination of Bids offering the lowest calculated cost to the Procuring Entity. Bid prices quoted shall correspond to all items specified for each lot and to all quantities specified for each item of a lot. Bid Security as required by **ITB** Clause 18 shall be submitted for each contract (lot) separately. The basis for evaluation of lots is specified inBDSClause28.3.

29. Post-Qualification

i. The BAC shall determine to its satisfaction whether the Bidder that is evaluated as having submitted the Lowest Calculated Bid complies with and is responsive to all the requirements and conditions specified in **ITB** Clauses 5, 12, and 13.

ii. Within a non-extendible period of five(5) calendar days from receipt by the bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

Failure to submit any of the post-qualification requirements on time, or a finding against the veracity thereof, shall disqualify the bidder for award. Provided in the event that a finding against the veracity of any of the documents submitted is made, it shall cause the forfeiture of the bid security in accordance with Section 69 of the IRR of RA 9184.

iii. The determination shall be based upon an examination of the documentary evidence of the Bidder’s qualifications submitted pursuant to **ITB** Clauses 12 and 13, as well as other information as the Procuring Entity deems necessary and appropriate, using a non-discretionary “pass/fail” criterion, which shall be completed within a period of twelve (12) calendar days.

iv. If the BAC determines that the Bidder with the Lowest Calculated Bid passes all the criteria for post-qualification, it shall declare the said bid as the LCRB, and recommend to the HoPE the award of contract to the said Bidder at its submitted price or its calculated bid price, whichever is lower.

v. A negative determination shall result in rejection of the Bidder’s Bid, in which event the Procuring Entity shall proceed to the next Lowest Calculated Bid with a fresh period to make a similar determination of that Bidder’s capabilities to perform satisfactorily. If the second Bidder, however, fails the post qualification, the procedure for post qualification shall be repeated for the Bidder with the next Lowest Calculated Bid, and so on until the LCRB is determined for recommendation for contract award.

vi. Within a period not exceeding fifteen (15) calendar days from the determination by the BAC of the LCRB and the recommendation to award the contract, the HoPE or his duly authorized representative shall approve or disapprove the said recommendation.

vii. In the event of disapproval, which shall be based on valid, reasonable, and justifiable grounds as provided for under Section 41 of the IRR of RA 9184, the HoPE shall notify the BAC and the Bidder in writing of such decision and the grounds for it. When applicable, the BAC shall conduct a post-qualification of the Bidder with the next Lowest Calculated Bid. A request for reconsideration may be filed by the bidder with the HoPE in accordance with Section 37.1.3 of the IRR of RA 9184.

30. Reservation Clause

i. Notwithstanding the eligibility or post-qualification of a Bidder, the Procuring Entity concerned reserves the right to review its qualifications at any stage of the procurement process if it has reasonable grounds to believe that a misrepresentation has been made by the said Bidder, or that there has been a change in the Bidder’s capability to undertake the project from the time it submitted its eligibility requirements. Should such review uncover any misrepresentation made in the eligibility and bidding requirements, statements or documents, or any changes in the situation of the Bidder which will affect its capability to undertake the project so that it fails the preset eligibility or bid evaluation criteria, the Procuring Entity shall consider the said Bidder as ineligible and shall disqualify it from submitting a bid or from obtaining an award or contract.

ii. Based on the following grounds, the Procuring Entity reserves the right to reject any and all bids, declare a Failure of Bidding at any time prior to the contract award, or not to award the contract, without thereby incurring any liability, and make no assurance that a contract shall be entered into as a result of the bidding:

(a) If there is *prima facie* evidence of collusion between appropriate public officers or employees of the Procuring Entity, or between the BAC and any of the Bidders, or if the collusion is between or among the bidders themselves, or between a Bidder and a third party, including any act which restricts, suppresses or nullifies or tends to restrict, suppress or nullify competition;

(b) If the Procuring Entity’s BAC is found to have failed in following the prescribed bidding procedures; or

(c) For any justifiable and reasonable ground where the award of the contract will not redound to the benefit of the GOP as follows:

(i) If the physical and economic conditions have significantly changed so as to render the project no longer economically, financially or technically feasible as determined by the HoPE;

(ii) If the project is no longer necessary as determined by the HoPE; and

(iii) If the source of funds for the project has been withheld or reduced through no fault of the Procuring Entity.

iii. In addition, the Procuring Entity may likewise declare a failure of bidding when:

(a) No bids are received;

(b) All prospective Bidders are declared ineligible;

(c) All bids fail to comply with all the bid requirements or fail post-qualification; or

(d) The bidder with the LCRB refuses, without justifiable cause to accept the award of contract, and no award is madein accordance with Section 40 of the IRR of RA 9184.

F. Award of Contract

31. Contract Award

i. Subject to **ITB** Clause 29, the HoPE or its duly authorized representative shall award the contract to the Bidder whose bid has been determined to be the LCRB.

ii. Prior to the expiration of the period of bid validity, the Procuring Entity shall notify the successful Bidder in writing that its bid has been accepted, through a Notice of Award duly received by the Bidder or its representative personally or sent by registered mail or electronically, receipt of which must be confirmed in writing within two (2) days by the Bidder with the LCRB and submitted personally or sent by registered mail or electronically to the Procuring Entity.

iii. Notwithstanding the issuance of the Notice of Award, award of contract shall be subject to the following conditions:

(a) Submission of valid JVA, if applicable, within ten (10) calendar days from receipt of the Notice of Award;

(b) Posting of the performance security in accordance with **ITB** Clause33;

(c) Signing of the contract as provided in **ITB** Clause 32; and

(d) Approval by higher authority, if required, as provided in Section 37.3 of the IRR of RA 9184.

iv. At the time of contract award, the Procuring Entity shall not increase or decrease the quantity of goods originally specified in Section VI. Schedule of Requirements.

32. Signing of the Contract

i. At the same time as the Procuring Entity notifies the successful Bidder that its bid has been accepted, the Procuring Entity shall send the Contract Form to the Bidder, which contract has been provided in the Bidding Documents, incorporating therein all agreements between the parties.

ii. Within ten (10) calendar days from receipt of the Notice of Award, the successful Bidder shall post the required performance security, sign and date the contract and return it to the Procuring Entity.

iii. The Procuring Entity shall enter into contract with the successful Bidder within the same ten (10) calendar day period provided that all the documentary requirements are complied with.

iv. The following documents shall form part of the contract:

(a) Contract Agreement;

(b) Bidding Documents;

(c) Winning bidder’s bid, including the Technical and Financial Proposals, and all other documents/statements submitted (*e.g.,*bidder’s response to request for clarifications on the bid), including corrections to the bid, if any, resulting from the Procuring Entity’s bid evaluation;

(d) Performance Security;

(e) Notice of Award of Contract; and

(f) Other contract documents that may be required by existing laws and/or specified in the **BDS**.

33. Performance Security

i. To guarantee the faithful performance by the winning Bidder of its obligations under the contract, it shall post a performance security within a maximum period of ten (10) calendar days from the receipt of the Notice of Award from the Procuring Entity and in no case later than the signing of the contract.

ii. The Performance Security shall be denominated in Philippine Pesos and posted in favor of the Procuring Entity in an amount not less than the percentage of the total contract price in accordance with the following schedule:

Form of Performance Security	Amount of Performance Security (Not less than the Percentage of the Total Contract Price)
(a) Cash or cashier's/manager's check issued by a Universal or Commercial Bank. *For biddings conducted by the LGUs, the Cashier's/Manager's Check may be issued by other banks certified by the BSP as authorized to issue such financial instrument.*	Five percent (5%)
(b) Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank. *For biddings conducted by the LGUs, the Bank Draft/Guarantee or Irrevocable Letter of Credit may be issued by other banks certified by the BSP as authorized to issue such financial instrument.*	
(c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	Thirty percent (30%)

iii. Failure of the successful Bidder to comply with the above-mentioned requirement shall constitute sufficient ground for the annulment of the award and forfeiture of the bid security, in which event the Procuring

Entity shall have a fresh period to initiate and complete the post qualification of the second Lowest Calculated Bid. The procedure shall be repeated until the LCRB is identified and selected for recommendation of contract award. However if no Bidder passed post-qualification, the BAC shall declare the bidding a failure and conduct a re-bidding with re-advertisement, if necessary.

34. Notice to Proceed

Within seven (7) calendar days from the date of approval of the contract by the appropriate government approving authority, the Procuring Entity shall issue the Notice to Proceed (NTP) together with a copy or copies of the approved contract to the successful Bidder. All notices called for by the terms of the contract shall be effective only at the time of receipt thereof by the successful Bidder.

35. Protest Mechanism

Decisions of the procuring entity at any stage of the procurement process may be questioned in accordance with Section 55 of the IRR of RA 9184.

Section III. Bid Data Sheet

Bid Data Sheet

ITB Clause	
1.i	The Procuring Entity is **PHILIPPINE STATISTICS AUTHORITY (PSA)**
1.ii	The lot and reference is: **Supply, installation, support and maintenance of Automated Biometric Identification System (ABIS) for Philippine Identification System (PhilSys)** **(PR No: PSYS-19-10-115)**
2	The Funding Source is: The General Appropriations Act (GAA) 2019 through the Approved Budget of Contract of the Philippine Statistics Authority in the amount of One Billion Seven Hundred Million Pesos (₱1, 7000,000,000.00). The name of the Project is: **Supply, installation, support and maintenance of Automated Biometric Identification System (ABIS) for Philippine Identification System (PhilSys).**
3.i	No further instructions.
5.i	No further instructions.
5.ii	Foreign bidders, except those falling under **ITB** Clause 5.ii(b), may not participate in this Project.
5.iv	The Bidder must have completed, within the period specified in the Invitation to Bid and **ITB** Clause 12.1(a)(ii), a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC. For this purpose, similar contracts shall refer to: Design and Implementation of Biometric Solutions (fingerprint, iris and/or face) project to conduct 1:N de-duplication matching for at least 40 million gallery size within the past ten (10) years - These projects should be in operation for at least 2 years and comprising of components such as Client Registration, IDMS, ABIS, Authentication solutions and O&M services. - These projects can be in the field of National Identification systems, Civil registration, Voter registration, driving license, passport, or

	other systems of similar nature.
7	No further instructions.
8.i	Subcontracting is **not** allowed.
8.ii	Not applicable.
9.i	The Procuring Entity will hold a pre-bid conference for this Project on **15 October 2019, 1:30 P.M. at 17th Floor, Cyberpod Centris Three, Eton Centris, EDSA corner Quezon Avenue, Quezon City.**
10.i	The Procuring Entity’s address is: PSA-BAC Secretariat Attn: Atty. Revelyn C. Cayetano-Abduhalim 11th Floor, Cyberpod Centris One, Eton Centris EDSA corner Quezon Avenue, Quezon City Tel.No.: (02) 374-8281 Email : r.abduhalim@psa.gov.ph Web : www.psa.gov.ph or https://procurement.psa.gov.ph
i(a)	No further instructions.
12.1(a)(ii)	The bidder’s SLCC similar to the contract to be bid should have been completed within **ten (10) years** prior to the deadline for the submission and receipt of bids.
13.i(b)	No additional requirements.
13.i(b)	No further instructions.
13.1(c)	No additional requirements.
13.ii	The ABC is Php1,700,000,000.00. Any bid with a financial component exceeding this amount shall not be accepted.
15.4(a)(iv)	1. Technical support during system integration 2. On-site presence during ramp-up phase (right after ABIS go-live) 3. Biometric performance analysis and configuration of algorithms
15.iv(b)(i)	Not applicable**.**
15.4(b)(ii)	No incidental services are required.
16.i(b)	The Bid prices for Goods supplied from outside of the Philippines shall be quoted in Philippine Pesos.
16.3	Not applicable
17.i	Bids will be valid for one hundred twenty (120) calendar days from the opening of bids.
18.i	The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts: 1. The amount of not less than P34,000,000.00 *[2% of ABC]*, if bid security is in cash, cashier’s/manager’s check, bank draft/guarantee or

	irrevocable letter of credit issued by a Universal or Commercial Bank; or 2. The amount of not less than P85,000,000.00 *[5% of ABC]* if bid security is in Surety Bond.
18.ii	The Bid Security shall be valid for one hundred twenty (120) calendar days from the opening of bids.
20.iii	Each Bidder shall submit one (1) original and two (2) certified true copies of the first and second components of its bid.
21	The address for submission of bids is: Bids and Awards Committee Attn: Atty. Revelyn C. Cayetano-Abduhalim 11th Floor, Cyberpod Centris One, Eton Centris EDSA corner Quezon Avenue, Quezon City The deadline for submission of bids is **29 October 2019 not later than 1:30PM.**
24.i	The place of bid opening is 17th Floor, Cyberpod Centris Three, Eton Centris, EDSA corner Quezon Avenue, Quezon City. The date and time of bid opening is **29 October 2019, 1:30 PM.**
24.2	No further instructions.
24.3	No further instructions.
27.i	No further instructions.
28.iii (a)	**Grouping and Evaluation of Lots –** Partial bid is not allowed. The goods are grouped in a single lot and the lot shall not be divided into sub-lots for the purpose of bidding, evaluation, and contract award. In all cases, the NFCC computation, if applicable, must be sufficient for all the lots or contracts to be awarded to the Bidder.
28.iv	No further instructions.
29.2	No additional requirement.
32.iv(f)	No additional requirement.

Section IV. General Conditions of Contract

TABLE OF CONTENTS

1. Definitions

i. In this Contract, the following terms shall be interpreted as indicated:

(a) “The Contract” means the agreement entered into between the Procuring Entity and the Supplier, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

(b) “The Contract Price” means the price payable to the Supplier under the Contract for the full and proper performance of its contractual obligations.

(c) “The Goods” means all of the supplies, equipment, machinery, spare parts, other materials and/or general support services which the Supplier is required to provide to the Procuring Entity under the Contract.

(d) “The Services” means those services ancillary to the supply of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training, and other such obligations of the Supplier covered under the Contract.

(e) “GCC” means the General Conditions of Contract contained in this Section.

(f) “SCC” means the Special Conditions of Contract.

(g) “The Procuring Entity” means the organization purchasing the Goods, as named in the **SCC**.

(h) “The Procuring Entity’s country” is the Philippines.

(i) “The Supplier” means the individual contractor, manufacturer distributor, or firm supplying/manufacturing the Goods and Services under this Contract and named in the **SCC**.

(j) The “Funding Source” means the organization named in the **SCC**.

(k) “The Project Site,” where applicable, means the place or places named in the **SCC**.

(l) “Day” means calendar day.

(m) The “Effective Date” of the contract will be the date of signing the contract, however the Supplier shall commence performance of its obligations only upon receipt of the Notice to Proceed and copy of the approved contract.

(n) “Verified Report” refers to the report submitted by the Implementing Unit to the HoPE setting forth its findings as to the existence of grounds or causes for termination and explicitly stating its recommendation for the issuance of a Notice to Terminate.

2. Corrupt, Fraudulent, Collusive, and Coercive Practices

i. Unless otherwise provided in the **SCC**, the Procuring Entity as well as the bidders, contractors, or suppliers shall observe the highest standard of ethics during the procurement and execution of this Contract. In pursuance of this policy, the Procuring Entity:

(a) defines, for the purposes of this provision, the terms set forth below as follows:

(i) "corrupt practice" means behavior on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves, others, or induce others to do so, by misusing the position in which they are placed, and it includes the offering, giving, receiving, or soliciting of anything of value to influence the action of any such official in the procurement process or in contract execution; entering, on behalf of the Government, into any contract or transaction manifestly and grossly disadvantageous to the same, whether or not the public officer profited or will profit thereby, and similar acts as provided in Republic Act 3019.

(ii) "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Procuring Entity, and includes collusive practices among Bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the Procuring Entity of the benefits of free and open competition.

(iii) “collusive practices” means a scheme or arrangement between two or more Bidders, with or without the knowledge of the Procuring Entity, designed to establish bid prices at artificial, non-competitive levels.

(iv) “coercive practices” means harming or threatening to harm, directly or indirectly, persons, or their property to influence their participation in a procurement process, or affect the execution of a contract;

(v) “obstructive practice” is

(aa) deliberately destroying, falsifying, altering or concealing of evidence material to an administrative proceedings or investigation or making false statements to investigators in order to materially impede an administrative proceedings or investigation of the Procuring Entity or any foreign government/foreign or international financing institution into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the administrative proceedings or investigation or from pursuing such proceedings or investigation; or

(bb) acts intended to materially impede the exercise of the inspection and audit rights of the Procuring Entity or any foreign government/foreign or international financing institution herein.

(b) will reject a proposal for award if it determines that the Bidder recommended for award has engaged in any of the practices mentioned in this Clause for purposes of competing for the contract.

ii. Further the Funding Source, Borrower or Procuring Entity, as appropriate, will seek to impose the maximum civil, administrative and/or criminal penalties available under the applicable law on individuals and organizations deemed to be involved with any of the practices mentioned in **GCC** Clause i(a).

3. Inspection and Audit by the Funding Source

The Supplier shall permit the Funding Source to inspect the Supplier’s accounts and records relating to the performance of the Supplier and to have them audited by auditors appointed by the Funding Source, if so required by the Funding Source.

4. Governing Law and Language

i. This Contract shall be interpreted in accordance with the laws of the Republic of the Philippines.

ii. This Contract has been executed in the English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract. All correspondence and other documents pertaining to this Contract exchanged by the parties shall be written in English.

5. Notices

i. Any notice, request, or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request, or consent shall be deemed to have been given or made when received by the concerned party, either in person or through an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram, or facsimile to such Party at the address specified in the **SCC**, which shall be effective when delivered and duly received or on the notice's effective date, whichever is later.

ii. A Party may change its address for notice hereunder by giving the other Party notice of such change pursuant to the provisions listed in the **SCC** for **GCC** Clause i.

6. Scope of Contract

i. The Goods and Related Services to be provided shall be as specified in Section VI. Schedule of Requirements.

ii. This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. Any additional requirements for the completion of this Contract shall be provided in the **SCC**.

7. Subcontracting

i. Subcontracting of any portion of the Goods, if allowed in the **BDS**, does not relieve the Supplier of any liability or obligation under this Contract. The Supplier will be responsible for the acts, defaults, and negligence of any subcontractor, its agents, servants or workmen as fully as if these were the Supplier's own acts, defaults, or negligence, or those of its agents, servants or workmen.

ii. If subcontracting is allowed, the Supplier may identify its subcontractor during contract implementation. Subcontractors disclosed and identified during the bidding may be changed during the implementation of this Contract. In either case, subcontractors must submit the documentary requirements under **ITB** Clause 12 and comply with the eligibility criteria specified in the **BDS.** In the event that any subcontractor is found by the Procuring Entity to be ineligible, the subcontracting of such portion of the Goods shall be disallowed.

8. Procuring Entity's Responsibilities

i. Whenever the performance of the obligations in this Contract requires that the Supplier obtain permits, approvals, import, and other licenses from local public authorities, the Procuring Entity shall, if so needed by the Supplier, make its best effort to assist the Supplier in complying with such requirements in a timely and expeditious manner.

ii. The Procuring Entity shall pay all costs involved in the performance of its responsibilities in accordance with **GCC** Clause 6.

9. Prices

i. For the given scope of work in this Contract as awarded, all bid prices are considered fixed prices, and therefore not subject to price escalation during contract implementation, except under extraordinary circumstances and upon prior approval of the GPPB in accordance with Section 61 of R.A. 9184 and its IRR or except as provided in this Clause.

ii. Prices charged by the Supplier for Goods delivered and/or services performed under this Contract shall not vary from the prices quoted by the Supplier in its bid, with the exception of any change in price resulting from a Change Order issued in accordance with **GCC** Clause 29.

10. Payment

i. Payments shall be made only upon a certification by the HoPE to the effect that the Goods have been rendered or delivered in accordance with the terms of this Contract and have been duly inspected and accepted**.** Except with the prior approval of the President no payment shall be made for services not yet rendered or for supplies and materials not yet delivered under this Contract. At least one percent (1%) but shall not exceed five percent (5%) of the amount of each payment shall be retained by the Procuring Entity to cover the Supplier's warranty obligations under this Contract as described in **GCC** Clause 17.

ii. The Supplier's request(s) for payment shall be made to the Procuring Entity in writing, accompanied by an invoice describing, as appropriate, the Goods delivered and/or Services performed, and by documents submitted pursuant to the **SCC** provision for **GCC** Clause 6.ii, and upon fulfillment of other obligations stipulated in this Contract.

iii. Pursuant to **GCC** Clause ii, payments shall be made promptly by the Procuring Entity, but in no case later than sixty (60) days after submission of an invoice or claim by the Supplier. Payments shall be in accordance with the schedule stated in the **SCC**.

iv. Unless otherwise provided in the **SCC**, the currency in which payment is made to the Supplier under this Contract shall be in Philippine Pesos.

v. Unless otherwise provided in the **SCC**, payments using Letter of Credit (LC), in accordance with the Guidelines issued by the GPPB, is allowed. For this purpose, the amount of provisional sum is indicated in the **SCC**. All charges for the opening of the LC and/or incidental expenses thereto shall be for the account of the Supplier.

11. Advance Payment and Terms of Payment

i. Advance payment shall be made only after prior approval of the President, and shall not exceed fifteen percent (15%) of the Contract amount, unless otherwise directed by the President or in cases allowed under Annex "D" of RA 9184.

ii. All progress payments shall first be charged against the advance payment until the latter has been fully exhausted.

iii. For Goods supplied from abroad, unless otherwise indicated in the **SCC**, the terms of payment shall be as follows:

(a) On Contract Signature: Fifteen Percent (15%) of the Contract Price shall be paid within sixty (60) days from signing of the Contract and upon submission of a claim and a bank guarantee for the equivalent amount valid until the Goods are delivered and in the form provided in Section VIII. Bidding Forms.

(b) On Delivery: Sixty-five percent (65%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of receipt of the Goods and upon submission of the documents (i) through (vi) specified in the SCC provision on Delivery and Documents.

(c) On Acceptance: The remaining twenty percent (20%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of submission of the acceptance and inspection certificate for the respective delivery issued by the Procuring Entity's authorized representative. In the event that no inspection or acceptance certificate is issued by the Procuring Entity's authorized representative within forty five (45) days of the date shown on the delivery receipt, the Supplier shall have the right to claim payment of the remaining twenty percent (20%) subject to the Procuring Entity's own verification of the reason(s) for the failure to issue documents (vii) and (viii) as described in the SCC provision on Delivery and Documents.

12. Taxes and Duties

The Supplier, whether local or foreign, shall be entirely responsible for all the necessary taxes, stamp duties, license fees, and other such levies imposed for the completion of this Contract.

13. Performance Security

i. Within ten (10) calendar days from receipt of the Notice of Award from the Procuring Entity but in no case later than the signing of the contract by both parties, the successful Bidder shall furnish the performance security in any the forms prescribed in the **ITB** Clause 33.ii.

ii. The performance security posted in favor of the Procuring Entity shall be forfeited in the event it is established that the winning bidder is in default in any of its obligations under the contract.

iii. The performance security shall remain valid until issuance by the Procuring Entity of the Certificate of Final Acceptance.

iv. The performance security may be released by the Procuring Entity and returned to the Supplier after the issuance of the Certificate of Final Acceptance subject to the following conditions:

(a) There are no pending claims against the Supplier or the surety company filed by the Procuring Entity;

(b) The Supplier has no pending claims for labor and materials filed against it; and

(c) Other terms specified in the **SCC**.

v. In case of a reduction of the contract value, the Procuring Entity shall allow a proportional reduction in the original performance security, provided that any such reduction is more than ten percent (10%) and that the aggregate of such reductions is not more than fifty percent (50%) of the original performance security.

14. Use of Contract Documents and Information

i. The Supplier shall not, except for purposes of performing the obligations in this Contract, without the Procuring Entity's prior written consent, disclose this Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the Procuring Entity. Any such disclosure shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

ii. Any document, other than this Contract itself, enumerated in **GCC** Clause i shall remain the property of the Procuring Entity and shall be returned (all copies) to the Procuring Entity on completion of the Supplier's performance under this Contract if so required by the Procuring Entity.

15. Standards

The Goods provided under this Contract shall conform to the standards mentioned in the Section VII. Technical Specifications; and, when no applicable standard is mentioned, to the authoritative standards appropriate to the Goods' country of origin. Such standards shall be the latest issued by the institution concerned.

16. Inspection and Tests

i. The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Contract specifications at no extra cost to the Procuring Entity. The **SCC** and Section VII. Technical Specifications shall specify what inspections and/or tests the Procuring Entity requires and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

ii. If applicable, the inspections and tests may be conducted on the premises of the Supplier or its subcontractor(s), at point of delivery, and/or at the goods' final destination. If conducted on the premises of the Supplier or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Procuring Entity. The Supplier shall provide the Procuring Entity with results of such inspections and tests.

iii. The Procuring Entity or its designated representative shall be entitled to attend the tests and/or inspections referred to in this Clause provided that the Procuring Entity shall bear all of its own costs and expenses incurred in connection with such attendance including, but not limited to, all traveling and board and lodging expenses.

iv. The Procuring Entity may reject any Goods or any part thereof that fail to pass any test and/or inspection or do not conform to the specifications. The Supplier shall either rectify or replace such rejected Goods or parts thereof or make alterations necessary to meet the specifications at no cost to the Procuring Entity, and shall repeat the test and/or inspection, at no cost to the Procuring Entity, upon giving a notice pursuant to **GCC** Clause 5.

v. The Supplier agrees that neither the execution of a test and/or inspection of the Goods or any part thereof, nor the attendance by the Procuring Entity or its representative, shall release the Supplier from any warranties or other obligations under this Contract.

17. Warranty

i. The Supplier warrants that the Goods supplied under the Contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials, except when the technical specifications required by the Procuring Entity provides otherwise.

ii. The Supplier further warrants that all Goods supplied under this Contract shall have no defect, arising from design, materials, or workmanship or from any act or omission of the Supplier that may develop under normal use of the supplied Goods in the conditions prevailing in the country of final destination.

iii. In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier for a minimum period specified in the **SCC**. The obligation for the warranty shall be covered by, at the Supplier's option, either retention money in an amount equivalent to at least one percent (1%) but shall not exceed five percent (5%) of every progress payment, or a special bank guarantee equivalent to at least one percent (1%) but shall not exceed five percent (5%) of the total Contract Price or other such amount if so specified in the **SCC**. The said amounts shall only be released after the lapse of the warranty period specified in the **SCC**; provided, however, that the

Supplies delivered are free from patent and latent defects and all the conditions imposed under this Contract have been fully met.

iv. The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, within the period specified in the **SCC** and with all reasonable speed, repair or replace the defective Goods or parts thereof, without cost to the Procuring Entity.

v. If the Supplier, having been notified, fails to remedy the defect(s) within the period specified in **GCC** Clause iv, the Procuring Entity may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights which the Procuring Entity may have against the Supplier under the Contract and under the applicable law.

18. Delays in the Supplier's Performance

i. Delivery of the Goods and/or performance of Services shall be made by the Supplier in accordance with the time schedule prescribed by the Procuring Entity in Section VI. Schedule of Requirements.

ii. If at any time during the performance of this Contract, the Supplier or its Subcontractor(s) should encounter conditions impeding timely delivery of the Goods and/or performance of Services, the Supplier shall promptly notify the Procuring Entity in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Supplier's notice, and upon causes provided for under **GCC** Clause 22, the Procuring Entity shall evaluate the situation and may extend the Supplier's time for performance, in which case the extension shall be ratified by the parties by amendment of Contract.

iii. Except as provided under **GCC** Clause 22, a delay by the Supplier in the performance of its obligations shall render the Supplier liable to the imposition of liquidated damages pursuant to **GCC** Clause 19, unless an extension of time is agreed upon pursuant to **GCC** Clause 29 without the application of liquidated damages.

19. Liquidated Damages

Subject to **GCC** Clauses 18 and 22, if the Supplier fails to satisfactorily deliver any or all of the Goods and/or to perform the Services within the period(s) specified in this Contract inclusive of duly granted time extensions if any, the Procuring Entity shall, without prejudice to its other remedies under this Contract and under the applicable law, deduct from the Contract Price, as liquidated damages, the applicable rate of one tenth (1/10) of one (1) percent of the cost of the unperformed portion for every day of delay until actual delivery or performance. The maximum deduction shall be ten percent (10%) of the amount of contract. Once the maximum is reached, the Procuring Entity may rescind or terminate the Contract pursuant to **GCC** Clause 23, without prejudice to other courses of action and remedies open to it.

20. Settlement of Disputes

i. If any dispute or difference of any kind whatsoever shall arise between the Procuring Entity and the Supplier in connection with or arising out of this Contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

ii. If after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the Procuring Entity or the Supplier may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

iii. Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this Clause shall be settled by arbitration. Arbitration may be commenced prior to or after delivery of the Goods under this Contract.

iv. In the case of a dispute between the Procuring Entity and the Supplier, the dispute shall be resolved in accordance with Republic Act 9285 ("R.A. 9285"), otherwise known as the "Alternative Dispute Resolution Act of 2004."

v. Notwithstanding any reference to arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree; and the Procuring Entity shall pay the Supplier any monies due the Supplier.

21. Liability of the Supplier

i. The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines, subject to additional provisions, if any, set forth in the **SCC**.

ii. Except in cases of criminal negligence or willful misconduct, and in the case of infringement of patent rights, if applicable, the aggregate liability of the Supplier to the Procuring Entity shall not exceed the total Contract Price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

22. Force Majeure

i. The Supplier shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default if and to the extent that the Supplier's delay in performance or other failure to perform its obligations under the Contract is the result of a *force majeure*.

ii. For purposes of this Contract the terms "*force majeure*" and "fortuitous event" may be used interchangeably. In this regard, a fortuitous event or *force majeure* shall be interpreted to mean an event which the Supplier could not have foreseen, or which though foreseen, was inevitable. It shall not include ordinary unfavorable weather conditions; and any other cause the effects of which could have been avoided with the exercise of reasonable diligence by the Supplier. Such events may include, but not limited to, acts of the Procuring Entity in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.

iii. If a *force majeure* situation arises, the Supplier shall promptly notify the Procuring Entity in writing of such condition and the cause thereof. Unless otherwise directed by the Procuring Entity in writing, the Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the *force majeure*.

23. Termination for Default

i. The Procuring Entity shall terminate this Contract for default when any of the following conditions attends its implementation:

(a) Outside of *force majeure*, the Supplier fails to deliver or perform any or all of the Goods within the period(s) specified in the contract, or within any extension thereof granted by the Procuring Entity pursuant to a request made by the Supplier prior to the delay, and such failure amounts to at least ten percent (10%) of the contact price;

(b) As a result of *force majeure*, the Supplier is unable to deliver or perform any or all of the Goods, amounting to at least ten percent (10%) of the contract price, for a period of not less than sixty (60) calendar days after receipt of the notice from the Procuring Entity stating that the circumstance of force majeure is deemed to have ceased; or

(c) The Supplier fails to perform any other obligation under the Contract.

ii. In the event the Procuring Entity terminates this Contract in whole or in part, for any of the reasons provided under **GCC** Clauses 23 to 26, the Procuring Entity may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Supplier shall be liable to the Procuring Entity for any excess costs for such similar Goods or Services. However, the Supplier shall continue performance of this Contract to the extent not terminated.

iii. In case the delay in the delivery of the Goods and/or performance of the Services exceeds a time duration equivalent to ten percent (10%) of the specified contract time plus any time extension duly granted to the Supplier, the Procuring Entity may terminate this Contract, forfeit the

Supplier's performance security and award the same to a qualified Supplier.

24. Termination for Insolvency

The Procuring Entity shall terminate this Contract if the Supplier is declared bankrupt or insolvent as determined with finality by a court of competent jurisdiction. In this event, termination will be without compensation to the Supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Procuring Entity and/or the Supplier.

25. Termination for Convenience

i. The Procuring Entity may terminate this Contract, in whole or in part, at any time for its convenience. The HoPE may terminate a contract for the convenience of the Government if he has determined the existence of conditions that make Project Implementation economically, financially or technically impractical and/or unnecessary, such as, but not limited to, fortuitous event(s) or changes in law and national government policies.

ii. The Goods that have been delivered and/or performed or are ready for delivery or performance within thirty (30) calendar days after the Supplier’s receipt of Notice to Terminate shall be accepted by the Procuring Entity at the contract terms and prices. For Goods not yet performed and/or ready for delivery, the Procuring Entity may elect:

(a) to have any portion delivered and/or performed and paid at the contract terms and prices; and/or

(b) to cancel the remainder and pay to the Supplier an agreed amount for partially completed and/or performed goods and for materials and parts previously procured by the Supplier.

iii. If the Supplier suffers loss in its initial performance of the terminated contract, such as purchase of raw materials for goods specially manufactured for the Procuring Entity which cannot be sold in open market, it shall be allowed to recover partially from this Contract, on a *quantum meruit* basis. Before recovery may be made, the fact of loss must be established under oath by the Supplier to the satisfaction of the Procuring Entity before recovery may be made.

26. Termination for Unlawful Acts

i. The Procuring Entity may terminate this Contract in case it is determined *prima facie* that the Supplier has engaged, before or during the implementation of this Contract, in unlawful deeds and behaviors relative to contract acquisition and implementation. Unlawful acts include, but are not limited to, the following:

(a) Corrupt, fraudulent, and coercive practices as defined in **ITB** Clause 3.i(a);

(b) Drawing up or using forged documents;

(c) Using adulterated materials, means or methods, or engaging in production contrary to rules of science or the trade; and

(d) Any other act analogous to the foregoing.

27. Procedures for Termination of Contracts

i. The following provisions shall govern the procedures for termination of this Contract:

(a) Upon receipt of a written report of acts or causes which may constitute ground(s) for termination as aforementioned, or upon its own initiative, the Implementing Unit shall, within a period of seven (7) calendar days, verify the existence of such ground(s) and cause the execution of a Verified Report, with all relevant evidence attached;

(b) Upon recommendation by the Implementing Unit, the HoPE shall terminate this Contract only by a written notice to the Supplier conveying the termination of this Contract. The notice shall state:

(i) that this Contract is being terminated for any of the ground(s) afore-mentioned, and a statement of the acts that constitute the ground(s) constituting the same;

(ii) the extent of termination, whether in whole or in part;

(iii) an instruction to the Supplier to show cause as to why this Contract should not be terminated; and

(iv) special instructions of the Procuring Entity, if any.

(c) The Notice to Terminate shall be accompanied by a copy of the Verified Report;

(d) Within a period of seven (7) calendar days from receipt of the Notice of Termination, the Supplier shall submit to the HoPE a verified position paper stating why this Contract should not be terminated. If the Supplier fails to show cause after the lapse of the seven (7) day period, either by inaction or by default, the HoPE shall issue an order terminating this Contract;

(e) The Procuring Entity may, at any time before receipt of the Supplier’s verified position paper described in item (d) above withdraw the Notice to Terminate if it is determined that certain items or works subject of the notice had been completed, delivered, or performed before the Supplier’s receipt of the notice;

(f) Within a non-extendible period of ten (10) calendar days from receipt of the verified position paper, the HoPE shall decide whether or not to terminate this Contract. It shall serve a written notice to the Supplier of its decision and, unless otherwise provided, this Contract is deemed terminated from receipt of the Supplier of the notice of decision. The termination shall only be based on the ground(s) stated in the Notice to Terminate;

(g) The HoPE may create a Contract Termination Review Committee (CTRC) to assist him in the discharge of this function. All decisions recommended by the CTRC shall be subject to the approval of the HoPE; and

(h) The Supplier must serve a written notice to the Procuring Entity of its intention to terminate the contract at least thirty (30) calendar days before its intended termination. The Contract is deemed terminated if it is not resumed in thirty (30) calendar days after the receipt of such notice by the Procuring Entity.

28. Assignment of Rights

The Supplier shall not assign his rights or obligations under this Contract, in whole or in part, except with the Procuring Entity's prior written consent.

29. Contract Amendment

Subject to applicable laws, no variation in or modification of the terms of this Contract shall be made except by written amendment signed by the parties.

30. Application

These General Conditions shall apply to the extent that they are not superseded by provisions of other parts of this Contract.

Section V. Special Conditions of Contract

Special Conditions of Contract

GCC Clause	
1.i(g)	The Procuring Entity is PHILIPPINE STATISTICS AUTHORITY.
1.i(i)	The Supplier is LOWEST CALCULATED RESPONSIVE BID.
1.i(j)	The Funding Source is the General Appropriations Act (GAA) 2019 in the amount of **₱1,700,000,000.00.**
1.i(k)	The Project Site is **PSA Complex, East Avenue, Quezon City.**
2.1	No further instructions.
5.i	The Procuring Entity's address for Notices is: **CANDIDO J. ASTROLOGO JR.** OIC-Deputy National Statistician, CTCO Chair, PSA Bids and Awards Committee Attn: Atty. Revelyn C. Cayetano-Abduhalim Head, BAC Secretariat Philippine Statistics Authority 11th Floor, Cyberpod Centris One, Eton Centris EDSA corner Quezon Avenue, Quezon City Telephone No. (02) 374-8281 Email: r.abduhalim@psa.gov.ph The Supplier's address for Notices is:*[Insert address including, name of contact, fax and telephone number]*
6.ii	**Delivery and Documents –** For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: *For Goods Supplied from Abroad, state* "The delivery terms applicable to the Contract are DDP delivered *[insert place of destination]*. In accordance with INCOTERMS." *For Goods Supplied from Within the Philippines, state* "The delivery terms applicable to this Contract are delivered *[insert place of destination]*. Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination." Delivery of the Goods shall be made by the Supplier in accordance

with the terms specified in Section VI. Schedule of Requirements. The details of shipping and/or other documents to be furnished by the Supplier are as follows:

For Goods supplied from within the Philippines:

Upon delivery of the Goods to the Project Site, the Supplier shall notify the Procuring Entity and present the following documents to the Procuring Entity:

(i) Original and four copies of the Supplier's invoice showing Goods' description, quantity, unit price, and total amount;

(ii) Original and four copies delivery receipt/note, railway receipt, or truck receipt;

(iii) Original Supplier's factory inspection report;

(iv) Original and four copies of the Manufacturer's and/or Supplier's warranty certificate;

(v) Original and four copies of the certificate of origin (for imported Goods);

(vi) Delivery receipt detailing number and description of items received signed by the authorized receiving personnel;

(vii) Certificate of Acceptance/Inspection Report signed by the Procuring Entity's representative at the Project Site; and

(viii) Four copies of the Invoice Receipt for Property signed by the Procuring Entity's representative at the Project Site.

For Goods supplied from abroad:

Upon shipment, the Supplier shall notify the Procuring Entity and the insurance company by cable the full details of the shipment, including Contract Number, description of the Goods, quantity, vessel, bill of lading number and date, port of loading, date of shipment, port of discharge etc. Upon delivery to the Project Site, the Supplier shall notify the Procuring Entity and present the following documents as applicable with the documentary requirements of any letter of credit issued taking precedence:

(i) Original and four copies of the Supplier's invoice showing Goods' description, quantity, unit price, and total amount;

(ii) Original and four copies of the negotiable, clean shipped on board bill of lading marked "freight pre-paid" and five copies of the non-negotiable bill of lading ;

(iii) Original Supplier's factory inspection report;

(iv) Original and four copies of the Manufacturer's and/or Supplier's warranty certificate;

	(v) Original and four copies of the certificate of origin (for imported Goods); (vi) Delivery receipt detailing number and description of items received signed by the Procuring Entity’s representative at the Project Site; (vii) Certificate of Acceptance/Inspection Report signed by the Procuring Entity’s representative at the Project Site; and (viii) Four copies of the Invoice Receipt for Property signed by the Procuring Entity’s representative at the Project Site. For purposes of this Clause the Procuring Entity’s Representative at the Project Site is: Edgar M. Fajutagana PSA Complex, East Avenue Barangay Pinyahan, Diliman Quezon City **Incidental Services –** The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements: (a) performance or supervision of on-site assembly and/or start-up of the supplied Goods; (b) furnishing of tools required for assembly and/or maintenance of the supplied Goods; (c) furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods; (d) performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract; and (e) training of the Procuring Entity’s personnel, at the Supplier’s plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods. The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services. **Spare Parts –** The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured

or distributed by the Supplier:

(a) such spare parts as the Procuring Entity may elect to purchase from the Supplier, provided that this election shall not relieve the Supplier of any warranty obligations under this Contract; and

(b) in the event of termination of production of the spare parts:

i. advance notification to the Procuring Entity of the pending termination, in sufficient time to permit the Procuring Entity to procure needed requirements; and

ii. following such termination, furnishing at no cost to the Procuring Entity, the blueprints, drawings, and specifications of the spare parts, if requested.

The spare parts required are listed in Section VI. Schedule of Requirements and the cost thereof are included in the Contract Price

The Supplier shall carry sufficient inventories to assure ex-stock supply of consumable spares for the Goods for a period of five (5) years.

Other spare parts and components shall be supplied as promptly as possible, but in any case within one (1) month of placing the order.

Packaging –

The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the GOODS' final destination and the absence of heavy handling facilities at all points in transit.

The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity.

The outer packaging must be clearly marked on at least four (4) sides as follows:

Name of the Procuring Entity

Name of the Supplier

Contract Description

Final Destination

Gross weight

Any special lifting instructions

Any special handling instructions

Any relevant HAZCHEM classifications

A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging.

Insurance –

The Goods supplied under this Contract shall be fully insured by the Supplier in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage, and delivery. The Goods remain at the risk and title of the Supplier until their final acceptance by the Procuring Entity.

Transportation –

Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price.

Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the Contract Price.

Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered *force majeure* in accordance with **GCC** Clause 22.

	The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP Deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. **Patent Rights –** The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
10.4	Not applicable.
10.5	Payment using LC is not allowed.
11.3	(a) On Contract Signature: Fifteen Percent (15%) of the Contract Price shall be paid within sixty (60) days from signing of the Contract and upon submission of a claim and a bank guarantee for the equivalent amount valid until the Goods are delivered and in the form provided in Section VIII. Bidding Forms. (b) On Delivery: The payment of 65% shall be made in three tranches, as stated below: i. Forty percent (40%) of the Contract Price shall be paid to the Supplier upon delivery of ABIS Software, Hardware and Peripherals within sixty (60) days after the date of receipt of the Goods and upon submission of the documents (i) through (vi) specified in the SCC provision on Delivery and Documents. ii. Fifteen percent (15%) of the Contract Price shall be paid to the Supplier upon Successful ABIS Go Live within sixty (60) days after the date of receipt of the Goods and upon submission of the documents (i) through (vi) specified in the SCC provision on Delivery and Documents. iii. Ten percent (10%) of the Contract Price shall be paid to the Supplier upon Successful PhilSys Go Live within sixty (60) days after the date of receipt of the Goods and upon submission of the documents (i) through (vi) specified in the SCC provision on Delivery and Documents. (c) On Acceptance: The remaining twenty percent (20%) of the Contract Price shall be paid upon successful installation and migration of ABIS at the permanent Data Center and DR site

	within sixty (60) days after the date of submission of the acceptance and inspection certificate for the respective delivery issued by PSA's authorized representative.
13.iv(c)	No further instructions.
i	The inspections and tests that will be conducted are: • Upon delivery, the Goods shall undergo preliminary physical inspection by the Inspection Team of PSA to ascertain the physical condition and acceptability of the Goods. • The supplier shall promptly replace the equivalent quantity of Goods taken as samples without cost to PSA.
17.iii	In order to assure that the manufacturing defects shall be corrected by the supplier, the warranty period for this project is five (5) years from date of Notice to Proceed (NTP) of ABIS. The warranty shall cover full replacement of defective items, free of charge, including labor, spare parts and materials. The obligation or the warranty for each item being bid shall be covered thru either of the following: • Retention Money equivalent to at least one percent (1%) of every progress payment; or • Special Bank Guarantee equivalent to five percent (5%) of the total Contract Price. The said amounts shall only be released after the lapse of the warranty period; provided, however, that the Supplies delivered are free from patent and latent defects and all the conditions imposed under this Contract have been fully met.
17.iv	The period for correction of defects in the warranty period shall not be more than 15 calendar days.
21.i	No additional provision. However, if the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

Section VI. Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

Description	Qty	Total	Delivered, Weeks/Months
Supply, installation, support and maintenance of Automated Biometric Identification System (ABIS) for Philippine Identification System (PhilSys).	1 Lot	PhP1,700,000,000.00	Delivery, installation and commissioning of sandbox of 1 Million Biometric Records must be sixty (60) days upon issuance of the Notice to Proceed. Delivery, installation and commissioning of ABIS hardware/software solution must be within ninety (90) calendar days upon issuance of the Notice to Proceed. Deliver to: PSA PhilSys Office, PSA Complex, East Avenue, Quezon City, and installation, commissioning at the identified PSA Data Centers and DR site.

I hereby commit to comply and deliver all the above requirements in accordance with the above-stated schedule.

Name of Company

Signature over Printed Name
Of Authorized Representative

Date

Section VII. Technical Specifications

Technical Specifications

Item	Specification	Statement of Compliance
		Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of **ITB** Clause 3.i(a)(ii) and/or **GCC** Clause 2.i(a)(ii).

TECHNICAL SPECIFICATIONS

Category	Specification	Statement of Compliance
Bidder		
Proposed ABIS Customization	• Bidder must be able to customize their proposed ABIS for fingerprint, face and iris according to the requirements of PhilSys. • Bidder must be able to provide brochures or documents related to the customization of their ABIS (for ABIS technical requirements)	

Experience	• Bidder must provide ABIS-related project references from at least two (2) different countries, as proof of their international competence. • Bidder must be an Original Design Manufacturer of the ABIS and must be on the biometrics market for at least ten (10) years in order to ensure that only well-proven and matured technology will be supplied. This should be proven by related company documents. • Bidder must have an Automated Biometric Identification System (ABIS) installations with at least forty (40) million records of at least one of the three (3) biometrics modalities in the database. This should be proven by related reference letters/documents.	
Financial Standing	• Bidder must be in good financial standing where Net Worth / Net Assets based on latest Annual Financial Statements (AFS) should be at least equal to 50% of the ABC and Reported Revenue of at least 50% of the ABC for the past 3 years based on the corresponding AFSs for that period. This should be proven by the financial statements for the last 3 years.	

The **Compliance Form – Technical Requirements – Bidder** is provided in page [81] of this Bidding Documents.

The Statement of Compliance to **Technical Specification Requirements (Volume 2).**

Technical Specification Requirements	**Specification (refer to page of Volume 2: Technical Specifications)**	**Statement of Compliance**
10. Biometric Solution	28	
10.1 ABIS solution design principles	28	
10.2 Biometric standards	29	
10.3 Interoperability Standards	29	
10.4 System Architecture Requirements	30	
10.5 Biometric Components	34	
10.6 ABIS Biometric Matcher	34	
11. Functional and Technical Requirements	35	
11.1 Enrollment	35	
11.2 Management	35	

Technical Specification Requirements	Specification (refer to page of Volume 2: Technical Specifications)	Statement of Compliance
11.3 Verification	36	
11.4 Data storage requirement	36	
11.5 Logging and monitoring	36	
11.5.1 ABIS Log	37	
11.5.2 Verification Log	37	
11.5.3 Management Functions Log	37	
11.6 Security Requirements	38	
11.7 Operator Interface Requirements	38	
11.8 Biometric Middleware	38	
11.9 Multimodal SDK	39	
11.9.1 Fingerprint	39	
11.9.2 Iris	39	
11.9.3 Face Photo	40	
11.10 Standards requirements	40	
11.11 Reliability Requirements	40	
11.12 Security Requirements	41	
11.13 User Interface Requirements	41	
11.14 Platform requirements	41	
11.15 Biometric Middleware	42	
11.16 Authentication Solution (SDKs and Integration Support)	42	
11.17 Biometric Manual Adjudication Solution	43	
11.18 Licensing Requirements	44	
11.19 Load Requirement	45	
12. Scope of Work	46	
12.1 Overview of scope of work	46	
12.2 Project Planning and Initiation	49	
12.3 Capacity Planning	50	
12.4 Requirements Analysis	51	
12.5 Solution Design	51	
12.6 Supply, Customization and Implementation of Biometric Solution	52	
12.7 Set up of Biometric Solution	52	
12.8 Integration Requirements	52	
12.8.1 Integration Requirements for PSA or its appointed party	52	
12.8.2 Integration Requirements for BioSP	53	
12.9 User Acceptance Testing (UAT)	53	
12.10 Roll out of Biometric Solution - ABIS Go-Live	54	
12.11 Conditions for re-templatization	54	
12.12 Setup of Data Center sites	55	
12.12.1 Data Center Strategy	55	

Technical Specification Requirements	Specification (refer to page of Volume 2: Technical Specifications)	Statement of Compliance
12.12.2 DC/DR set up in the interim	55	
12.12.3 Permanent DC/DR set up	55	
12.13 Transition and Migration of Data Center	56	
12.14 Biometric Solution Hosting Requirements	56	
12.14.1 Supply of Hardware	56	
12.14.2 Environment Creation	58	
13. Benchmarking, Acceptance and Go-Live	58	
13.1 Benchmarking	58	
13.2 Commissioning	61	
13.3 Acceptance	61	
13.4 Go-Live	61	
14. Manpower Requirement	61	
14.1 Guidelines for staffing and provisioning of manpower	61	
14.2 BioSP functions that can be performed off-site	62	
14.3 Replacement of Personnel	62	
14.4 Removal of Personnel	63	
14.5 Logistics requirements of the Personnel	63	
14.6 Escalation Matrix	63	
14.7 Deployment of Resources	63	
14.8 Profile Qualifications	64	
14.9 Indicative deployment schedule	66	
15. Ongoing Maintenance	66	
15.1 Maintenance Management	66	
15.2 Biometric Solution Management	67	
15.3 Infrastructure Management	68	
15.4 Information Security	69	
15.4.1 ISO certification readiness for Information Security Management	69	
15.4.2 Responsibility for the overall security of the biometric solution	69	
15.5 Help desk Support	69	
15.6 Business Continuity Support	70	
15.7 Warranty and Annual Technical Support (ATS)	71	
16. Project Management	71	
16.1 Project Status Monitoring and Reporting	71	
16.2 Risk and Issue Management	71	
16.3 Change Control Management	72	
16.4 Transition and Migration to new Data Center sites	72	
16.5 Training	73	
16.6 Reporting	74	
16.6.1 ABIS Reports	74	

Technical Specification Requirements	Specification (refer to page of Volume 2: Technical Specifications)	Statement of Compliance
16.6.2 Data Quality Monitoring & Reporting	74	
16.6.3 Incident and Issue Reporting	75	
16.6.4 SLA Reporting	75	
17. Implementation Schedule	77	
18. Knowledge Transfer & Exit Management	77	
18.1 Knowledge Transfer	77	
18.2 Exit Management Plan	78	
19. Service Level Agreement	79	
19.1 Service Levels	79	
19.2 Definition of Terms	79	
19.3 Service Levels and Targets	80	
19.4 SLA Framework	80	
19.4.1 Responsibilities of Parties	80	
19.4.2 Reporting Procedures	81	
19.4.3 SLA Change Process	81	
19.4.4 Liquidated Damages	81	
19.4.5 Category of Service Levels	82	
19.4.6 Service Levels and Targets	83	

Conforme:

____
Name of Company

____
Name and Signature of Company Authorized Representative

____
Date

Section VIII. Bidding Forms

TABLE OF CONTENTS

Bid Form

Date: ______________________
Invitation to Bid No: ______________________

CANDIDO J. ASTROLOGO JR.
BAC Chairperson
Philippine Statistics Authority
11th Floor, Cyberpod Centris One, Eton Centris
EDSA corner Quezon Avenue, Quezon City

Sir:

Having examined the Bidding Documents including Bid Bulletin Numbers *[insert numbers]*, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to *[supply/deliver/perform] [description of the Goods]* in conformity with the said Bidding Documents for the sum of *[total Bid amount in words and figures]* or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Bid.

We undertake, if our Bid is accepted, to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements.

If our Bid is accepted, we undertake to provide a performance security in the form, amounts, and within the times specified in the Bidding Documents.

We agree to abide by this Bid for the Bid Validity Period specified in **BDS** provision for **ITB** Clause 17.1 and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

We understand that you are not bound to accept the Lowest Calculated Bid or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements as per **ITB** Clause 5 of the Bidding Documents.

We likewise certify/confirm that the undersigned, *[for sole proprietorships, insert:* as the owner and sole proprietor or authorized representative of *Name of Bidder*, has the full power and authority to participate, submit the bid, and to sign and execute the ensuing contract, on the latter's behalf for the *Name of Project* of the *Name of the Procuring Entity][for partnerships, corporations, cooperatives, or joint ventures, insert:* is granted full power and authority by the *Name of Bidder*, to participate, submit the bid, and to sign and execute the ensuing contract on the latter's behalf for *Name of Project* of the *Name of the Procuring Entity]*.

We acknowledge that failure to sign each and every page of this Bid Form, including the attached Schedule of Prices, shall be a ground for the rejection of our bid.

Dated this _________________ day of _________________ 20______.

________________________________ _____________________________________

[signature] *[in the capacity of]*

Duly authorized to sign Bid for and on behalf of __________________________________

For Goods Offered From Abroad

Name of Bidder ______________________. Invitation to Bid Number ____. Page ____ of ____________________________________.

1	2	3	4	5	6	7	8	9
Item	Description	Country of origin	Quantity	Unit price CIF port of entry (specify port) or CIP named place (specify border point or place of destination)	Total CIF or CIP price per item (col. 4 x 5)	Unit Price Delivered Duty Unpaid (DDU)	Unit price Delivered Duty Paid (DDP)	Total Price delivered DDP (col 4 x 8)

______________________________ *[signature]*

__________________________________ *[in the capacity of]*

Duly authorized to sign Bid for and on behalf of ________________________________

For Goods Offered From Within the Philippines

Name of Bidder ________________________. Invitation to Bid Number __. Page _ of ____.

1	2	3	4	5	6	7	8	9	10
Item	Description	Country of origin	Quantity	Unit price EXWper item	Transportation and Insurance and all other costs incidental to delivery, per item	Sales and other taxes payable if Contract is awarded, per item	Cost of Incidental Services, if applicable, per item	Total Price, per unit (col 5+6+7+8)	Total Price delivered Final Destination (col 9) x (col 4)

________________________________ *[signature]*

________________________________ *[in the capacity of]*

Duly authorized to sign Bid for and on behalf of ________________________________

Compliance Form
Technical Specification Requirements - Bidder

1. Proposed ABIS Customization

Bidder to provide details on how to customize the proposed ABIS according to the requirements of PhilSys. Please provide a short description in the space provided. Please use extra sheets if necessary.

a. For Fingerprint modality: ____
____
____
____

Brochure or document related to the fingerprint modality customization attached as Annex(es)_____.

b. For Face modality: ____
____
____
____

Brochure or document related to the face modality customization attached as Annex(es) _____.

c. For Iris modality: __-
____
____
____
____

Brochure or document related to the iris modality customization attached as Annex(es) _____.

2. Bidder Experience

a. Project References

Bidder to provide ABIS-related project references from at least two (2) different countries, as proof of its international competence. Please use extra sheets if necessary.

	Name of Project – Country of Operation	**Project Description (include as Annex certified copies of ANSI/NIST-ITL-1, ISO/IEC certifications, awards, or recognitions)**
		Refer to Annex(es) _____.
		Refer to Annex(es) _____.

b. Biometrics Market Experience

Bidder must be an Original Design Manufacturer of the ABIS and must be on the biometrics market for at least ten (10) years in order to ensure that only well-proven and matured technology will be supplied. Please use extra sheets if necessary.

Relevant Year(s)	**Product/Technology Model**	**Description and Developments (include related company documents)**
		Refer to Annex(es) _____.
		Refer to Annex(es) _____.

		Refer to Annex(es) _____.
		Refer to Annex(es) _____.
		Refer to Annex(es) _____.

c. ABIS Installations

Bidder must have a minimum of Two (2) Automated Biometric Identification System (ABIS) installations with at least 20 million records of at least one of the three biometrics modalities in the database. Please use extra sheets if necessary.

	ABIS Installation (include related reference letters)	**Biometric Modality (Fingerprint, Face, and/or Iris)**	**Number of ABIS Records**
	Refer to Annex(es) _____.		
	Refer to Annex(es) _____.		

3. Financial Standing

Bidder must be in good financial standing where (1) Net Worth / Net Assets, based on latest Annual Financial Statements (AFS), is at least equal to 50% of the Approved Budget for the Contract (ABC) and (2) Reported Revenue of at least 50% of the ABC for the past 3 years based on the corresponding AFS for that period. The ABC is PhP 1,700,000,000.00.

For this purpose, the latest AFS stamped received by the tax authority for the preceding calendar year, which should not be earlier than two (2) years from the date of submission of the bid.

a. Net Worth/Net Asset

[Y0 (Based on Latest AFS)]	
Net Worth (in PhP)	
Net Asset (in PhP)	
Net Worth ÷ Net Assets	

b. Reported Revenue

Fiscal Year (past 3 years from latest AFS)	**Total Revenue (in PhP)**	**Equal to, Less than, or More than PhP 850,000,000.00 (50% of ABC)**
[Y1]		
[Y2]		
[Y3]		

Annual Financial Statements are attached as Annex(es) _____.

Contract Agreement Form

THIS AGREEMENT made the _____ day of __________ 20_____ between *[name of PROCURING ENTITY]* of the Philippines(hereinafter called “the Entity”) of the one part and *[name of Supplier]* of *[city and country of Supplier]* (hereinafter called “the Supplier”) of the other part:

WHEREAS the Entity invited Bids for certain goods and ancillary services, viz., *[brief description of goods and services]* and has accepted a Bid by the Supplier for the supply of those goods and services in the sum of *[contract price in words and figures]* (hereinafter called “the Contract Price”).

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:

(a) the Supplier’s Bid, including the Technical and Financial Proposals, and all other documents/statements submitted(*e.g.* bidder’s response to clarifications on the bid), including corrections to the bid resulting from the Procuring Entity’s bid evaluation;
(b) the Schedule of Requirements;
(c) the Technical Specifications;
(d) the General Conditions of Contract;
(e) the Special Conditions of Contract;
(f) the Performance Security; and
(g) the Entity’s Notice of Award.

3. In consideration of the payments to be made by the Entity to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Entity to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the Contract

4. The Entity hereby covenants to pay the Supplier in consideration of the provision of the goods and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the time and in the manner prescribed by the contract.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with the laws of the Republic of the Philippines on the day and year first above written.

Signed, sealed, delivered by _________________ the _________________ (for the Entity)

Signed, sealed, delivered by _________________ the _________________ (for the Supplier).

Omnibus Sworn Statement

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

AFFIDAVIT

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

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

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

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

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

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

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

3. *[Name of Bidder]* is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board;

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

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

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

   If a sole proprietorship: The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   If a partnership or cooperative: None of the officers and members of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   If a corporation or joint venture: None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards; and

8. *[Name of Bidder]* is aware of and has undertaken the following responsibilities as a Bidder:

   a) Carefully examine all of the Bidding Documents;

   b) Acknowledge all conditions, local or otherwise, affecting the implementation of the Contract;

   c) Made an estimate of the facilities available and needed for the contract to be bid, if any; and

   d) Inquire or secure Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.

9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

IN WITNESS WHEREOF, I have hereunto set my hand this __ day of ___, 20__ at ____________, Philippines.

____
Bidder's Representative/Authorized Signatory

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

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

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 _____

Bank Guarantee Form for Advance Payment

To: *[name and address of PROCURING ENTITY]*
[name of Contract]

Gentlemen and/or Ladies:

In accordance with the payment provision included in the Special Conditions of Contract, which amends Clause 10 of the General Conditions of Contract to provide for advance payment, *[name and address of Supplier]* (hereinafter called the "Supplier") shall deposit with the PROCURING ENTITY a bank guarantee to guarantee its proper and faithful performance under the said Clause of the Contract in an amount of *[amount of guarantee in figures and words]*.

We, the *[bank or financial institution]*, as instructed by the Supplier, agree unconditionally and irrevocably to guarantee as primary obligator and not as surety merely, the payment to the PROCURING ENTITY on its first demand without whatsoever right of objection on our part and without its first claim to the Supplier, in the amount not exceeding *[amount of guarantee in figures and words]*.

We further agree that no change or addition to or other modification of the terms of the Contract to be performed thereunder or of any of the Contract documents which may be made between the PROCURING ENTITY and the Supplier, shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition, or modification.

This guarantee shall remain valid and in full effect from the date of the advance payment received by the Supplier under the Contract until *[date]*.

Yours truly,

Signature and seal of the Guarantors

[name of bank or financial institution]

[address]

[date]

Bid Securing Declaration Form

REPUBLIC OF THE PHILIPPINES)
CITY OF _______________________) S.S.

x---x

BID SECURING DECLARATION

Invitation to Bid:*[Insert Reference number]*

To: *[Insert name and address of the Procuring Entity]*

I/We[1], the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid-Securing Declaration.

2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1(f), of the IRR of RA 9184; without prejudice to other legal action the government may undertake.

3. I/We understand that this Bid Securing Declaration shall cease to be valid on the following circumstances:

   (a) Upon expiration of the bid validity period, or any extension thereof pursuant to your request;

   (b) I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right;

   (c) I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

[1] *Select one and delete the other. Adopt the same instruction for similar terms throughout the document.*

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this ____ day of *[month] [year]* at *[place of execution]*.

[Insert NAME OF BIDDER'S AUTHORIZED REPRESENTATIVE]
[Insert Signatory's Legal Capacity]
Affiant

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

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

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 _____

CHECKLIST OF ELIGIBILITY REQUIREMENTS

FIRST ENVELOPE

ELIGIBILITY & TECHNICAL DOCUMENTS

A. ELIGIBILITY DOCUMENTS: CLASS "A" DOCUMENTS

1. PhilGEPS Certificate of Registration and Membership

2. Statement of all ongoing and completed government & private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid; and

Statement of the Bidder's SLCC similar to the contract to be bid, in accordance with ITB Clause 5.4.

The two statements required shall indicate for each contract the following:

a) name of contract,
b) date of the contract;
c) contract duration;
d) owner's name and address;
e) kinds of goods;
f) For Statement of Ongoing Contracts - amount of contract and value of outstanding contracts;
g) For Statement of SLCC - amount of completed contracts
h) date of delivery; and
i) end user's acceptance or official receipt(s) issued for the contract, if completed;

3. NFCC Computation in accordance with ITB Clause 5.5 or Committed Line of Credit (CLC) from a Universal or commercial bank.

CLASS "B" DOCUMENTS

4. Valid Joint Venture Agreement (JVA), if applicable.

B. TECHNICAL DOCUMENTS

1. **Bid security** in accordance with ITB Clause 18. Bid Securing Declaration or:
   If the bidder opts to submit bid security in the form of:
   a. Cash, Cashier's/Manager's check, Bank draft/guarantee or an irrevocable Letter of Credit in the amount of 2% of ABC;
   b. Surety bond, accompanied by a certification by the Insurance Commission that the surety or insurance company is authorized to issue such instruments in the amount equivalent to 5%.

2. **Conformity with Technical Specifications** as enumerated and specified in Sections VI and VII of the PBD;

3. **Omnibus Sworn statement** in accordance with Section 25.3 of the IRR (duly notarized)
   a. Certification that the prospective bidder is not "blacklisted" or barred from bidding.
   b. Certification under oath that each of the documents submitted in satisfaction of the eligibility requirements is an authentic and original copy, or a true and faithful reproduction of the original, complete, and that all statements and information provided therein are true and correct.
   c. Certification authorizing the BAC or its duly authorized representative(s) to verify any or all of the documents submitted for the eligibility check.

d. Authority of the Signatory
e. Certification of Disclosure of No Relationship
f. Certification attesting to the responsibilities of bidder
g. Certification of compliance with existing labor laws and standards
h. Certification that the bidder did not give or pay directly or indirectly, any commission, amount, fee or any form of consideration to any person or official, personnel or representative of the government in relation to any procurement project or activity.
SECOND ENVELOPE
FINANCIAL DOCUMENTS 1. Financial Bid Form

Republic of the Philippines

gppb

Government Procurement Policy Board

PHILIPPINE BIDDING DOCUMENTS

Supply, installation, support and maintenance of Automated Biometric Identification Systems (ABIS) for Philippine Identification System (PhilSys)

Government of the Republic of the Philippines
PHILIPPINE STATISTICS AUTHORITY

Quezon City, Philippines

PUBLIC BIDDING NO. PRO-003

October 2019

VOLUME 2: TECHNICAL SPECIFICATIONS

Fifth Edition
October 2016

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 About the Philippine Identification System

Republic Act No. 11055 (the "*Philippine Identification System Act*"), signed into law in August 2018, established the Philippine Identification System (or PhilSys) as a foundational identification system for all citizens and resident aliens of the Republic of the Philippines. According to R.A. 11055, the declared policies of the State with respect to the PhilSys are to: (a) promote seamless delivery of service; (b) improve the efficiency, transparency, and targeted delivery of public and social services; (c) enhance administrative governance; (d) reduce corruption and curtail bureaucratic red tape; (e) avert fraudulent transactions and misinterpretations; (f) strengthen financial inclusion; and (g) promote ease of doing business. Furthermore, the declared policies place importance on the deployment of a resilient digital system to secure the data collected and that the people's right to privacy, confidentiality and other basic rights are at all times upheld and protected. Implementing rules and regulations (IRRs) for R.A. 11055 and a 5-year PhilSys Implementation Plan were respectively approved by the Government of the Republic of the Philippines in October 2018 and March 2019.

1.2 About the Philippine Statistics Authority

The Philippine Statistics Authority (PSA) is the primary implementing agency for R.A. 11055 and has the mandate for overall planning, management and administration of the PhilSys, with technical assistance from the Department of Information and Communications Technology (DICT). This new responsibility builds on the PSA and its predecessors' historic mandate for maintaining the Philippines' civil registration and vital statistics (CRVS) system and recognizes the critical link of the integrity and sustainability of PhilSys with the continuous registration of births, deaths, marriages and other vital events. The PhilSys Policy and Coordination Council (PSPCC), chaired by the Secretary of the National Economic and Development Authority (NEDA) and co-chaired by the National Statistician and Civil Registrar-General PSA and Undersecretary of the Department of Budget and Management (DBM), formulates policies and guidelines to ensure effective coordination and implementation of the PhilSys.

1.3 Procurement of Main Components of the PhilSys

In the interest of promoting cost-efficiency, interoperability, specialization by bidders, exchangeability, and full ownership of the PhilSys and its data, the PSA has decided to procure the main components of the PhilSys separately in four major blocks, namely: (a) Supply, Delivery and Managed Services of 5,000 Registration Kits for the Philippine Identification System (PhilSys) (awarded in August 2019); (b) Supply, installation, support and maintenance of Automated Biometric Identification Systems (ABIS) for Philippine Identification System (PhilSys); (c) Consultancy Services as System Integrator for the Philippine Identification System (PhilSys); and (d) Supply, Delivery and Managed Services of the personalization and distribution of PhilID cards. Furthermore, pre-personalized PhilID cards will be provided by the Bangko Sentral Ng Pilipinas (BSP), which will carry out its own procurement.

1.4 Purpose of this Term of Reference

Bidders are invited to submit Proposal Information and Cost Quotations to the PSA for the provision of Supply, installation, support and maintenance of Automated Biometric Identification Systems (ABIS) for Philippine Identification System (PhilSys). Proposals should set forth an automated solution to the specific applications listed herein, identify the operating environment, hardware and software needed to run the systems, describe an implementation approach and timeline, and recommend an appropriate approach to training and implementation services. The PSA is committed to selecting a Bidder for 5-year contract from issuance of Notice to Proceed (NTP) and conducting this procurement in an open and competitive manner in full compliance with appropriate regulations and policies.

2. Background

The Philippines' economy has been booming since 2010 and one of the best performers in East Asia, with average annual growth of over 6%. However, over 20% of the population lives below the national and international poverty line. The Government has adopted AmBisyon Natin 2040, a collective long-term vision for the country to become a prosperous middle-class economy without any poverty by 2040 with all Filipinos enjoying a life that is Matatag (strongly rooted), Maginhawa (comfortable) and Panatag (secure). To achieve this, AmBisyon Natin 2040 acknowledges a key role for technology and innovation, as well as the Philippines becoming a high-trust society.

The Philippines is one of the few remaining countries without a foundational identification system, beyond its civil registration system, and the only one in ASEAN. While the coverage of birth registration (93.5% of the entire population according to the 2010 Population and Housing Census) and some functional identification systems and registries (e.g. the PhilHealth registry with more than 90 million records and the Commission on Elections (COMELEC) voter registry with more than 55 million records or around 85% of eligible adults) are high, the overall identification landscape currently in the Philippines could be described as fragmented.

Without a platform for public and private sector service providers to authenticate the identity of their customers, identity proofing and authentication is typically carried out by requiring the presentation of several physical documents that must have matching demographic information and are compared by a human without the ability to easily validate information on the physical documents against the source registries. In many cases, this will also involve the submission of an actual copy of the customer's birth certificate, which must be obtained from PSA. Some functional identification systems and registries – notably the Unified Multi-Purpose ID (UMID) operated by the PSA, Social Security System (SSS) and Government Social Insurance System (GSIS), the voter registry, and the Alien Certificate of Registration Identification (ACR-I) card operated by the Bureau of Immigration – have made significant investments in technology to carry out their own deduplication and automated identity authentication functions, but these services are not offered to third parties.

Because of the manual and independent processes and systems described above, transactions in the Philippines are more expensive (in terms of direct and indirect costs, such as taking time off work to obtain physical documents), bureaucratic, time-consuming and exposed to identity theft and fraud risks than what they should be. Operators of functional identification systems and registries are also likely making needless duplicative investments in standalone systems for identity proofing and authentication instead of being able to depend on a foundational identification system as a public infrastructure, in the same way as roads and rails support physical mobility. Furthermore, no existing Government-operated identification system or registry can be used to do transactions online, which creates a fundamental barrier for moving Government services online and for building an inclusive and trusted digital economy.

The current situation also give rise to exclusion for some people to access services, such as banking and social services, which could be exacerbating inequality. The 2017 ID4D-Findex Survey found that 19% of the poorest 40% of the Philippine population aged 15 and older have been denied a Government service and 16% have been denied Government financial support for lacking identification, compared with 12% and 8% of the wealthiest 60%, respectively. The same survey found that 14% of Filipinos (without any differences by wealth quintile) have been denied financial services for lacking identification. While, as noted above, the aggregate of existing identification systems in the Philippines might have high coverage, none of the more "trusted" identification systems (i.e. with higher levels of assurance) – such as the UMID card, driving license, passport, ACR-I card – have coverage higher than 30% of the Philippines' population, primarily because of costs and eligibility requirements. On the other hand, a foundational identification system such as the PhilSys will make "trusted" identification accessible to all, and free for Filipinos.

Another consequence of the current situation is that it is challenging for Government back-end information systems to reliably share and exchange data because there is no ubiquitous unique identity that would allow the automated linking – with consent – of data about the same individual across systems. It would significantly improve the operations of social security and welfare programs, for example, if they were able to share and update data on their members and beneficiaries. Importantly, the Philippines is committed to tokenization and virtualization of a permanent unique identifier to protect privacy and prevent unwarranted correlation of data in cases of breaches and misuse.

Owing to the relatively high birth registration coverage and that it is well-institutionalized, the existing civil registration system (CRS) operated by the PSA offers a good asset on which to build the PhilSys and enhance its sustainability and integrity, including to enroll newborns in the PhilSys at the time of birth registration and to retire records in the PhilSys for deceased PSN holders. While actual registration of births, deaths and marriages are at the municipal/city level by Local Civil Registration Offices (LCROs) in a decentralized manner, the PSA is responsible for technical oversight and maintaining a digitized, searchable and central repository, as well as the issuance of authenticated certificates. Two key challenges that are relevant for the PhilSys are reducing the time for data to get from LCROs to PSA (currently 4-6 weeks) and increasing death registration (estimated in 2010 at 63%).

The Philippines introduced a general data protection law when R.A. 10173 (the "*Data Privacy Act*") was signed into law in 2012 with the declared policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. This law governs the processing of personal information including issues around consent, Government-controlled personal data, and enforcement including through the establishment of the National Privacy Commission (NPC). NPC has approved IRRs for the *Data Privacy Act* and several circulars.

It was against this backdrop that the Philippine House of Representatives passed House Bill 6221 in September 2017 and the Senate passed Senate Bill 1738 in March 2018. These bills were consolidated through a bicameral conference in May 2018 that led to R.A. 11055.

3. Objective of the PhilSys

As a foundational identification system, the objective of the PhilSys is to improve the lives of all citizens and residents of the Philippines by making access, delivery and administration of Government and private sector services easier, wider, cheaper, faster, more secure, and more responsive to people's needs. Towards this end, the design and implementation of the PhilSys will ensure that the people's right to privacy, confidentiality and other basic rights are at all times upheld and protected.

3.1 Roles

The PhilSys will have two basic roles:

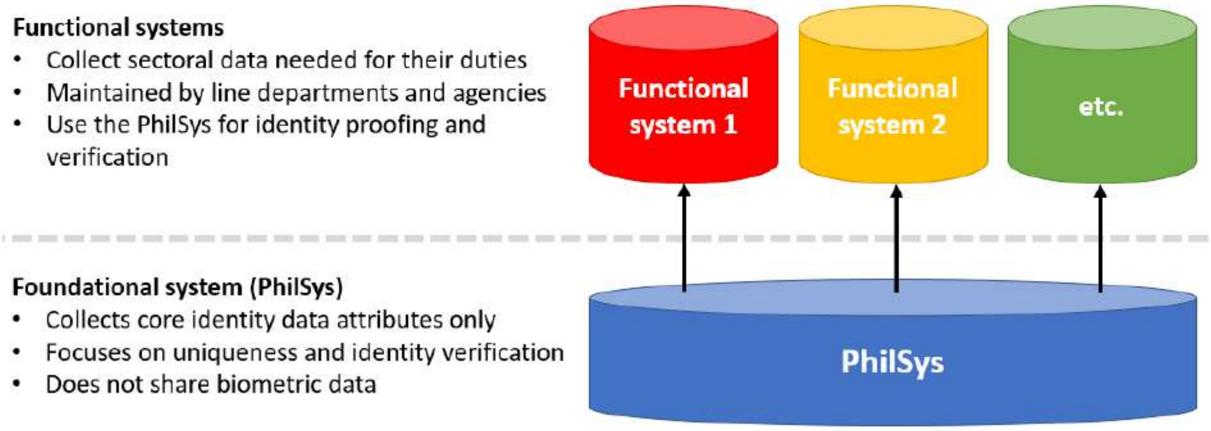
1) Creating a unique and secure digital legal identity for each PhilSys Number (PSN) holder; and
2) Allowing that digital legal identity to be controlled by the registered person and reliably verified both in-person and online for both Government and private sector transactions.

By simplifying the PhilSys to these two basic but important roles, the intention of the Government of the Philippines is to build an interoperable platform and public infrastructure that can reach scale more quickly and cost-efficiently, taking advantage of relevant emerging digital technologies. Minimizing the data to be collected and managed by the PhilSys to core identity attributes that are useful for most day-to-day transactions is a deliberate measure to safeguard data protection and privacy.

3.2 Implications for functional identification systems and registries

The focus of the PhilSys, as a foundational identification system, on those two roles and on interoperability and minimization allows relying parties and operators of functional identification systems and registries to have the flexibility build and manage their applications (e.g. for authorization) on top of the PhilSys. To reduce duplication, the PhilSys may replace existing functional identification systems and registries that exclusively serve the purposes of identification and verification.

On the other hand, there are functional identification systems and registries that do more than this (i.e. authorization) and have specific uses (e.g. a driving license proves that a holder is eligible to drive, a passport facilitate travel across international borders for the holder, and the UMID is used for a variety of benefits including as a cash card), which will not be replaced by the PhilSys. However, these systems will have their integrity and efficiency enhanced by basing their identity proofing and deduplication on the PhilSys (see following illustration).



Functional systems

- Collect sectoral data needed for their duties
- Maintained by line departments and agencies
- Use the PhilSys for identity proofing and verification

Foundational system (PhilSys)

- Collects core identity data attributes only
- Focuses on uniqueness and identity verification
- Does not share biometric data

Figure 1. Relationship between the PhilSys and functional identification systems and registries

4. Principles

The PhilSys will adopt and create international best practices in terms of inclusion, design, technology neutrality, performance, interoperability, cost-efficiency, data protection and privacy, and cybersecurity, In doing so, the PhilSys should observe the *Principles on Identification for Sustainable Development* as a guiding framework for maximizing its developmental impact while mitigating the risks (see box below).

Principles on Identification for Sustainable Development: Towards the digital age[1]

Inclusion: Universal coverage and accessibility

1. Ensuring universal coverage for individuals from birth to death, free from discrimination.
2. Removing barriers to access and usage and disparities in the availability of information and technology.

Design: Robust, secure, responsive and sustainable

3. Establishing a robust—unique, secure, and accurate—identity.
4. Creating a platform that is interoperable and responsive to the needs of various users.
5. Using open standards and ensuring vendor and technology neutrality.
6. Protecting user privacy and control through system design.
7. Planning for financial and operational sustainability without compromising accessibility.

Governance: Building trust by protecting privacy and user rights

8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.
9. Establishing clear institutional mandates and accountability.
10. Enforcing legal and trust frameworks though independent oversight and adjudication of grievances.

[1] The Principles have been developed and endorsed by 25 international organizations since 2017, including the World Bank Group, the Asian Development Bank, and UN agencies.

5. Envisaged benefits

The PhilSys will transform the Government and private sectors in the Philippines and make them more inclusive by digitalizing and automating the identification and verification of Filipinos and resident aliens, which are fundamental processes in accessing, delivery and administering all services that involve interacting with people.

The PhilSys will accelerate achievement of AmBisyon Natin 2040, the Philippines' long-term development vision, and the medium-term Philippine Development Plan (2017-2022) – and, in particular, its objectives of Malasakit (fostering trust in public institutions and among Filipinos), Pagbabago (inequality-reducing transformation) and Patuloy na Pag-unlad (increasing potential growth). It will also support implementation of priority initiatives of the Government of the Philippines including the Tax Reform for Acceleration and Inclusion (TRAIN) agenda, the Universal Healthcare Coverage Act, the National Strategy for Financial Inclusion (NSFI), the modernization of social protection and social security, the E-Government Master Plan (e-GMP), and efforts to strengthen the resilience and response of the Philippines to natural calamities. In doing so, the Philsys will also contribute to achieving the Sustainable Development Goals (SDGs), including targets related to ending poverty, universal health coverage, financial inclusion, and providing legal identity for all, among others.

The benefits of the PhilSys can be summarized as follows:

a) Making services more accessible: Because the PhilSys will itself be accessible to all Filipinos and resident aliens (with inclusive registration requirements) and its credentials will be accepted by themselves for most transactions, it will democratize access to financial, social welfare and security, health, education, and other Government services. This will be especially beneficial for remote and far-flung areas where, using technology, the PhilSys will reduce the costs for service providers and make it easier for service providers to offer more services either through the internet or using agents with equipment that can leverage the PhilSys, without depending on brick-and-mortar offices.

b) Promoting ease of doing business Because the PhilSys will provide a platform for Government and private sector service providers to identify and verify their customers in a digital and automated manner for both in-person and online transactions, it will reduce the paper-work, red-tape and bureaucracy required for processes that are currently often done manually, and therefore reduce administrative costs, time and risks. This will be especially beneficial for local and central Government services that are partially or completely made available through online channels (e.g. various registrations, renewals and permits).

c) Enhancing the integrity of services and reducing fraud: Because the PhilSys will uniquely identify each registered person at a national scale and allow that identity to be verified with a high-level of assurance, it will help eliminate instances of identity fraud (e.g. impersonation, theft and ‘ghosts’) and strengthen the integrity of functional identification systems and registries. This will be especially beneficial in social welfare and social security programs, where the PhilSys will contribute to ensuring that the right beneficiaries are receiving benefits (e.g. through verification and by linking the PSN to a beneficiary’s financial address), and the financial sector, where the PhilSys will contribute to addressing money-laundering risks and better credit history data.

d) Enabling and promoting participation and trust in digital government and the digital economy: Because the PhilSys will digitalize underlying processes for service access, delivery and administration and enable the verification of identity over the internet with a high-level of assurance (i.e. without the need for a face-to-face transaction), the PhilSys should enable a broader transition to digital, online citizen-centric service delivery by Government and the private sector, as well as create opportunities innovation and new products and services. This will be especially beneficial for allowing Government departments and agencies to exchange data, when consented or warranted, to improve the effectiveness and efficiency of their programs.

e) Empowering Filipinos and resident aliens with greater control over their personal data: Because the PhilSys will give PSN-holders the ability to determine who sees what data about them when carrying out transactions using the PhilSys, it will contribute to greater transparency and accountability for how data is used in the Philippines. Aside from promoting data protection, this will be especially beneficial as the Philippines’ digital economy grows and new products and services making use of data emerge.

f) Facilitating cross-border transactions: In the long-run, there is an opportunity for PhilSys credentials to be recognized in other jurisdictions both in-person and online, which could facilitate migration and trade. This will be especially beneficial for boosting the Philippines’ international economic competitiveness and in the context of the ASEAN Economic Community. The European Union’s eIDAS regulations offer a useful example and model in this regard.

6. Indicative Use Cases

The use cases of the PhilSys will support implementation of important initiatives of the Government of the Philippines including the Tax Reform for Acceleration and Inclusion (TRAIN) agenda, the *Universal Healthcare Coverage Act*, the National Strategy for Financial Inclusion (NSFI), the modernization of social protection and social security, the E-Government Master Plan (e-GMP), and efforts to strengthen the resilience and response of the Philippines to natural calamities.

In addition, Philsys can be a critical enabler for improving people's access to public and private services, and the efficiency and quality of these services. PhilSys offers a high level of assurance and adopts advanced security features and protocols to protect identities and personal data. This includes potential applications of ID across the following sectors: financial services, mobile and telecommunications, social protection, health care and insurance, education, agriculture, digital government, e-commerce and digital trade, taxpayer identification and revenue generation, voter identification, property ownership and transfer, civil servant payroll management and passport issuance and border security. (Refer to Appendix D, Section 6 for more details)

7. Stakeholders

A variety of actors are typically involved in establishing, maintaining, and using PhilSys throughout the identity lifecycle. In the context of PhilSys, important stakeholders include:

a) **Philippine Statistics Authority (PSA).** Lead implementing entity, including for development of the PhilSys (and procurement), communications, development of use cases, provision of authentication services, coordination of mass and continuous registration, managing and processing data, and handling grievances. Implementation of the PhilSys will be specifically by the PhilSys Registry Office, headed by a Deputy National Statistician (Assistant Secretary-level).

b) **PhilSys Policy and Coordination Council (PSPCC).** Formulating policies and guidelines to ensure effective coordination and implementation of the PhilSys, and ensuring compatibility of the respective technology infrastructure of different government agencies in order to comply with the requirements of PhilSys

   Members: Secretary, NEDA (Chair); National Statistician and Civil Registrar General, PSA (Co-Chair; Undersecretary, DBM (Co-Chair); Undersecretary, DFA; Undersecretary, DICT; Undersecretary, DOF; Undersecretary, DSWD; Undersecretary, DILG; Chairman, NPC; Deputy Governor, BSP; President and General Manager, GSIS; President and CEO, PhilHealth; President and CEO, SSS; Postmaster General, PHLPost.

c) **Individuals.** People are the center of ID systems. As both the subject of these systems and the end-users who use their identity to access rights and services, they have the right to consent, know, and exercise appropriate oversight over how their data is collected, used, stored, and shared. Understanding and responding to people's ID-related needs and concerns, protecting their privacy and personal data, and ensuring their agency throughout the identity lifecycle must be the starting point for building an ID system capable of furthering development goals.

d) **Governments.** Government agencies either rely on these foundational systems to interact with people and/or are themselves providers of functional ID systems. Finally, other government bodies play a regulatory role, provide oversight for ID systems, and may also be involved in implementing specific components or setting standards for technology and data formats. For instance, national cybersecurity agencies help ID agencies reduce cybersecurity risks and effectively respond to breaches, and ICT agencies may provide infrastructure or shared services, such as a datacenter, government cloud, or public key infrastructure (PKI).

e) **Private sector**. Private companies are developers, innovators, and suppliers of most ID system components and infrastructure. In addition, private companies may also be ID providers themselves, either as part of their core business or to identify and authenticate customers for other services, such as financial service providers and mobile operators. In addition, many private companies will rely on PhilSys to identify their customers (e.g. requiring government-issued credentials to open bank accounts, register SIM cards, or create credit reporting systems). Governments have also partnered with private companies to deliver forms of digital ID, such as mobile identity and digital authentication platforms, or to perform specific roles within a government-provided ID system.

f) **Civil society**. NGOs, community-based organizations, and other local groups are important partners for generating demand for ID and assisting people in obtaining the proof of identity they need to fully engage in economic, political, and social life. Civil society actors are also important potential partners in the implementation of PhilSys.

g) **International organizations and development partners**. Development and humanitarian agencies may provide support for PhilSys in the form of funding and technical assistance or be involved in establishing ID systems themselves to administer programs. For asylum seekers and refugees, for example, the 1951 Convention on the Status of Refugees (articles 25 and 27) provides that host States are responsible for registration, refugee status determination and providing IDs. However, in some cases, host States may not have the capacity or willingness to do so, and UNHCR may take on this responsibility in partnership with the host State and in line with its mandate established in international law.

h) Other stakeholders

Table 1. Stakeholders roles, core activities and primary goal

Role	Stakeholders	Core Activities	Primary Goal
“End-users” Subjects of the ID system	People Residents, citizens, beneficiaries, customers, etc.	• Register in ID system • Use credentials and proof of ID to access rights and services • Update data as needed • Exercise control and oversight over their data	• Accessibility • User-friendliness and control • Transparency and consent regarding data usage • Privacy & data protection
“ID providers” Issue and manage identities	Government agencies **Foundational:** PhilSys, local civil registrars, etc. **Functional:** electoral commission; social protection, health ministries; tax authorities, etc. **Private companies** PPP partners, mobile operators, financial service providers, online commercial platforms, private health providers, credit rating agencies, etc. **International organizations** UNHCR, WFP, etc	• Register people in the ID system • Issue and manage credentials • Manage and update identity information • Provide authentication/verification services at different levels of assurance • Raise awareness, conduct public consultations, and redress grievances	• Create accurate, trusted identities • Deliver services efficiently and effectively • Protect data against misuse and breaches • Prevent fraud • Reduce operating costs
“**Relying parties”** Rely on ID systems provided by others to identify/verify/ authenticate end users	**Government agencies** Passport office, electoral commission, tax authorities, social protection agency, etc. **Private companies** Mobile network operators, financial service providers, online commercial platforms, private health providers, credit rating agencies, etc	• Use platforms, credentials, and services of ID providers to authenticate and/or verify the identity of end-users • Authorize people to access specific rights or services	• Identify and authenticate people with appropriate level of assurance for transaction • Deliver services efficiently and effectively • Prevent fraud • Reduce operating costs

Role	Stakeholders	Core Activities	Primary Goal
“Enablers” Support the development, implementation, and oversight of the ID system	**Regulatory bodies** Government oversight and enforcement agencies	• Promulgate and enforce regulations and trust frameworks related to ID	• Data protection and privacy • Consistent identity management • Accountability
	Standard setting bodies and trust frameworks Government and international organizations, private identity organizations and associations	• Provide technical and data standards • Build trust • Support information security and cybersecurity	• Build trusted ID systems that are vendor and technology neutral • Facilitate interoperability • Establish trust between identity stakeholders
	Development and local partners Donor agencies, NGOs, community-based organizations	• Provide funding and technical assistance for ID system design and implementation • Assist people will accessing and using ID systems and related services • Advocate for inclusive and trusted ID systems	• Support client goals • Build local capacity • Ensure accountability to users

8. Key features of the PhilSys

8.1 Eligibility for registration

The PhilSys is accessible to all Filipino citizens inside and outside of the Philippines as well as resident aliens, defined as non-citizens who have established residence in the Philippines for a period of aggregate of more than 180 days. The PhilSys will cover all age groups.

8.2 Data collected

Pursuant to R.A. 11055, the following data will be collected in the PhilSys and kept in each registered person’s record:

a. Demographic data (collected at all ages)
   i. Full name (mandatory)
   ii. Sex (mandatory)
   iii. Date of birth (mandatory)
   iv. Filipino or Resident Alien (mandatory)
   v. Blood type (mandatory)

vi. Permanent address (mandatory)
vii. Present address (optional)
viii. Mobile number (optional)
ix. Email address (optional)
x. Marital status (optional)

b. Biometric data (collected at age 5 and re-collected at age 15)
i. Facial image (mandatory, subject to exceptions)
ii. 10 fingerprints (mandatory, subject to exceptions)
iii. 2 iris scans (mandatory, subject to exceptions)
iv. If necessary, other identifiable features of an individual as may be determined in the IRRs (this is not part of the scope of this PBD)

c. Record history / Meta data (collected at all ages)
i. Place of registration (mandatory)
ii. Date and time of registration (mandatory)
iii. Registration operator (mandatory)
iv. Scan of the registration form (mandatory)
v. Scan of supporting documentation for registration (mandatory)
vi. Modifications made to the record (mandatory)
vii. Date and time of modifications (mandatory)
viii. Scan of application form for modifications (mandatory)
ix. Scan of supporting documentation for modifications (mandatory)
x. Date and reasons of issuance, reissuance and cancellation of the PhilID
xi. Reasons for the omission of any mandatory data (mandatory)
xii. Details of authentication requests, including the date, requesting entity and response provided by the PhilSys (mandatory, period of retention defined by the registered person)
xiii. Disclosure, conveyance, dissemination, publication and use of information by third parties (mandatory)
a. Other relevant information regarding the registration, modification and authentication of personal information of a registered person under R.A. 11055

8.3 Registration channels and processes

The PSA will offer registration and other PhilSys related services to Filipino citizens inside the Philippines and resident aliens by establishing: (a) Fixed Registration Centers in the premises of government agencies and GOCCs (e.g. PSA Regional and Provincial Offices, LCROs, and branches of PhilHealth, PHLPost, SSS and GSIS); and (b) Mobile Registration Centers in public spaces, in coordination with LGUs. The PSA will provide all necessary software, hardware and staff, and will set standards on the physical environment of Fixed Registration Centers and Mobile Registration Centers. The terms of the use of premises and public spaces will be negotiated with each partner through a Memorandum of Agreement (MOA).

The PSA will coordinate with the Department of Foreign Affairs (DFA) to offer registration and other PhilSys related services to Filipino citizens outside of the Philippines at overseas Philippine missions. The PSA will provide all necessary software and hardware, and will set standards on the physical environment of DFA-based PhilSys registration channel. DFA staff will be trained by PSA to carry out registration and other PhilSys related services.

By 2022, newborn babies should be automatically registered in the PhilSys at the same time as their birth registration.

8.4 Credentials

The 12-digit PhilSys Number (PSN) is the primary PhilSys credential for each registered person. It is unique and randomized.

To maintain privacy of the registered person and security of the PSN as a permanent unique identifier – as well as to give registered persons better control over their identity – the PSN is NOT to be printed in a human-readable format on the PhilID card and there are various derivatives of the PSN to facilitate authentication and unique identification.

1. **PhilID Card Number** (printed on the PhilID card): An *Alyas* PSN (see below) that is human-readable on the face of the PhilID card and valid for the period that the PhilID is valid (i.e. until it is replaced or reported as lost or stolen).
2. ***Alyas* PSN (temporary):** A random unique number that is a derivative of the permanent PSN, which is **generated by the PhilSys for a registered person until they generate a new *Alyas* PSN** (i.e. to conceal their permanent PSN and PhilID Number).
3. **PSN Token (for back-end seeding in other systems):** A random unique number that is a derivative of the permanent PSN, which is generated by the PhilSys for a relying party following a successful authentication, for the purposes of seeding that number in the relying party’s registry. Multiple PSN tokens, for each relying party, will be active at the same time for a registered person

The secondary PhilSys credentials are the:

4. **PhilID**: A simple plastic card with overt security features used primarily as a physical medium to convey the PhilID Number, registered demographic data and facial image, and a Quick Response (QR) barcode encoded with a digitally-signed facial image (for offline authentication) and best finger detection (BFD) labels for the two highest quality fingerprints in the PhilSys (for online authentication). Rather than incorporate expensive covert or forensic physical security features, the PhilID card will primarily draw its security from online authentication by the PhilSys.

5. **Mobile PhilID**: A mobile-phone version of the PhilID. The timeline for implementation and precise form (e.g. using the SIM card and/or a smartphone) are to be determined at a later date.

8.5 Methods of authentication

The following methods of authentication will be offered by the PhilSys:

1. **PhilID taken at face value:** For low-risk transactions, the relying party will review the PhilID or Mobile PhilID and compare the information (e.g. the facial image) with that of the bearer as well as examine the quality of the card and overt security features of the PhilID.
2. **Fingerprint, iris or facial image biometric authentication:** A PSN, PSN Token or *Alyas* PSN and an image of a fingerprint, iris and/or face of a person claiming an identity are captured by a registered relying party and this data is transmitted through a secure connection to the PhilSys, templated and compared with templates of the same biometric(s) in the record of the corresponding PSN, PSN Token or Virtual PSN. Based on the matching threshold, a positive or negative response is returned to the relying party.
3. **One Time Password (OTP) by SMS:** A PSN, PSN Token or Virtual PSN of a person claiming an identity is captured by a registered relying party and this data is transmitted through a secure connection to the PhilSys for the PhilSys to send a temporary 6-digit number by SMS to the mobile number in the record of the corresponding PSN, PSN Token or Virtual PSN. The person claiming the identity should provide the 6-digit code to the relying party, which is transmitted through a secure connection to the PhilSys to match against the 6-digit code it sent. A positive or negative response is returned to the relying party.
4. **Electronic Know Your Customer (E-KYC):** Only in circumstances enabled by law and consented by the registered person (e.g. customer due diligence regulations in the financial sector or applying for a passport or social benefit), the relying party may receive through secure transmission specific demographic data and the facial image from the PhilSys following a successful biometric and/or OTP authentication.
5. **Mobile PhilID:** The methods of authentication using the Mobile PhilID will be determined at a later stage, drawing on the experiences of implementing existing methods of authentication.

8.6 Data protection, privacy and cybersecurity

The security and integrity of Personally Identifiable Information (PII) in the PhilSys is the highest priority. Therefore, the design and implementation of the PhilSys will emphasize data protection, cybersecurity and the privacy of the people whose data it holds. Furthermore, the PhilSys will give registered persons – as data subjects – ultimate control over their personal data.

These outcomes will be achieved through a privacy-by-design and information security-centric approach in strict compliance with safeguards provided for by the *Data Privacy Act* and the *Philippine Identification System Act,* and adoption of cutting-edge privacy enhancing technologies.

Key features and principles of the PhilSys in this context include:

a. data collection as prescribed by R.A. 11055;
b. focusing on authenticating registered persons through a binary “yes/no” approach;
c. only disclosing information when consented by the end-user;
d. enabling tokenization of the permanent PhilSys Number (PSN);
e. strict access controls and security for data at capture, exchange and storage stages;
f. providing a self-service hub for transparency to and control by registered persons, including to see who has accessed their data, when and why, to lock/unlock their record for authentications, and to choose the period that authentication transactions logs will be retained;
g. tamper-proof logging of transactions for auditing and traceability purposes;
h. regular security audits of PhilSys software, hardware and processes;
i. making freely- and easily-available grievance mechanisms.

In recognition of the PhilSys being a national strategic asset, the PSA will implement the PhilSys solution in accordance to all relevant provisions of the National Cybersecurity Plan (NCSP) 2022.

8.7 Interoperability and technology neutrality

The Government of the Philippines is committed to building the PhilSys as an interoperable platform that is fully owned and operated by the Government aligned to the Philippine eGovernment Interoperability Framework (PeGIF). Technology neutrality is important for making components of the PhilSys exchangeable and upgradeable, when the needs arise.

As part of this, the PhilSys will adopt international open standards and open source software (where appropriate) and ensure that procurement and contract management will reduce risks of technology and vendor lock-in or dependency.

PSA will use the Modular Open Source Identity Platform (MOSIP) as its identity platform for the PhilSys solution (see Appendix A).

8.8 High-level functional architecture

The following figures show the PhilSys high-level functional architecture:

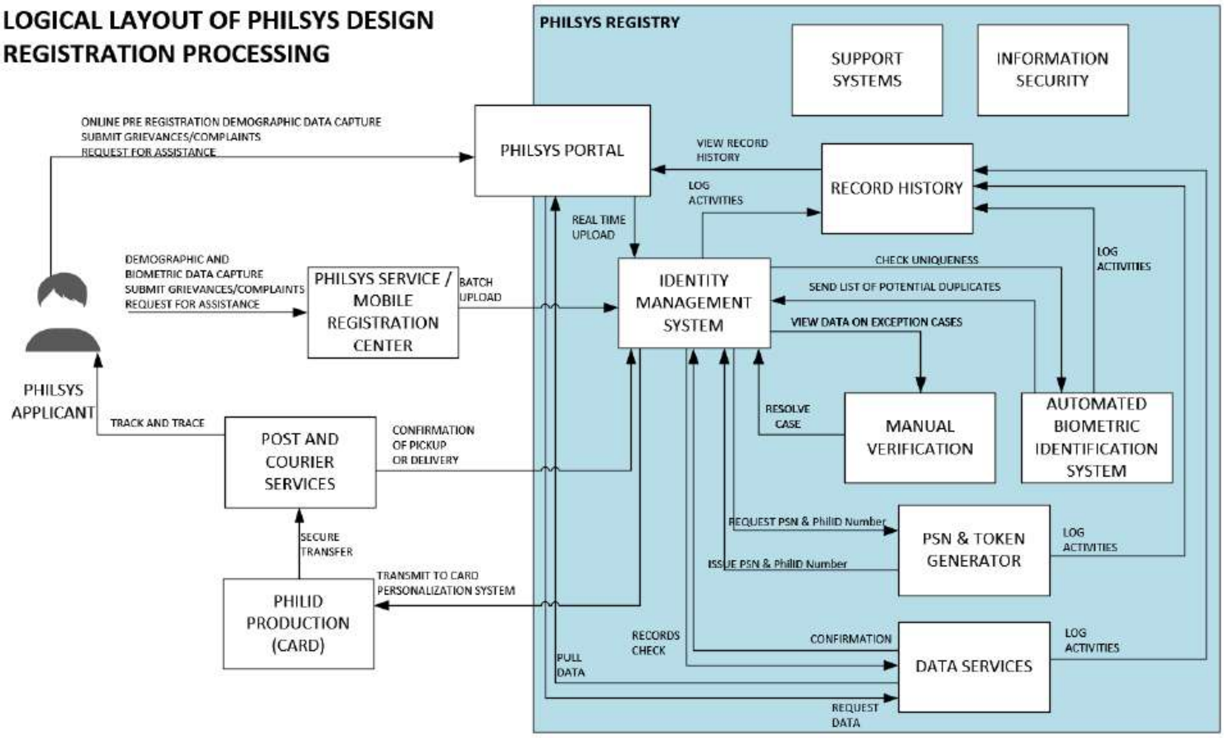

LOGICAL LAYOUT OF PHILSYS DESIGN REGISTRATION PROCESSING
PHILSYS REGISTRY
SUPPORT SYSTEMS
INFORMATION SECURITY
ONLINE PRE REGISTRATION DEMOGRAPHIC DATA CAPTURE
SUBMIT GRIEVANCES/COMPLAINTS
REQUEST FOR ASSISTANCE
PHILSYS PORTAL
VIEW RECORD HISTORY
LOG ACTIVITIES
RECORD HISTORY
REAL TIME UPLOAD
DEMOGRAPHIC AND BIOMETRIC DATA CAPTURE
SUBMIT GRIEVANCES/COMPLAINTS
REQUEST FOR ASSISTANCE
PHILSYS SERVICE / MOBILE REGISTRATION CENTER
BATCH UPLOAD
IDENTITY MANAGEMENT SYSTEM
CHECK UNIQUENESS
SEND LIST OF POTENTIAL DUPLICATES
VIEW DATA ON EXCEPTION CASES
LOG ACTIVITIES
PHILSYS APPLICANT
TRACK AND TRACE
POST AND COURIER SERVICES
CONFIRMATION OF PICKUP OR DELIVERY
RESOLVE CASE
MANUAL VERIFICATION
AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM
SECURE TRANSFER
REQUEST PSN & PhilID Number
ISSUE PSN & PhilID Number
PSN & TOKEN GENERATOR
LOG ACTIVITIES
TRANSMIT TO CARD PERSONALIZATION SYSTEM
PHILID PRODUCTION (CARD)
RECORDS CHECK
CONFIRMATION
LOG ACTIVITIES
PULL DATA
DATA SERVICES
REQUEST DATA

Figure 2. Logical Layout of PhilSys Design Registration Processing

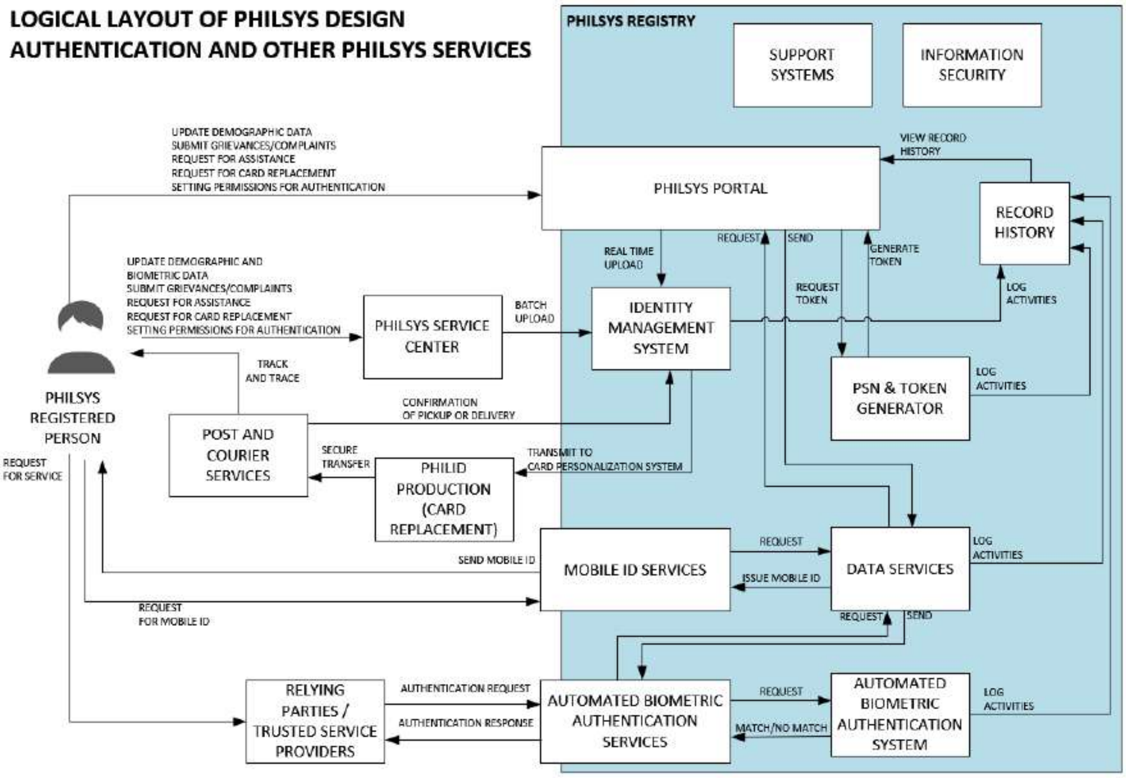

LOGICAL LAYOUT OF PHILSYS DESIGN AUTHENTICATION AND OTHER PHILSYS SERVICES
PHILSYS REGISTRY
SUPPORT SYSTEMS
INFORMATION SECURITY
UPDATE DEMOGRAPHIC DATA
SUBMIT GRIEVANCES/COMPLAINTS
REQUEST FOR ASSISTANCE
REQUEST FOR CARD REPLACEMENT
SETTING PERMISSIONS FOR AUTHENTICATION
VIEW RECORD HISTORY
PHILSYS PORTAL
RECORD HISTORY
REQUEST
SEND
GENERATE TOKEN
REAL TIME UPLOAD
UPDATE DEMOGRAPHIC AND BIOMETRIC DATA
SUBMIT GRIEVANCES/COMPLAINTS
REQUEST FOR ASSISTANCE
REQUEST FOR CARD REPLACEMENT
SETTING PERMISSIONS FOR AUTHENTICATION
PHILSYS SERVICE CENTER
BATCH UPLOAD
IDENTITY MANAGEMENT SYSTEM
REQUEST TOKEN
LOG ACTIVITIES
TRACK AND TRACE
PSN & TOKEN GENERATOR
LOG ACTIVITIES
PHILSYS REGISTERED PERSON
CONFIRMATION OF PICKUP OR DELIVERY
POST AND COURIER SERVICES
SECURE TRANSFER
PHILID PRODUCTION (CARD REPLACEMENT)
TRANSMIT TO CARD PERSONALIZATION SYSTEM
REQUEST FOR SERVICE
SEND MOBILE ID
MOBILE ID SERVICES
REQUEST
ISSUE MOBILE ID
DATA SERVICES
LOG ACTIVITIES
REQUEST FOR MOBILE ID
REQUEST
SEND
RELYING PARTIES / TRUSTED SERVICE PROVIDERS
AUTHENTICATION REQUEST
AUTHENTICATION RESPONSE
AUTOMATED BIOMETRIC AUTHENTICATION SERVICES
REQUEST
MATCH/NO MATCH
AUTOMATED BIOMETRIC AUTHENTICATION SYSTEM
LOG ACTIVITIES

Figure 3. Logical Layout of PhilSys Design Authentication and other PhilSys Services

8.9 Architecture Principles

The architecture principles adopted for the PhilSys are as follows:

- **Scalability & Modularity:** The system should be scalable in-line with the rollout plan for all IT Infrastructure. It should be modular for each business service, catered by a separate module thus ensuring separation of transactions. As the system would increase the coverage, new authentication agencies would start using the system. Therefore, the system should be designed in such a way that required hardware can be augmented into the Data Center in an incremental manner on a need basis with minimal service downtime. Data partitioning/sharing should be leveraged to ensure that system can scale with growth in data. Application scalability should be ensured using Open API's and asynchronous design in logic allowing each resource to do its job, loosely coupled through a messaging layer. Use of Open API's also provide a layer to integrate application components from different vendors addressing issues related to single vendor.
- **Security by Design:** The system should have the ability to secure data from thefts, tampering, unwanted modifications, network attacks, and other security threats. Use of Hardware Security Module (HSM) Technologies, Public Key Infrastructure (PKI) based encryption, hashing algorithms, strong physical security, access management, stringent audits, non-repudiation, 24x7 Network Operations Center (NOC) and Security Operations Center (SOC) monitoring, data encryption should be strongly enforced to make system robust and secure from any data thefts. Further, only necessary and minimal information would be shared after the consent by the end-user for using the online authentication service of PhilSys.
- **Manageability & Upgradeability:** The system should have the ability for end-to-end management of the components to ensure health of the system and adherence to service levels. For complete lights out operation, all layers of the system such as application, infrastructure must be managed through automation and proactive alerts rather than manual management. The entire application must be architected in such a way that every component of the system is monitored in a non-intrusive fashion (without affecting the performance or functionality of that component) and business metrics are published in a near real-time fashion. This allows data center operators to be alerted proactively in the event of system issues at a granular level. Application architecture shall also allow specific components to be watched very closely through a component level debugging scheme. The system should have the ability to seamlessly upgrade services, components, and modules without affecting services.
- **Flexibility:** The system should be designed for extensibility for specific features using a Metadata based approach, Business Rules and/or Service Oriented Architecture (SOA) based open APIs. Open Architecture adopting open standards followed by multiple vendors would mean that the system can work with hardware and software procured from different vendors at different times. Open API's would enable the applications to be developed in such a way that the applications can run from mobiles, smartphones, tablets, desktops and laptops. Further, open APIs create a layer that is vendor neutral allowing multiple vendor products and applications to

co-exist also enabling change of vendors whenever technology or scalability issues are encountered.

- **Cost Effective:** Low cost technology would be used to maximize benefits, avoid vendor locking, etc. Use of scale out architecture through horizontal scaling capability of hardware and data, use of open API's allowing different vendors to co-exist together would ensure low Total Cost of Ownership (TCO).
- **Use of Automation:** Automation would be adopted to minimize the cost of ownership especially in areas of testing, application & infrastructure monitoring, provisioning of new environments using virtualization technology and run book automation.
- **Performance & Availability:** Infrastructure and networks should be designed to support performance as per the agreed Service Level Agreements (SLAs). Each application should be tested to identify and mitigate performance issues. The potential performance bottlenecks need to be identified and cost-effective paths for performance improvements should be provided for these identified problem areas. The system infrastructure should be architected considering failover requirements and ensure, a single server or network link failure does not bring down the entire system. The platform solution should support effective disaster recovery.

9. Demand Capacity

The tables below provide the details of registration workload and age analysis of the citizens and residents proposed to be registered in the PhilSys. The estimated population of Philippines as per the census 2015 stands at 100.98 million. Whereas the estimated population by year 2022 based on the current growth rate is projected to be 110 million. It is understood that children below the age of 5 years will not be registered with biometric data. Hence, the net biometric registration works out to approximately 94 million. However, children crossing the age of year 5 and going to year 6 will be eligible for biometric registration. The workload is worked and shown in the tables below. Annual number of births is approximately 1.7 million, hence, on a base population of 94 million for biometric registration, it can be estimated that additional 1.7 million biometric registrations would be added to the base registration every year.

9.1 Volume analysis

A brief snapshot of the volumes of population of Philippines citizens is provided.

Table 2. Snapshot of the volumes of Philippine population

Parameter	Description	Sizing Estimations
Current Population	Population in 2015 (a)	100.98 million (Source: Census 2015)
Estimated Population	Estimated Population in 2022 (b)	110 million
Population below 5 years	Estimated Population in 2022 (c)	16 million
Philippines Citizens outside country	Estimated population (d)	10 million
Adult Population for Biometric registration by July -2023	(d) = (b) – (c)-(d)	84 million
Population Growth Rate (%)	Average annual population growth rate (2010-2015)	1.72%
Crude Birth Rate (%)	Number of Births in 2018	1.52%
Crude Death Rate (%)	Number of Deaths in 2018	0.55%
Average No. of Births	Annual number of births in the period 2020-2030	1.7 million to 1.8 million per annum

Parameter	Description	Sizing Estimations
Average No. of Deaths	Annual number of deaths in the period 2020-2030	0.6 million per annum
Estimated registration of Citizens outside Philippines	Annual %	20% of 10 million

9.2 Estimates of registration volume

The estimates of registration volumes are given below. The overall registration target is 110 million registration of citizens and residents of Philippines. However, some facts need to be noticed while undertaking the capacity planning. These are that:

(i) The count of population below 5 years is approximately 16 million;

(ii) The count of Overseas Filipinos Workers is approximately 2.3 million in 2018; and

(iii) These citizens at (i) and (ii) above shall come for Registration in a phased manner.

Table 3. Estimates of Registration volume

Parameter	Description	Sizing Estimations
Pilot registration	Including biometric capture	1 million – Sept. 2019 to June 2020
Registration for de-duplication and PSN allotment	84 % population	By July 2022
Registration Target for de-duplication and PSN allotment	Entire Population of Philippines	110 million, by end 2022 and beyond
Continuous registration of Children	Population comprising of 0-4 age group	15 % of population of the base year of 2015 census age group 0-4
Continuous Registration of Citizens outside Philippines	10% of total population	20% per annum
Existing PSN Deactivations	After PSN generation (due to deaths)	Annual Death Rate of 0.6%
Biometric Updates	At 5 years	2.2 million per annum (population of 4-year-old children)

Parameter	Description	Sizing Estimations
Biometric Updates	At 15 years	2.2 million per annum (population of 14-year-old children)
Biometric Updates of All Population	Others (e.g. PhilID replacements)	25 million per annum (25% of the population)
Demographic Updates	Change in demographic details	5.5 million per annum (5% of Population)

10. Biometric Solution

10.1 ABIS solution design principles

The following are the key design principles for the biometric solutions that shall be deployed/developed by the BioSP:

a. **Modularity**: The design must allow for replacement and updating of various components deployed without any impact on the other components. The components should be as granular as possible. For example, the registration infrastructure and authentication infrastructure are decoupled and will use separate databases.

b. **Standards**: Use of standards prescribed by PSA in this PBD is mandatory. All interfaces to the outside systems must be based on current industry standards adopted by PSA for maximum interoperability.

c. **Avoidance of vendor lock-in**: In the area of 1: N biometrics deduplication, proprietary algorithms and data representations are perhaps required to achieve performance and accuracy requirements of the PSA. The system should be designed in such a manner that these algorithms and data representation form a part of the ABIS, and the entire ABIS or a sub-system can be replaced without any impact on the other components of PhilSys. All proprietary data formats needed for 1: N deduplications shall not be exposed outside of the ABIS.

d. **Risk Mitigation**: Philippines is proposing to undertake biometric data collection of the entire population and biometric authentication for service delivery. As the quality and availability of biometric measures across the population is currently not known, high quality ABIS features and functionality for de-duplication and strategy to achieve performance targets must be incorporated in the design to ensure quality.

e. **Universality:** To support scalability and inclusiveness of the solution, three biometric profiles will be collected fingerprint, face and iris. Fingerprint images will be collected in slap mode (4x4x2), both Iris images will be collected and Facial image will be full frontal.

f. **Security:** Biometric Solution must be secure and must comply with safeguards provided for by the *Data Privacy Act* and the *Philippine Identification System Act,* and adopt cutting-edge privacy enhancing technologies. For example, all personal information stored on a permanent storage media must be encrypted.

g. **Service Oriented Architecture (SOA):** The ABIS components shall follow SOA principles and provide specific services using well-defined interfaces.

h. **Isolation**: ABIS will not have access and should not try to access any network resources except the resources referenced by the URLs provided through the API.

i. **Connectivity with IDMS** (ID Management System): The ABIS shall be able to process the data delivered by IDMS and should be able to return ABIS results to IDMS.

10.2 Biometric standards

The biometric solution should be compliant with the standards mentioned in the table given below:

Table 4. Biometric Standards

S. No.	Description	Proposed Standard
1	Fingerprint Minutiae (Authentication)	ISO 19794-2
2	Fingerprint Image	ISO 19794-4
3	Iris Image	JPEG 2000
4	Iris Image (Authentication)	ISO 19794-6
5	Face Image Data	ISO 19794-5
6	Face Image Compression	WSQ

10.3 Interoperability Standards

The ABIS and the Multimodal SDKs for PhilSys must generate standard, interoperable ISO format biometric templates. The fingerprint encoding algorithm proposed must have participated to at least one recent MINEX benchmark organized by the US NIST (National

Institute of Standard and Technology). This must be substantiated by an official report as part of the BioSP's Technical Proposal, and will be subject to evaluation.

10.4 System Architecture Requirements

The Biometric architecture requirements are given below. The ABIS solution at a minimum should meet the below mentioned requirements.

Table 5. Biometric Architecture Requirements

S. No.	Dimension	Requirements
1.	Scalability	Dynamic or rule-based ability to scale the system within servers, across servers without inherent bottlenecks and code changes, and ability to scale at data centers. • The system shall have ability to scale dynamically depending upon the load without bringing the system down. • The system shall have ability to load balance across servers. • The system should not have a single point of failure and inherent design bottlenecks that stops it from scaling.
2.	Security	Ability to secure all data from thefts, tampering, unwanted modifications, network attacks, and other security threats using physical and logical measures as per PSA specified security and data protection policies. The solution shall support: • Storing of primary data in encrypted fashion • secure communication protocols while communicating with external components • communication with only the IDMS • only authorized users should be able to access the data • changing the encryption schemes dynamically and periodically, if required • integration with external security components • configuring Access Control Lists • running services without super user privileges Auditing all access and modifications (by any user) to biometric data and make these audits trails available. Audit trail should be stored as per the archival procedures of PSA.

S. No.	Dimension	Requirements
3.	Interoperability	Ability to interoperate with other systems/services within and across any open interfaces and ability to continually re-factor and/or replace specific components without affecting rest of the system. The solution shall support: • open standard protocol-based communication • command line-based interface for interaction • re-factor / replace individual services without bringing the whole system down. • all APIs and interfaces defined by PSA as part of biometric vendor integration specifications. • integration from external management products such as systems management, network management, and other tools.
4.	Manageability	Ability to manage end-to-end solution and its components to ensure solution health and SLAs using external data center management tools. The solution shall support: • monitoring of its services using management tools; • ability to bring its services up and down; • monitoring its CPU/network/storage utilization; • monitoring the response time of individual services; • maintenance of its services without affecting client access; and • continuous availability of its services even during regular management activities.
5.	Availability	• The solution shall be available at least 99.5% as measured over the course of each calendar month (“Service Period”). “Available” means the solution is available and operable for access and use by the PSA and its Authorized Users over the Internet in conformity with the Contract. The solution is not considered Available in the event of a material performance degradation or inoperability of the solution in whole or in part.
6.	Upgradeability	Ability to seamlessly upgrade services, components, and modules without affecting services and open interfaces. Ability to upgrade without bringing down the solution. The solution shall support: • upgrade of individual modules without bringing the solution down; • backward compatibility; • upgrading using third party software delivery systems; • reverting to original configuration in case of an upgrade failure; • reverting to old configuration after a successful upgrade.

S. No.	Dimension	Requirements
7.	Installation and Configuration	The solution shall support: • connectivity with IDMS • installation and configuration without super user privileges on the whole solution
8.	Maintainability	The solution shall have the: • Ability to continuously maintain, enhance, re-factor solution without breaking other parts. • Ability to support maintenance, enhancement and refactoring the solution without breaking other parts
9.	Open Standards based	Technology choices should be based on open standards and widely adopted frameworks as long as they meet the needs of the system. The solution shall have: • technologies that are based on open standards • frameworks that are widely adopted • can process inputs in open standard format (see Table 4. Biometric Standards) • can generate outputs in open standard format (see Table 4. Biometric Standards)
10.	Administration	Ability to administer the ABIS during its operation. The solution should support: • ability to administer the solution with minimal user intervention with well-defined user interfaces and access policies • easy to use operator interface • command line for all administrative operations • role-based administration • automation of administrative tasks
11.	Logging and Reporting	Ability to log and report the health of the solution at a sub-system level state. It shall also log different events encountered by the sub-system. The solution shall have: • The ability to log and create reports to know the current state of the solution and improve the quality of different services offered by the solution • a mechanism to configure the logging level for different modules • a mechanism to rotate the logs based on policies • a mechanism to search through the logs with different filters • a mechanism to integrate with alert management tools • a mechanism to generate reports on various performance indicators • a mechanism to integrate with external reporting tools

S. No.	Dimension	Requirements
12.	Storage Access	Ability to use heterogeneous storage environments. The solution should: • work in heterogeneous storage environments with data partitioned across servers • function with storage getting provisioned using heterogeneous storage technologies like NAS/SAN/DAS • access only the data to which it was given access • support data partitioned across different servers
13.	Backup / Restore	Ability to provide backup and restore of the persistent data. The solution should have: • capability to backup and restore the data generated in the solution • ability to backup the data generated in the solution while continuing to process service requests. • allowance for incremental/differential/full backup methods • ability to take backup of application consistent with the data • proper functioning after a restore operation

10.5 Biometric Components

The PhilSys intends to deploy a Biometric Solution (ABIS) for 1:N identification. The minimum components of the proposed ABIS to be deployed are listed below:

1. ABIS Biometric Matcher
2. Middleware
3. ABIS database of biometric images and templates
4. Multimodal Software Development Kits (SDKs)
5. Manual Adjudication
6. Administrative tools

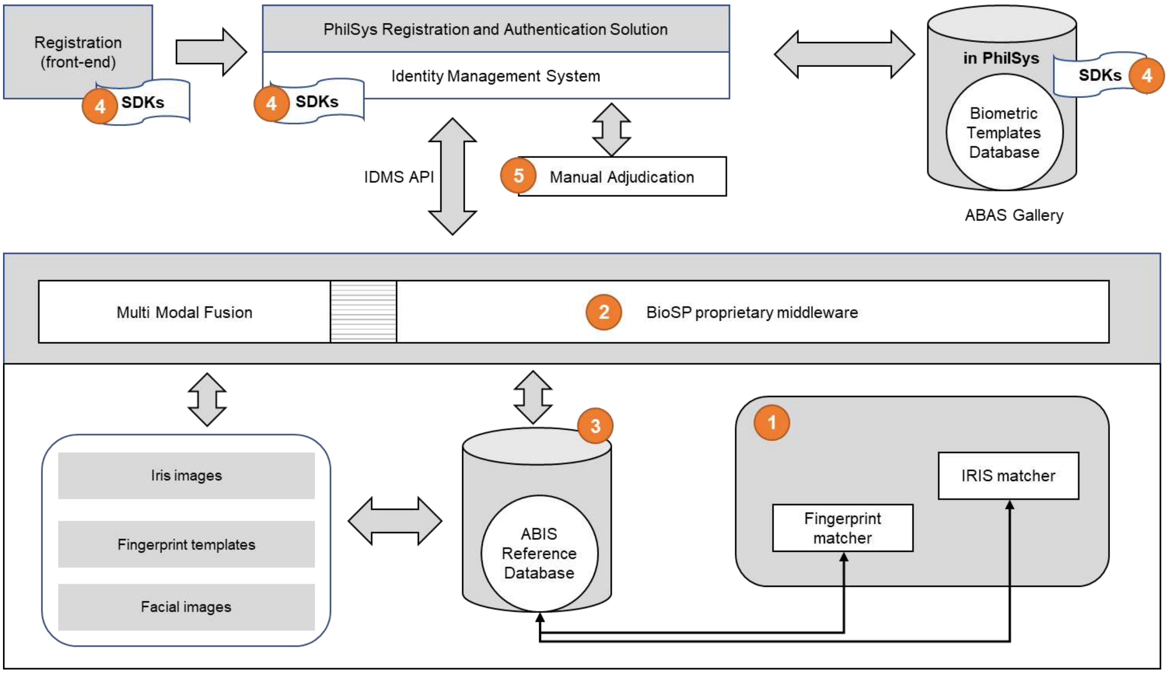


Figure 4. Biometric Solution Logical Diagram identifying the components

10.6 ABIS Biometric Matcher

The figure above shows that ABIS should provide biometrics de-duplication functions. It should communicate with the PhilSys through the API. ABIS shall maintain its own database of indexed biometric references (called the ABIS database). This ABIS database is separate from PhilSys database that is outside of ABIS and not accessible to ABIS.

ABIS is an essential integrated component within overall PhilSys solution. The system shall have the functionality of 1:N deduplication with reference to fingerprint and iris biometric modalities captured during registration with the existing biometric gallery in the ABIS solution. ABIS is a multi-modal biometric matching solution, which shall use biometric modalities like fingerprint and iris captured during the registration. For every new record, the solution shall perform 1:N matches to ensure that there are no duplicates in the system.

- For unique records, the ABIS will send back the results to IDMS for PSN generation.
- The registration records within matching threshold levels that are labelled as potential duplicates shall undergo manual adjudication. The results of the manual adjudication will be sent to the IDMS. After the completion of 1:N matching and successful biometric manual adjudication, the manual adjudication module will send back the results to IDMS for PSN generation or further manual verification of biometrics and demographics data.
- Registration records exceeding the sure match threshold level, shall not undergo manual adjudication but ABIS will send the sure match result information to the IDMS.

11. Functional and Technical Requirements

The ABIS at a minimum should meet the below mentioned functional and technical requirements.

11.1 Enrollment

a) **Insert**: This function is used to insert biometric data (templates) into the ABIS database without performing biometric matching. Obtain the biometric data for the given registration record, process the biometric samples as required by the biometric solution and store the templates in the ABIS database. The function will internally invoke segmentation, feature extraction and template generation.

b) **Identify**: This function is used to perform de-duplication and identification (in case of lost PSN of a registered person) across entire or sub-set of the database. It compares the query data for the supplied index against the entire reference database, sub-set of the database, and a set of supplied indices. Incoming query data samples always consist of images possibly cropped and loosely compressed. The function returns a candidate list of transaction numbers of potential duplicates above a threshold and associated comparison scores scaled on the interval based on the BioSP’s technical proposal.

c) **Delete**: This function is used to remove a record from the reference database. The removal need could arise for variety of reasons. This functionality will only be use upon approval of the PSA.

11.2 Management

Management related functions will be at two (2) levels of security and allow the ABIS component to be managed using programming interface. On the higher security level, the key required functions include:

a) **Shutdown**. The ABIS component is required to shut itself down.
b) **Clear**. The ABIS component is required to delete all the data from its reference database and clear all queues.
c) **Configure**. At the time of initialization, ABIS component is provided with vendor specific information to configure itself. The information will include operating characteristics.
d) **Pinging the system at the lower security level**. Additional functions required for system management, configuration, logging and reporting should be provided under the appropriate requirements.

11.3 Verification

Verify is a special case of Identify mentioned above where only 1:1 comparison is performed. The ABIS is sent a query consisting of a fingerprint and iris images and the record ID of the enrolment record to which the query is to be compared. A scaled comparison score and a “match/non-match” decision is always returned to IDMS. Fingerprint verification utilizing 19794-2-compliant templates will be done without use of proprietary extended data.

11.4 Data storage requirement

Persistent data including the reference database may be stored in industry standard database or in file system. In both cases, the BioSP should provide export tools to allow access to the data in situations including but not limited to change of vendor, database synchronization, backup, upgrade or maintenance. The exported data should be in industry standard format readable using open source tools and compliant to defined biometric standards (Table 4. Biometric Standards). ABIS should have necessary backup and restore functions for routine system administration.

A copy of the ABIS database will be stored in an industry standard database or file system existing at a separate location. Therefore, BioSP shall provide all necessary assistance for the same. The BioSP should be able to design a backup strategy compliant to the SLAs, as defined by PSA.

11.5 Logging and monitoring

Capability to log transactions at the component interface level should be implemented such that it allows dynamic starting and stopping of this transaction logging service. The level of logging should be controllable using a configuration parameter.

The audit system should be centrally managed and should be tamper-proof. The system should be able to capture before and after values from transaction logs, privileged user audits, raise alerts on suspicious activity. It should provide security facilities for role segregation within audit organization in terms of administrator, auditor etc. These audit logs should be kept as per the retention policy of the PSA. Until PSA retention policy is published, BioSP will retain all logs as specified in list below.

Audit and logging system should be scalable and should have the space to grow. The system should be flexible to accommodate new audit requirements in the future. The systems should comply at a minimum with the logs listed below.

11.5.1 ABIS Log

- Template generation Time
- Total time taken for multi modal matching process (in seconds)
- Matching algorithm throughput
- Matching scores of each matcher including fusion and the decision/results
- Percentage of automated identification vs. manual intervention rate
- Above parameters should be recorded along with record information, time of access, and the operator name performing the matching
- System availability reports
- System usage reports (CPU usage, memory usage, IO usage)

11.5.2 Verification Log

- Verification Transaction Time
- System availability reports
- System usage reports (CPU usage, memory usage, IO usage)

11.5.3 Management Functions Log

- Information on user (operator/manager/supervisor/auditor) roles and/or privileges, including creation/deletion of users and changes to roles.
- Changes to database records, including deletion of records
- Periodic (such as hourly) statistics on various databases including size
- Access log (including physical access of biometric servers)
- Activity log
- Change log
- Error log
- Denial of access

- Audit log

11.6 Security Requirements

All persistent personal information data will be encrypted. Encryption password or username/password should be required for data access. ABIS will not have access and should not try to access any network resources except the resources referenced by the URLs provided through the API. All backup data shall be stored in encrypted format using a key(s) available to PSA. Various options are given below:

- **HSM Key(s)**: The PSA will specify its requirement and share with the BioSP during implementation.
- **Storage OEM Key(s)**: The BioSP should ensure availability of key to the PSA from the time of installation of hardware.
- **Proprietary Key(s) of BioSP**: The BioSP should ensure availability of key to the PSA from the time of installation.

11.7 Operator Interface Requirements

All administration and configuration features should be available through graphical UI in addition to command level access.

11.8 Biometric Middleware

BioSP middleware will be a standardized data exchange platform between ABIS and IDMS component of the PhilSys. The key features of the middleware are as follows:

- Routing of request and response
- Guaranteed delivery of request and response
- Fault tolerance and load balancing (in future)
- Open Standard based Messaging
- Support of web based ABIS API
- Support of biometric data exchange format standards
- Encapsulation and isolation of biometric solution components
- Connectivity to other components like IDMS of PhilSys solution

11.9 Multimodal SDK

The SDK is a set of libraries that provide following functions. The BioSP must provide the following set of SDK libraries.

11.9.1 Fingerprint

(i) **Segmentation:** Slap sequence check / segmentation will be used to check if the claimed sequence: right or left slap is correct and also to visualize the segmentation result and use it for the feature extraction. It segments slap image of 2 to 4 fingers into respective digits with associated confidence level of segmentation accuracy. It will allow specification of missing or extra digits.

(ii) **Quality check:** The quality check will be used to determine if the enrolment software needs to re-capture the biometric feature and provide corrective action; for example, finger is misplaced on the scanner. Quality check must be able to provide actionable feedback (e.g., “move finger to the left”). Furthermore, the quality check SDKs will also need to be integrated at the backend for additional quality control and Best Finger Detection (BFD) by the IDMS.

(iii) **Compression/decompression and format conversion:** For verification, transmission of single fingerprints compressed by WSQ compression will be required, with decompression upon receipt by the verification function. During enrolment, the SDK is required to convert the image format such as from RAW to PNG. The SDK will supply WSQ compression and de-compression algorithms with tunable compression ratio

(iv) **Template generation:** The SDK should be able to generate ISO 19794-2 compliant templates that have been tested to be interoperable with other third-party matchers in an independent test.

(v) **Identification (1:N_{few}):** The SDK will be able to extract features compared from a fingerprint image against a set of reference templates to be defined in the BioSP’s technical proposal and return a scaled comparison score to be specified by the BioSP’s technical proposal.

(vi) **Verification (1:1):** The SDK will be able to compare features extracted from a fingerprint image against specified reference templates and return a scaled comparison score to be specified by the BioSP’s technical proposal.

11.9.2 Iris

(i) **Quality check:** The capture quality check will be used to determine if the enrolment software needs to re-capture and provide corrective action, for example image is out of focus or has motion blur. Quality check should be able to provide actionable feedback. Furthermore, the quality check SDKs will also need to be integrated at the backend for additional quality control by the IDMS.

(ii) **Segmentation:** The SDK will be able to extract uncompressed iris image out of sensor (KIND_VGA), uncompressed centered and cropped iris image (KIND_CROPPED), and KIND_CROPPED_AND_MASKED from ocular image.

(iii) **Compression/decompression and format conversion:** The SDK will be able to convert image from one format to another (for example, BMP to KIND_VGA)

(iv) **Feature/Template generation:** The SDK may extract and store a proprietary template/image from the segmented iris image both for Identification and for Verification.

(v) **Identification (1:N$_{few}$).** The SDK will be able to extract features compared from a query iris image against a set of reference templates and return a scaled comparison score to be specified by the BioSP's technical proposal.

(vi) **Verification (1:1):** The SDK will be able to compare features extracted from a query iris image against a specified reference template and return a scaled comparison score to be specified by the BioSP's technical proposal.

11.9.3 Face Photo

(i) **Automatic Capture:** Automatic capture will analyze video frames from the camera, provide the actionable feedback, and select the best frame.

(ii) **Quality check:** The capture quality check is an automated compliance check against ICAO/ISO standard to determine if the enrolment software needs to re-capture and/or provide corrective action.

(iii) **Feature/Template generation:** The SDK may extract and store a proprietary template/image from the segmented facial image for Verification.

(iv) **Compression/decompression and format conversion:** The SDK will be able to convert image from one format to another (for example, BMP to JPEG 2000) and compress or decompress images.

(v) **Verification (1:1).** The SDK will be able to compare features extracted from a query face image against a specified reference template, and return a scaled comparison score to be specified by the BioSP's technical proposal.

11.10 Standards requirements

(i) All uncompressed images should be as per prescribed standards (see Table 4. Biometric Standards).

(ii) All compressed images should be as per prescribed standards (see Table 4. Biometric Standards).

11.11 Reliability Requirements

The SDK should be consistent with the specifications, for all possible data in the specified formats. The libraries should work without any segmentation violations, memory faults or memory leaks.

11.12 Security Requirements

SDKs should be purely computational libraries, should have minimum system dependencies, and should not attempt to access any resources such as hardware, files or network.

11.13 User Interface Requirements

SDKs should not have any user interface.

11.14 Platform requirements

The BioSP shall provide SDKs for registration kits, registration client, and 1:1 authentication.

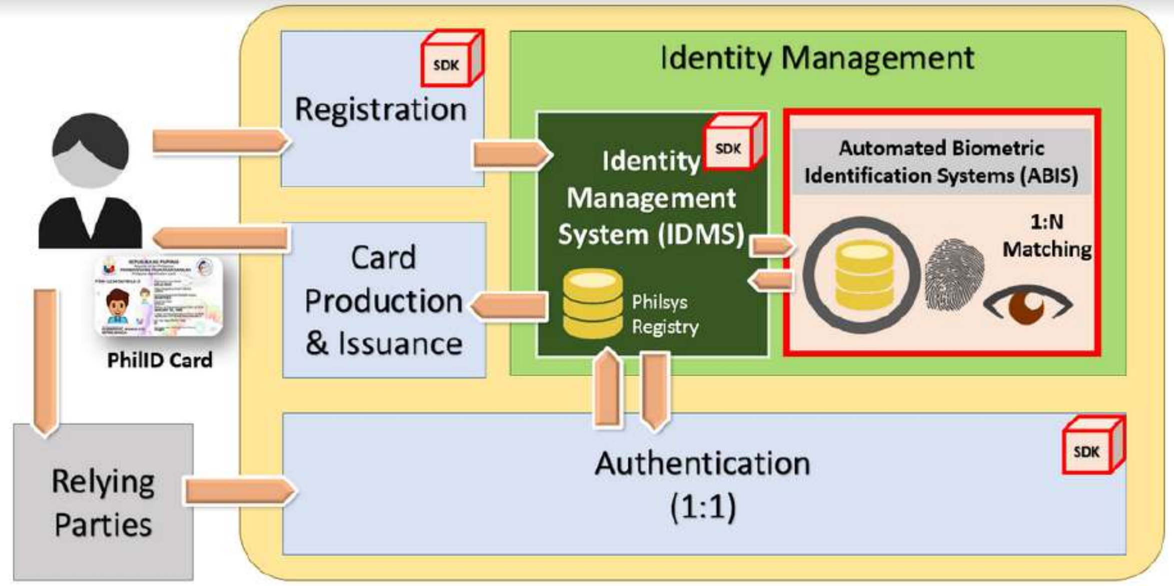


Figure 5. Overview of PhilSys Solution showing SDK requirements

The SDKs should be compatible with the operating system of the registration kits and the PhilSys Registry.

11.15 Biometric Middleware

(i) API Layer for Integration with other applications
(ii) ABIS must not expose native service to external applications to manage its services and biometric records. Instead, an API layer must be provided to access services and data in a secure way to internal applications only.
(iii) Non-ABIS components of PhilSys platform will not have direct access to native methods of ABIS, therefore access to ABIS services will be made available through representation state transfer (REST) web services.

11.16 Authentication Solution (SDKs and Integration Support)

The PSA or its appointed party will develop the PhilSys Authentication Solution. The biometric image data shall be extracted and stored outside the ABIS in order to provide authentication and e-KYC service at the required Service Level. The PSA or its appointed party will provide the database licenses and infrastructure (server, storage, etc.) of the Authentication Database (ABAS Gallery) and be responsible for commissioning and administration, operation and maintenance. The BioSP shall provide the SDKs to the PhilSys authentication solution. The BioSP will support the PSA or its appointed party in the extraction of the templates and ensuring that the ABIS database (ABIS Gallery) consistently provides the biometric records to the PhilSys Authentication Solution. The PSA or its appointed party will be responsible of the synchronization of the ABIS and ABAS Galleries, through the IDMS. The SDKs should be able to support the gallery size and performance levels.

The role of BioSP shall be limited to the following:

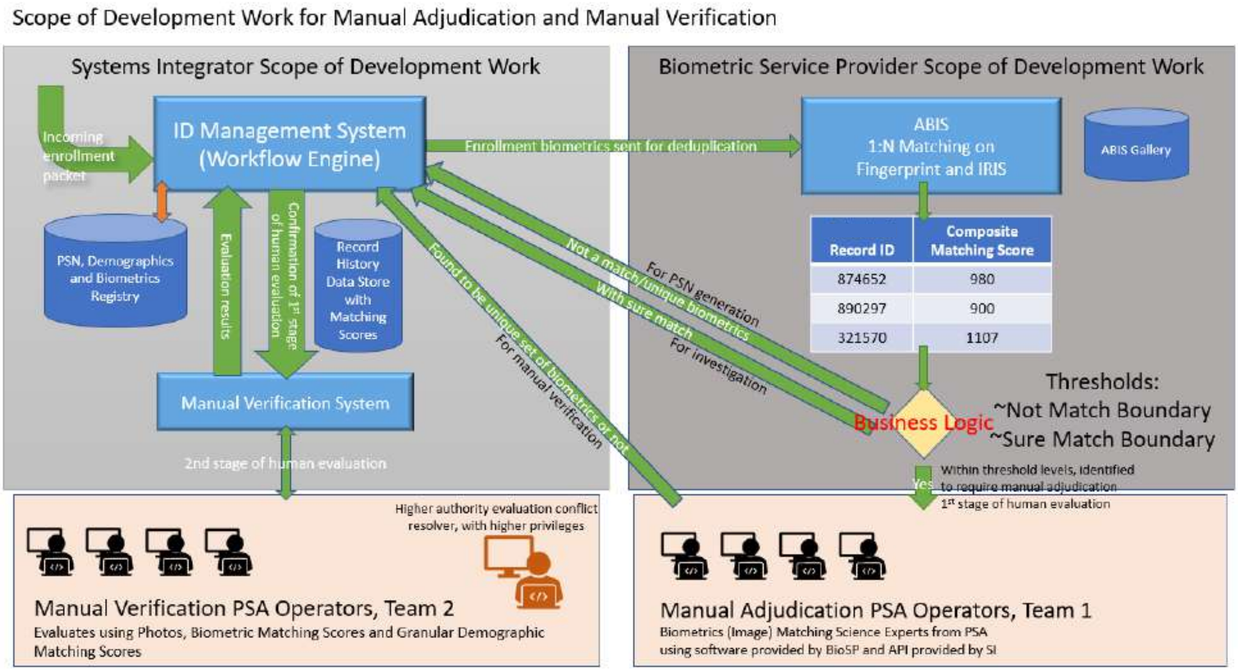
- provide SDKs (libraries) for extraction of biometric features from the raw packets,
- provide SDKs which meet functional and performance requirements, and
- provide integration and synchronization support to PSA or its appointed party.

To serve the biometric authentication request, the authentication solution will utilize the ABAS Gallery to extract the relevant biometric and will utilize the SDK for matching the stored biometric modalities with the biometric modalities received as part of the request. The following will be stored in ABAS Gallery:

- **Fingerprints**: ISO Standard Compliant Template (refer to Table 4. Biometric Standards)
- **Iris**: Compressed ISO Standard Compliant Image (for interoperability and device independence, refer to Table 4. Biometric Standards) and proprietary template/image (for high performance)
- **Face**: Compressed ISO Standard Compliant Image (for interoperability and device independence, refer to Table 4. Biometric Standards) and proprietary template/image (for high performance)

11.17 Biometric Manual Adjudication Solution

The following figure illustrates the flow of data between IDMS and ABIS that involves manual adjudication:


Scope of Development Work for Manual Adjudication and Manual Verification
Systems Integrator Scope of Development Work
Biometric Service Provider Scope of Development Work
Incoming enrollment packet
ID Management System (Workflow Engine)
Enrollment biometrics sent for deduplication
ABIS 1:N Matching on Fingerprint and IRIS
ABIS Gallery
PSN, Demographics and Biometrics Registry
Evaluation results
Confirmation of 1st stage of human evaluation
Record History Data Store with Matching Scores
Found to be unique set of biometrics or not
For manual verification
Not a match/unique biometrics
For PSN generation
With sure match
For investigation
Manual Verification System
2nd stage of human evaluation
Business Logic
Thresholds:
~Not Match Boundary
~Sure Match Boundary
Yes
Within threshold levels, identified to require manual adjudication
1st stage of human evaluation
Higher authority evaluation conflict resolver, with higher privileges
Manual Verification PSA Operators, Team 2
Evaluates using Photos, Biometric Matching Scores and Granular Demographic Matching Scores
Manual Adjudication PSA Operators, Team 1
Biometrics (Image) Matching Science Experts from PSA using software provided by BioSP and API provided by SI

Record ID	Composite Matching Score
874652	980
890297	900
321570	1107

Figure 6. Scope of Development Work for Manual Adjudication and Manual Verification

The ABIS Solution receives registration packets containing biometric data coming from the IDMS. The ABIS solution will generate biometric templates from the registration packets and perform 1:N matching against the ABIS gallery. A configurable set of thresholds will be used on the ABIS solution to determine the uniqueness of the biometric data from the registration packet in the 1:N deduplication.

All records found to be unique by the ABIS 1:N deduplication shall be forwarded to the IDMS for PSN generation. The records forwarded to the IDMS shall include record ID and biometric templates in ISO format of the registration packet.

The Manual Adjudication Module of the BioSP will be used for resolution of possible duplicates tagged by the 1:N deduplication. Hence, the registration packets that do not clear 1:N deduplication shall undergo manual adjudication. For avoidance of doubt, the Manual Adjudication Module shall not process demographic information.

The Manual Adjudication Module should be able to fetch the details regarding subjects from the ABIS Database, and after 1:N matching, display the results to the adjudicating officer(s) for their evaluation. The record shall be displayed in stages that includes biometric information (iris and fingerprint) which may enable the adjudicating officer(s) to resolve the possible duplicates. For the biometric information, the system should provide the exact details both qualitative (points of similarity and points of dissimilarity) and statistical (match score, etc.).

Once the adjudicating officer has done the evaluation, the case shall be forwarded to the IDMS for further processing.

For manual adjudication process, the PSA will provide the manpower. The BioSP shall be required to provide the Manual Adjudication Module and will train these officials on process of manual adjudication.

The records forwarded to the IDMS shall include matching scores, record ID's of possible matches coming from the ABIS gallery, Manual Adjudication evaluation results and biometric templates in ISO format of the registration packet.

The BioSP must indicate an estimate of the number of manual adjudication workstations that will be needed to manually review all potential duplicates during peak enrollment, without creating a backlog and assuming eight (8) working hours per day (single shift).

11.18 Licensing Requirements

The licensing on deduplication is required for performing 110 million registrations notwithstanding number of servers being used, scalable up to 150 million, over the contract period. License must not use hardware license key or keyed to ID (such as CPU, serial number, Ethernet ID).

The SDK licensing is also required for:

(i) **Registration Kits**. Total 5,000 Registration Kits required to perform 110 million registrations, scalable up to 150 million, over the contract period.

- SDK licenses must not use hardware license key or keyed to ID (such as CPU, serial number, Ethernet ID)
- Usable on Registration Kits required to perform 110 million registration over the contract period
- Transferable from one Registration Kit to another for PSA-owned Registration Kits and permits software-based management of license

(ii) **Authentication**. The multimodal SDK license(s) provided to PSA shall be perpetual, irrevocable, for both authentication (ABAS Gallery) and registration client. PSA shall have unrestricted, unfettered, unlimited right to use the license(s) for contracted volumes for the deployed solution of PhilSys and generation of PSN

- PSA shall have the right to deploy the SDK on additional Authentication servers to meet the horizontal and/or vertical scalability requirements to support peak authentication requests at the specified response time level

- BioSP SDK license, however, shall be contracted for a specified authentication volume

11.19 Load Requirement

This section provides an overview of the scalability and performance requirements of the proposed ABIS solution. The ABIS at a minimum, needs to provide 1:N deduplication functionality for a gallery size of 110 million records . However, at peak capacity the gallery size is estimated to be 150 million records. This is being provisioned to meet the 1.72% annual growth in population for next years. In other words, the ABIS gallery scalability should take into account the base population as of 2020 and an incremental growth per year till 2030 to cater to the performance requirements of a gallery size of 150 million records.

The following should also be considered:

(i) Deaths will be recorded and the ABIS gallery record will be marked as inactive (not updatable anymore). However, the record shall not be deleted from the gallery or ABIS database. The death rate is given above in the Table 2. Snapshot of the volumes of Philippine population.

(ii) 1:1 verification will happen through ABIS feature in case of biometric updates. The volume of these biometric updates is estimated at 25% of the total records. It may be noted that update record shall not be treated as a new record for the purpose of ABIS licensing. The old record will not be deleted from the gallery and ABIS database. The ABIS should undertake the 1:N deduplication from the ABIS Gallery including the deactivated records.

The following table shows the indicative transaction volumes and capacity parameters:

	Item	**Description**
1	Peak Biometric Gallery size	Scalable to peak capacity 150 million unique records
2	Biometric Gallery Size	Capacity 110 million unique records
3	Peak Registration per day	Capacity 175,000 registration per day
4	Peak Registration packet to be uploaded per day (incl. backlog)	At peak capacity 200,000 registration per day
5	Peak Registration batch process per hour (incl. backlog) for peak capacity	8,500 registration packets per hour

12. Scope of Work

12.1 Overview of scope of work

This section provides an overview of the scope of work. This overview covers only the summary of the scope of work. However, for detailed understanding of the tasks and activities the BioSP should refer to the respective section in the scope of work. These subsequent sections detail out the scope of work for the BioSP.

A reference summary of the scope of work is provided in the table given below:

Table 6. Overview of BioSP's Scope of Work

S. No.	Scope	Section	Brief Scope Description
1.	Project Planning and Initiation	12.2 Project Planning and Initiation	Following is the scope summary: • Mobilize the project team key resources • Prepare a detailed project schedule and prepare formats for progress reports, issue register, risk register, SLA report, incident report, etc. • Conduct a kick-off meeting along with key resources and discuss the project plan with the PSA • Coordinate with PSA or its appointed party to understand the overall project plan, dependencies, etc. • Conduct visit to assess the Data Center and Disaster Recovery sites of PSA • Prepare a plan for timely readiness of its IT infrastructure in line with other requirements (shared infrastructure provided by PSA or its appointed party, power, bandwidth, etc.) at the Data Center and Disaster Recovery sites in coordination with PSA or its appointed party.
2.	Capacity Planning	12.3 Capacity Planning	BioSP shall: • Undertake a capacity planning exercise • Prepare and submit a Capacity Planning Report.

S. No.	Scope	Section	Brief Scope Description
3.	Requirement Analysis	12.4 Requirements Analysis	BioSP shall: • Study the PhilSys solution • Study the solution planned by PSA or its appointed party • Study the biometric profiles from pilot registration • Carry out a detailed assessment to refine: ○ Functional Requirement Specification (FRS) ○ Integration Requirements ○ Service Level Requirements ○ Reporting Requirements • Formulate a detailed Implementation Plan and Iterative Test Plan incorporating the requirements.
4.	Solution Design	12.5 Solution Design	BioSP shall: • Develop a detailed design document • Prepare Biometric Solution Architecture • Implement measures for the Information Security and Business Continuity of ABIS, aligned with the overall PhilSys Information Security and Business Continuity requirements. • Design Dashboards and reporting formats • Define Exceptions and Business Alerts • Validate the infrastructure planning for servers, storage, racks, network equipment, power, utilities, hosting environment, etc. • Assist PSA or its appointed party in preparation of elevation plan and layout design for Data Center and Disaster Recovery sites
5.	Supply, Customization and Implementation of Biometric Solution	12.6 Supply, Customization and Implementation of Biometric Solution	BioSP shall: • Setup the biometric solution • Delivered as a solution with standard interfaces and that the PSA or its appointed party will integrate it with the IDMS. • Rollout the biometric solution • Integrate biometric solution with PhilSys

S. No.	Scope	Section	Brief Scope Description
6.	Biometric Solution Testing	12.7 Set up of Biometric Solution	BioSP shall perform: • Integration Test Planning and Testing • System Test Planning and Testing • Performance Testing • Security Testing (including penetration and vulnerability testing) • Creation of tests cases for User Acceptance Testing (UAT) • Perform facilitation for PSA to conduct UAT BioSP shall provide the test reports to PSA.
7.	Setup of ABIS at Data Center Sites and Migration to New Data Centers	12.12 Setup of Data Center sites	The BioSP shall setup the ABIS at the Data Center and at the Disaster Recovery Sites. The BioSP shall also transition and migrate the ABIS from the existing data centers to the new data centers, if required.
8.	Biometric Solution Hosting requirements	12.14 Biometric Solution Hosting Requirements	The BioSP should deliver, install and commission the infrastructure to meet the requirement of 110 Million registrations. The BioSP should supply the required SAN/ NAS, Tape Library to perform data backup (on tapes) and replication to Disaster Recovery Sites.
9.	Benchmarking, Acceptance and Go-Live	13. Benchmarking, Acceptance and Go-Live	BioSP shall do the following: • Benchmarking • Commissioning • Acceptance • ABIS Go-Live
10.	Manpower requirement	14. Manpower Requirement	BioSP shall deploy the Manpower as per deployment schedule.
11.	Operations and On-going Maintenance	15. Ongoing Maintenance	BioSP shall undertake the following in respect of the biometric solution: • Biometric Solution Management • Infrastructure Management • Information Security Management • Helpdesk Support

S. No.	Scope	Section	Brief Scope Description
			• Business Continuity Support • Warranty
12.	Project Management and Governance	16. Project Management	BioSP shall undertake the following in respect of the biometric solution: • Project Management • Reporting • Project Status Monitoring and Reporting • Risk and Issue Management • Change Control Management • Establish mechanism for SLA Monitoring and Reporting to be done by PSA • Exit Management and Knowledge Transfer
13.	Training and Handholding	16.5 Training	BioSP shall prepare training plan, training curriculum and conduct training for topics that shall include at least the list of courses as mentioned below: • ABIS System Configuration and Administration (including backup and restoration) • Manual Adjudication Configuration and Integration • Manual Adjudication Operation • SDK Tool Kit – Development, Configuration, Integration, and Troubleshooting • ABIS quality and accuracy management • Input Data Quality Monitoring • Performance Measurement

12.2 Project Planning and Initiation

The BioSP needs to plan all the important tasks to ensure delivery of the project as per the timelines, requirements and defined Service Levels. During the course of the project, the BioSP would be required to prepare project plan, project initiation document, progress reports, risk register, issue register and other project management related documents.

As per the scope, the BioSP is required to do the following:

(i) Mobilize the project team especially the key resources.

(ii) Prepare a detailed project plan and prepare formats for progress reports, issue register, risk register, SLA report, incident report, etc.

(iii) Conduct a kick-off meeting along with key resources and discuss the project plan with the PSA

(iv) Coordinate with the PSA or its appointed party to understand its project plan, dependencies, etc.

(v) Conduct visits to assess the Data Center and Disaster Recovery Sites of PSA

(vi) Prepare a plan for timely readiness of its IT infrastructure in line with other requirements (shared infrastructure provided by PSA or its appointed party, power, bandwidth, etc.) at the Data Center and Disaster Recovery Sites in coordination with PSA or its appointed party.

The indicative list of project management documents that are required to be prepared and presented to PSA would include, but not limited to, the following:

- **Project Plan**: Prepare detailed project plan indicating various activities to be performed along with completion dates for the same shall be provided by the BioSP.
- **Project Initiation Report**: The project initiation report shall be prepared by the BioSP. The report shall contain manpower deployment plan, project plan, risk mitigation plan, escalation matrix, etc.
- **Progress Reports**: Detailed Weekly and Monthly Progress Report along with issues/escalations/risks. The format shall be finalized in consultation with the PSA prior to start of the project.
- **Project Governance:** The governance structure proposed for the project.
- **Risk Register**: BioSP shall be required to maintain an online risk register, which shall enlist all possible risks, which shall influence project along with their occurrence and likelihood. The BioSP shall also propose the mechanism to mitigate the identified risks.
- **Issue Register**: Apart from the risk register the BioSP shall also maintain an online issue register which shall list down the issue that have occurred in the project and the decision/remedial measures taken in reference to the issue.

12.3 Capacity Planning

The BioSP is required to undertake a capacity planning exercise and submit the Bill of Materials along with the Technical Proposal. This report along with result of requirements analysis will act as an input to the overall Implementation Plan of the ABIS.

(i) An indicative volume and workload analysis are provided in Section 9.1 Volume analysis. The BioSP is expected to study the given volume, undertake a capacity planning exercise, and provide a Bill of Materials in its proposal.

(ii) The scope of BioSP also requires supply, installation, and commissioning of the underlying system and network infrastructure (Servers, Storage, Tape library, Network component, chassis, racks, switch, cables, etc.) for the biometric solution.

(iii) The Minimum Technical Requirements Specifications of system and network infrastructure are provided in Appendix B to this document.

(iv) The BioSP shall provide the Bill of Materials for the following scenarios:
- For undertaking a de-duplication considering a capacity gallery size of 110 million records
- For undertaking a de-duplication considering a peak capacity gallery size of 150 million records

(v) Deployment plan for IT infrastructure commensurate with Section 17, Implementation Schedule, should also be provided.

12.4 Requirements Analysis

(i) The BioSP shall carry out a detailed assessment and validation to finalize the functional requirements specifications (FRS) provided in this PBD and update the FRS incorporating the requirements provided by the PSA or its appointed party.

(ii) As part of the requirements gathering activity, the BioSP should study the PhilSys solution. The key sections in this study shall include Integration Requirements with PhilSys Solution, Functional Requirements, Service Level (Availability, Quality and Performance), Reporting Requirements, Implementation Schedule, etc.

(i) The indicative deliverables under this item shall be the Implementation Plan covering, but not limited to, the following:
- Augmented / enhanced Functional Requirements, Technical Requirements and Integration Requirements documents
- Requirement Traceability Matrix and Gap Assessment Report
- Iterative Test Plan

12.5 Solution Design

The BioSP shall develop a detailed design document that shall meet the PSA requirements. Moreover, BioSP shall be required to perform the following:
- Preparation of Biometric Solution Architecture Design detailing the Deployment Architecture, Network Architecture and Security Architecture for ABIS and provide to PSA or its appointed party as an input for overall design
- Dashboard and analytical report design for ABIS solution only
- Exceptions and Business Alerts definitions

The BioSP as part of the requirement gathering, workload analysis, capacity planning, and solution design process shall validate the infrastructure specified in this PBD. In coordination with PSA, the BioSP should also provide a layout design for ABIS at the DC and DR. In view of the limited DC/DR space availability, the planning and design should be done in a manner to optimally utilize the existing resources (space, racks, power, network, air conditioning, etc.). Before starting the installation, the BioSP should obtain necessary approval from, and coordinate with PSA.

The BioSP shall implement measures for the Information Security and Business Continuity of ABIS, aligned with the overall PhilSys Information Security and Business Continuity requirements.

The deliverables for this activity are the Detailed Solution Design covering, but not limited to, the following:

- Deployment Architecture Document (including Data Flow Diagram)
- High-Level Design Document and Low-Level Design Document (including Schema Diagram)
- Layout Design of ABIS Solution

12.6 Supply, Customization and Implementation of Biometric Solution

The BioSP scope includes supply, customization, and implementation of the biometric solution in accordance with the terms and conditions of the PBD. The overall solution should be implemented in the PSA Data Center and/or PSA specified locations. During this activity the BioSP is required to customize the biometric solution including ABIS, Biometric Middleware, Manual Adjudication Module, and Multimodal SDKs.

12.7 Set up of Biometric Solution

Once the BioSP has commissioned the infrastructure, it will be responsible for the supply, installation, configuration, and continuous fine tuning of necessary software to operate the biometric solution. In addition to the biometric solution, the BioSP shall also provide server operating system, systems software (e.g. virtualization), database, etc. The BioSP should tune parameters for optimal performance of the ABIS and should configure the system to harden the security of the OS for protection against malicious and unwarranted attacks.

In addition to installing and tuning the ABIS software, the BioSP will also be responsible for configuring the ABIS for interfacing with systems to be provided by the PSA or its appointed party (e.g., Enterprise Management System agents, SIEM agents, etc.).

12.8 Integration Requirements

12.8.1 Integration Requirements for PSA or its appointed party

The PSA or its appointed party is responsible for the integration of the PhilSys solution.

12.8.2 Integration Requirements for BioSP

The BioSP will be responsible for the integration of ABIS with IDMS through the APIs to be provided by PSA or its appointed party.

The BioSP should extend necessary, adequate and timely support to the PSA or its appointed party to achieve the integration and thereafter to monitor and manage the requirements and service levels.

- Integration of Manual Adjudication Module of ABIS with IDMS.
- Customize the ABIS to receive biometric deduplication request from IDMS and submit 1:N matching results to IDMS.
- Integration of Multimodal SDKs with the Registration Client, Registration Kits and the PhilSys Authentication Solution

The BioSP should provide technical support before, during and after the integration is completed.

12.9 User Acceptance Testing (UAT)

The objective of the UAT is to determine whether the biometric solution meets the PSA requirements. It is mandatory for BioSP to create end-to-end test cases as part of UAT. The test cases need to be validated by PSA. The BioSP would make the necessary changes to the solution to ensure that it successfully passes through UAT.

Test Plan for UAT would be prepared by the BioSP with the approval of the PSA. The BioSP will plan all aspects of UAT (including the preparation of test data and test environment) and obtain required assistance to ensure its success. The test cases prepared by BioSP shall be approved and used by PSA for the purpose of testing.

The BioSP shall provide support to document the test results along with defects statistics. BioSP shall ensure that defects found are corrected and is retested by the user group. The testing shall be done in iterations until the specified requirements are met. At the discretion of PSA, a third party may audit the result of testing. On successful completion of the UAT, BioSP shall obtain a formal approval from PSA for ABIS to Go-Live.

The BioSP shall be required to demonstrate all the services/features/functionalities as mentioned in the agreement. The pre-requisites for carrying out UAT activity shall be:

- Submission of a detailed test plan by BioSP and approval of this plan by PSA.
- All documentation related to ABIS solution should be completed & submitted.
- The training requirements as mentioned as part of this PBD should be completed before the final acceptance.
- Licenses/manuals/brochures/Data Sheets/CD/DVD/media as required.

12.10 Roll out of Biometric Solution – ABIS Go-Live

The following activities shall be undertaken prior to the ABIS Go-Live:

- The UAT should be completed before the ABIS Go-Live.
- The BioSP shall deploy the biometric solution at both Data Center and Disaster Recovery sites prior to the ABIS Go-Live.
- With a view on accuracy, throughput and optimal resource utilization, the BioSP shall undertake continuous performance monitoring and improvement.
- Configuration of ABIS solution’s own internal persistence/database component with adequate back-up, maintenance, and recovery to ensure business continuity.
- Provide training to PSA and its appointed party on the integration of the ABIS and Multimodal SDKs with PhilSys application.
- Submit documentation of key configuration settings, business rules, and policies adopted along with key design and solution features along with user manuals to PSA for their review and approval.
- Configure the solution to comply with the PhilSys policies and other business rules and application level policies as stated.

12.11 Conditions for re-templatization

Re-templating the ABIS Gallery may arise in two (2) conditions:

a) The minutiae gallery is old and percentage of records needing update over the years is very large, and authentication solution is prone to high percentage of errors; and

b) In case of change / replacement of the BioSP.

In case of (a) above the BioSP shall undertake an analysis and upon review, the BioSP shall,

- Submit a report clearly specifying the advantages, time, additional infrastructure and cost needed for re-template creation, and rollback procedures in case of error, etc.
- The analysis should be done keeping in mind that the system downtime is either zero or minimal during this exercise.
- PSA will review the analysis presented by the BioSP and may approve the exercise of re-template creation. Upon approval from PSA, the BioSP should undertake this exercise and submit a periodic progress report to the PSA.

The BioSP should support re-template creation i.e. re-creation of biometric gallery from raw images based on latest algorithm with zero or minimal downtime during this re-template exercise. However, the re-templatization shall not be considered as de-duplication.

12.12 Setup of Data Center sites

PSA shall provide the physical space for hosting IT Infrastructure in Primary Site, Disaster Recovery Site. PSA shall be responsible for providing physical infrastructure in these sites. For each rack within these Data Centers, a power capacity of 5 KVA has been planned.

12.12.1 Data Center Strategy

PSA has visualized an interim strategy of Data Center as well as a permanent strategy. In short term, the PSA has decided to utilize two-way setup containing DC and DR sites. In the long term, the PSA may decide to utilize a three-way setup containing Primary DC, Secondary DC and DR sites. The Primary DC and DR sites will be in 1:1 configuration i.e. exact replica of each other. For the entire duration, a mechanism for storage and safekeeping of backup tapes, a remote site will be utilized. The details of the strategy are provided below:

12.12.2 DC/DR set up in the interim

Upon completion of the respective Primary and Disaster Recovery Site by the PSA for hosting of PhilSys System, the BioSP shall assist the PSA in relation to the hosting of the biometric solution. For hosting of the solution, the BioSP shall do the following in coordination with PSA:

- Undertake a site survey to highlight the positioning of racks, power and backup
- Prepare a site survey report and submit it to the PSA
- Prepare a detailed rack deployment plan for site set-up and obtain approval from PSA
- Execute the plan and commission the IT infrastructure
- Commission the network link and test it post commissioning

12.12.3 Permanent DC/DR set up

The migration of DC and DR may be carried out upon reaching saturation of capacity in existing data center or completion of the preparation of the permanent DC/DR. In this activity, the BioSP shall assist the PSA in relation to hosting the biometric solution. In setting up the site, the BioSP shall do the following:

- Undertake a site survey to highlight the positioning of racks, power and backup systems and chart and prepare a site survey report.
- Prepare a detailed rack plan for site set-up and obtain approval from the PSA
- Prepare a rack plan positioning infrastructure set up within the racks
- Execute the plan and commission the IT infrastructure
- Commission the network link and test it post commissioning

12.13 Transition and Migration of Data Center

The BioSP shall be responsible for transition and migration of Primary Data Center and Disaster Recovery to the new Primary Data Center and Disaster Recovery site for the biometric solution. Migration may be carried out upon reaching saturation of capacity in existing data center or at PSA's directive. The BioSP shall inform the PSA at least three (3) months before the expected saturation of the data center. The BioSP should provide an overall strategy and approach for migration of sites (including data) as part of their Technical Proposal. PSA or its appointed party and BioSP should carry out the transition and migration exercise in a manner, which minimizes service downtime, if any, with approval of PSA.

The BioSP shall undertake the transfer of biometric solution and infrastructure to another Data Center facility during the contract period. BioSP, upon prior notice from PSA, shall deploy required personnel to undertake the migration of the infrastructure, setting up, installation, configuration, and commissioning of the biometric solution at the new facility until the solution is operating at the Service Level requirements.

For overall transition and migration, the BioSP shall:

- Prepare a detailed strategy and approach for migration including a detailed plan for migration.
- Ensure that there is minimal service downtime of PhilSys during migration. The detailed strategy and approach should also include potential risks during migration and steps which the BioSP shall take to mitigate those risks.
- Coordinate with PSA as regards to the transition and migration
- Obtain approval on the strategy and approach from the PSA
- Undertake transition and migration as per the approved strategy and approach
- Once migration is complete, test the success of migration
- Prepare a report detailing the migration activities including testing and its results and submit it to the PSA
- Ensure no physical damage is done to the systems during the physical migration activity from one site to other
- Ensure there's no data loss and performance degradation during the migration activity
- Conduct DR drill as part of successful completion of the site set up

12.14 Biometric Solution Hosting Requirements

12.14.1 Supply of Hardware

BioSP must provide underlying hardware for the biometric solution, for undertaking biometric 1:N de-duplication, and for manual adjudication. The hardware, and its refresh if needed, must be sufficient to meet the Service Levels as defined. The hardware at Primary Site and Disaster Recovery Site must be supplied in 1:1 configuration. ABIS

Hardware implementation design must be able to support a Tier 3 data center configuration.

The hardware and software components to be delivered by BioSP includes, but is not limited to, the following:

Table 7. Indicative Components of Hardware

Component	Primary Site	Disaster Recovery	PRO
Server (including blade chassis/ rack server as required)	Yes	Yes	
Storage Area Network (including disks)	Yes	Yes	
Racks and KVM Switch	Yes	Yes	
Network Switches and Cable	Yes	Yes	
Backup Software	Yes	Yes	
Tape Library	Yes	Yes	
OS and other software	Yes	Yes	
Fully-operational workstations for Manual Adjudication (each including printers, pre-installed OS, 3rd party anti-virus and manual adjudication module, dual monitors at least 21")			Yes

The BioSP is free to propose servers of any specifications that meet their solution requirements and the conditions below.

The BioSP shall be responsible for supply, installation and commission of all hardware supplied along with installation and commissioning of the biometric solution. In the Data Center, PSA shall provide the data center space, power, cooling infrastructure and a standard network switch to connect with the rest of network in the data centers.

The hardware components to be provided by BioSP shall adhere to following:

- Hardware components must be commercially available in the Philippines
- Proprietary hardware component for servers are not allowed
- Branded and brand new
- Compatible with all required interfacing devices and appliances in the data center
- Be able to interconnect and interoperate with all required interfacing devices and appliances in the data center
- Compatible with the Philippines standard power ratings and power configurations
- The OEMs of servers and storage proposed to be supplied should figure in reports published at any time in last three years from leading and widely recognized international IT publications.

Table below provides some of the data center environment constraints that the BioSP should note while finalizing the Hardware Infrastructure to be provided.

Parameter	Value
Preferable Rack Size	42 RU / 19 Inch high, 600 mm wide, 1000 mm deep
Allocated Power per Rack	5 KVA

12.14.2 Environment Creation

The BioSP will be required to arrange the below mentioned environments

Environment	Description
Development	The necessary development and testing environment for biometric solution will be arranged in-house at its offshore location by the BioSP.
Testing except UAT	
Testing (only UAT)	Disaster Recovery Site will act as the testing environment for UAT
Benchmarking	Disaster Recovery Site will act as the testing environment for Benchmarking exercise
Staging	Staging environment should be created in Primary Site as well as Disaster Recovery Site
Production	Production environment should be created in Primary Site as well as Disaster Recovery Site

In addition, the BioSP will provide an end-to-end sandbox environment within the PSA Data Center that can cater to one million records.

13. Benchmarking, Acceptance and Go-Live

13.1 Benchmarking

The benchmarking exercise is intended to evaluate the ability of the proposed ABIS System to scale to the intended usage. Benchmark shall cover the entire PhilSys including but not limited to biometric solution, PhilSys Data Store and all related interfaces. The Benchmarking process does not intend to simulate all the aspects of PhilSys, however, all design parameters, components and related interfaces shall be considered.

Benchmarking shall be in accordance with the production deployment and biometric solution architecture proposed in the Technical Proposal of the BioSP.

BioSP shall be responsible to undertake the benchmarking of the biometric solution of the PhilSys. The BioSP in consultation with PSA or its appointed party shall:

- Prepare benchmarking test cases and obtain approval on the test cases from the PSA
- Supply, build, commission, configure, tune and execute the benchmarks at the DR site
- Provide the tools (load generator), scripts for etc. for benchmarking.
- Create test data from base data provided by PSA
- Demonstrate at least one successful (live) run
- Undertake benchmarking of the biometric solution as per the parameter shown in the table below:

Table 8. Benchmarking scenarios of the biometric solution

Gallery Size Test Scenario (ABIS)	Test Description	Gallery Size	Deduplication Rate	Test Duration
0 to 10 Million	Basic Performance Test with proposed sizing of associated IT Hardware	10 million	125,000	24 Hours
10 to 25 Million	Scalability and proposed sizing for associated IT Hardware	25 million	200,000	24 Hours

Where:

Deduplication Rate – Successful biometric deduplication of resident within 24 hours of receipt of request, subject to a maximum of 125,000 and 200,000 biometric deduplication requests

Test Duration – Duration in which 1: N deduplication of each registration packet should get completed within 24 hours.

(SDK)	Description	Rate	Duration	Concurrency	Response
Auth_1	Basic Performance Test	0.083 Million per Hour	8 Hours	1,000	0.5 seconds
Auth_2	Advanced Performance Test	0.25 Million per Hour	8 Hours	1,000	0.5 seconds

Where:

Authentication Request Rate (Basic Performance Test) – 0.083 million Authentication Requests are expected per hour with a response service time of 0.5 seconds with 1,000 concurrent users during basic performance test.

Authentication Request Rate (Advanced Performance Test) – 0.25 million Authentication Requests are expected per hour with a response service time of 0.5 seconds with 1,000 concurrent users during advanced performance test.

Test Duration – Duration in which 1:1 matching authentication completes as per expected SLA of 0.5 seconds for SDK matching in the entire test cycle.

Modes – Fingerprint (1 or multiple), Iris (both), Face.

Basic Test – OTP based**.**

Advanced Test – e-KYC including biometric authentication.

Report the benchmarking output in the format specified by PSA or its appointed party. Key guidelines for reporting benchmarking output are as follows:

- Resource usage should have graphs with a sampling interval of 5 minutes for all resources (all servers, routers, switches, disk arrays, firewalls etc.)
- Response Time Reports should include minimum, maximum, average and 90 percentile response times. Response Time should be shown as a function of time for the duration of the test.
- The test results should also include the iterative configuration changes/tuning required to achieve the benchmark results.
- The equipment used for the test shall be the same as proposed by the BioSP, if however there is a shortfall in the quantity of the equipment proposed, the BioSP should provide the required quantity of equipment/licenses, as the case may-be to achieve the benchmark results and Service Level requirements.

PSA shall witness the benchmark or appoint an agency at its own cost to verify and validate the benchmarking tests and certify the results of the benchmarking. Benchmark test report provided by the BioSP shall be approved by the PSA

In the event the solution and the corresponding Bill of Materials proposed by the BioSP fails to meet the benchmarking performance criteria, BioSP shall enhance/augment and supply additional components (including server, storage, networking equipment, etc.) without any additional cost to the PSA.

The BioSP shall propose the parameters to measure performance of PhilSys in consultation with PSA.

13.2 Commissioning

After successful benchmarking of Biometric Solution, the BioSP shall commission the ABIS in the PSA Data Center and Disaster Recovery Site for production with the approval of PSA.

13.3 Acceptance

The Acceptance of the solution shall be provided by the PSA once following conditions have been met successfully to the satisfaction of the PSA:

- Successful Go-Live of the ABIS at Data Center and to Disaster Recovery
- Completion of all the documentation required as part of this PBD
- Completion of the application-related training to all identified users
- Successful operation of biometric solution for 30 working days after Go-Live

13.4 Go-Live

The formal approval from PSA after successful completion of the UAT constitutes Go-Live**.**

14. Manpower Requirement

This section outlines the guideline for staffing and provisioning of manpower in the implementation of ABIS system by the BioSP. Any adherence or deviations to any terms should be clearly highlighted in the Technical Proposal.

14.1 Guidelines for staffing and provisioning of manpower

(i) The BioSP is expected to deploy a minimum manpower as specified under 14.7 Deployment of Resources. The key resources, other than the Biometrics Specialist, have to be on the permanent payrolls of the BioSP. The Biometrics Specialist may be engaged on a part-time basis, provided that, he/she will be engaged for the duration specified in the deployment schedule.

(ii) The Key Resources are expected to work at the PSA offices (onsite), for the entire duration of the project as per the deployment plan of BioSP. The BioSP is free to deploy additional resources over and above the minimum resources required as per the PBD at no extra cost to the PSA.

(iii) In case of a Joint Venture (JV), the resource mix has to be as per the expertise of the JV Partners. The biometric technical expertise should mandatorily come from the JV member relied on for the biometric experience.

(iv) The BioSP shall provide a detailed staffing schedule as part of the Technical Proposal with list of all resources proposed by BioSP in Key Resource Category.

(v) The staffing schedule should also include an organizational chart showing the proposed organization to be established by the BioSP for execution of the scope of work. The chart should clearly bring out variations to the Organization structure, if any, envisaged by the BioSP for various stages of the project.

(vi) Detailed curriculum vitae and supporting documents should be provided for Key Resources that are subject to evaluation. The area of expertise, role and tasks assigned should be clearly identified for each of the Key Resources.

(vii) The experience and expertise of the human resource of the BioSP or JV Member, who are to be allocated for the key roles/positions is a significant component of BioSP evaluation.

(viii) The staffing schedule should contain the schedule of deployment of the Key Resources onsite.

(ix) The PSA shall approve this schedule after its careful study and may request the BioSP to make the changes in the schedule, if required.

(x) The PSA reserves the right to conduct security clearance for any Key Resource of the BioSP deployed on the Project.

14.2 BioSP functions that can be performed off-site

The BioSP may carry out any of the following functions off-site:

1) BioSP application development
2) System and integration testing
3) Biometric gallery creation for benchmarking exercise
4) Biometric modality profile study
5) SDK integration and testing

14.3 Replacement of Personnel

(i) The BioSP should avoid any change in the team proposed for execution of the scope of services or replacement of any manpower resource.

(ii) If the same is however unavoidable, due to circumstances such as the resource leaving the BioSP’s organization or the sub-contracted agency’s organization, BioSP shall promptly inform the PSA in writing.

(iii) In case of replacement of any manpower resource, the BioSP should seek approval from the PSA and ensure efficient knowledge transfer from the outgoing resource to the incoming resource, and adequate hand-holding period and training for the incoming resource in order to maintain the continued level of service.

14.4 Removal of Personnel

(i) The PSA may at any time object to and require the BioSP to remove forthwith from the Project Site any authorized representative or employee of the BioSP or any person(s) of the BioSP's team, if, upon the evaluation of PSA the person in question has mis-conducted or his/her deployment is otherwise considered undesirable by PSA. The BioSP shall forthwith remove and shall not again deploy the person without the written consent of PSA.

(ii) PSA may at any time object to and request the BioSP to remove from the Sites any of BioSP's authorized representative including any employee of the BioSP or his team or any person(s) deployed by BioSP or his team for professional incompetence or negligence or for being deployed for work for which he/she is not suited.

(iii) In case their performance is found to be below the Service Level requirements, the same shall be informed to the BioSP who shall provide a replacement of the resource within 15 days.

14.5 Logistics requirements of the Personnel

The BioSP shall be responsible for the deployment, transportation, accommodation, and other requirements of all its employees required for the execution of the work and provision of services.

14.6 Escalation Matrix

(i) As part of the Technical Proposal, the BioSP shall provide a detailed Escalation Matrix in concurrence to the proposed BioSP's organizational structure.

(ii) The Escalation Matrix should include a steering committee for expedited decision making with PSA as the head of the committee.

(iii) The Escalation Matrix should address key requirements stated in the Service Level Agreements for various service delivery activities and cover all major service delivery activities.

14.7 Deployment of Resources

Given below is the indicative key manpower resources for implementation and operation and maintenance phase of biometric solution. BioSP shall provide the profiles as prescribed and seek PSA's approval prior to deployment of resources.

Table 9. List of Key Resources

#	Key Resource Category	Quantity
Leadership		
1.	Delivery Head / Project Director	1
2.	Project Manager	1
Key Resources		
3.	Integration Engineer	2
4.	Biometric Specialist	1
5.	System Engineer	2
6.	QA and Test Engineer	1
7.	Training Manager	1
8.	O&M Manager	1
9.	Helpdesk Agent	1

14.8 Profile Qualifications

A summary of the qualification and experience criteria is mentioned in the table given below.

Table 10. Minimum Manpower Qualification

Position	Minimum Qualification	Certification	Experience (in Years)	
			Total	**Relevant**
Project Manager	Bachelor’s Degree	Preferable Certified PMP, PRINCE 2 or equivalent Must have the experience of working as a project Manager in at least one ABIS deployment	10	10
Integration Engineer	Bachelor’s Degree in Computer	Must have the experience of deploying ABIS and	10	5

Position	**Minimum Qualification**	**Certification**	**Experience (in Years)**	
			Total	**Relevant**
	Science or related fields	SDK in at least two ABIS deployment		
Biometrics Specialist	PhD in Imaging Science or related fields	Must be a biometrics specialist with experience in deployment of citizen identity projects.	10	5
System Engineer	Bachelor’s Degree in Computer Science or related fields	Experience in deployment of ABIS / Authentication solution in at least one ABIS deployment	10	5
QA and Test Engineer	Bachelor’s Degree in Computer Science or related fields	Certified Software Test Engineer or equivalent	10	5
Training Manager	Bachelor’s Degree	Must have experience in training for biometric solutions and resolution aspects	10	5
O&M Manager	Bachelor’s Degree	Must have experience in at least one (1) project relating to biometric solutions	10	5
Helpdesk Agent	At least two (2) years of college education	-	5	5

14.9 Indicative deployment schedule

The BioSP will plan for the manpower deployment in accordance with the table given below:

Table 11. Manpower Deployment Schedule

Position	Before Go-Live		After Go-Live		
	Deployment	Location	Deployment	Location	Duration
Project Director	Part Time	Onsite	Part time	Onsite	BioSP to decide deployment
Project Manager	Full-Time for entire duration	Onsite	Part time	Onsite	7 days in a month
Integration Engineer	Full-Time after design phase	Onsite	Part-time	Onsite	BioSP to decide deployment
Biometric Specialist	Full-Time for two months	Onsite	Part-Time for at least 15 working days in a year	Onsite	BioSP to decide deployment
System Engineer	Full-Time after design phase	Onsite	Part-time	Onsite	BioSP to decide deployment
QA and Test Engineer	Part time after design phase	Onsite	Part time	Offsite	BioSP to decide deployment
Training Manager	Full-Time during training phase	Onsite	Part-Time	Onsite	BioSP to decide deployment
O&M Manager	None	None	Full-Time	Onsite	--
Helpdesk Agent	24/7 for the entire duration	Onsite	Full-Time	Onsite	--

15. Ongoing Maintenance

15.1 Maintenance Management

The BioSP shall be required to undertake maintenance for 5 years from Contract Signing. The BioSP shall be responsible to provide resolution of incidents being raised by the PSA and its appointed party for ABIS solution, provide helpdesk services, monitor the biometric solution SLAs, optimize its performance, provide updates for ABIS and managing the solution.

The various activities to be performed by the PSA and its appointed party during the maintenance of the biometric solution, but not limited to, are categorized as (i) Biometric

Solution Management, (ii) Infrastructure Management, (iii) Information Security, (iv) Helpdesk Management, (v) Business Continuity Support, and (vi) Warranty and Annual Technical Support (ATS).

15.2 Biometric Solution Management

This section includes, but not limited to, the various activities to be performed by the BioSP during the maintenance of the solution:

(i) Analysis should be done to ensure 99.5% system availability.

(ii) Re-creation of templates, if required, upon approval by PSA. The BioSP should undertake this exercise and submit a periodic progress report to the PSA.

(iii) The BioSP shall provide warranty for biometric solution, including the supplied hardware, for the duration of contract commencing from ABIS Go Live Date. The warranty should include that the solution supplied under this contract shall have no defect arising from design or workmanship or from any act or omission of the successful vendor that may develop under normal use of the supplied solution.

(iv) During the warranty period, BioSP shall be completely responsible for defect-free functionality of the biometric solution and shall resolve any solution-related issues as per service level defined in the contract. This shall include request-based services (defects/issues), bug fixing, enhancements, configuration management, VAPT analysis and post release support.

(v) BioSP shall provide the latest updates, patches, bug fixes, enhancements at no extra cost to PSA. PSA should be informed of all version upgrades (minor & major), patches, releases and enhancements along with impacts to the biometric solution.

(vi) BioSP shall be responsible for software version management, software documentation management reflecting current features and functionality of the solution.

(vii) For support, the BioSP may decide an appropriate onsite-offsite model to meet the service levels, with approval of PSA.

(viii) For bug fixes and end-user problem resolution, the stakeholder support would include all activities related to resolving the defects reported by the users. Every defect should be logged and should be categorized on the severity levels. BioSP should identify the solution and take necessary approvals from the stakeholders and release the patch for User Acceptance Testing (UAT) after fixing the defects. BioSP should document defects encountered as well as document the resolution of the same.

(ix) For new development and enhancements, BioSP in consultation with PSA is expected to define a formal process (change management process) to manage the requirements changes as defined for illustration below:

- BioSP shall be responsible to initiate the change requests suggested by stakeholders, assess the need to implement the suggested changes, take necessary approvals to implement the suggested changes. PSA will forward the approved change requests to BioSP.

- BioSP shall maintain a change request log to keep track of the change requests. Each entry in the log shall contain a Change Request Number, a brief description of the change, the effect of the change, the status of the change request, and the key date.
- BioSP shall assess the effect of the change by performing impact analysis.
- BioSP shall maintain the change request log with updated information and provide the same to PSA as and when desired.

(x) The BioSP shall have a system for Configuration management and Version Control. This will ensure that all versions updates in the application are tracked and approved after due scrutiny. BioSP may be required to ensure that a copy of the production environment is backed up and stored in the repository before the new / modified components are copied to Production.

(xi) For test management, and also as part of the release management, BioSP should perform the following activities:

- BioSP should group the related change requests, assess their development progress and accordingly prepare a schedule for their release to production.
- BioSP should in consultation with PSA prepare a release plan for every release. This plan should include the release number and date of release.

15.3 Infrastructure Management

The various activities to be performed by the BioSP for the System Administration of the biometric solution:

(i) Overall management and administration of infrastructure solution including servers, storage, networking & security components, etc.

(ii) Performance tuning of the system

(iii) Monitor and track server performance and take corrective actions to optimize the performance

(iv) System administration tasks such as creating and managing users etc.

(v) Data storage management activities including backup, restore and archival etc.

(vi) Attend to user request for assistance related to usage and management of the solution

(vii) Other important activities shall include but not limited to:

- Maintenance of system configuration
- Implementation of system security features
- Tracking the servers' performance and take remedial and preventive actions in case of problems
- Proper upkeep of storage media for taking backups
- Hardware refresh, if required

15.4 Information Security

15.4.1 ISO certification readiness for Information Security Management

The BioSP's proposed ABIS must be ISO 27001 certification ready. Changes and amendments to ABIS to achieve ISO 27001 compliance will be the responsibility of the ABIS supplier at no additional cost to the PSA.

15.4.2 Responsibility for the overall security of the biometric solution

The BioSP shall be responsible for implementing measures to ensure the overall security of the biometric solution and confidentiality of the data in compliance with the Data Privacy Act of 2012.

The BioSP shall monitor biometric solution for events or activities, which might compromise (fraudulently or accidentally) the confidentiality, integrity or availability of the Services.

The various activities to be performed by the BioSP for information security of the solution:

(i) Compliance to the Data Privacy Act of 2012

(ii) Monitoring the security of the system

- As per the incident reports shared by the PSA and its appointed Party , etc.
- Audit review tools and VAPT analysis
- Manual processes

(iii) The BioSP shall co-operate with the appointed representatives of PSA in case of security incidents. The incident response process will seek to limit damage and may include the investigation of the incident and notification of the appropriate authorities. A summary of all security incidents shall be made available to PSA on a weekly basis. The significant security incidents will be reported immediately.

(iv) The BioSP shall produce and maintain system audit logs on the system for a period of two (2) years, at which point they will be archived and stored at off-site or as desired by PSA. The BioSP will regularly review the audit logs for relevant security exceptions.

15.5 Help desk Support

The BioSP shall operate a helpdesk to address technical queries 24/7 on all working days during the implementation stage. An indicative activities list is given below:

(i) Deployment of one helpdesk agent to attend the helpdesk requests for extending technical support on biometric solution.

(ii) The BioSP ensures that the helpdesk is staffed, at least one month before ABIS Go–Live.

(iii) It is expected that the helpdesk agent deployed would be technically competent to handle all technical issues including but not limited to trouble shooting, resolution of service tickets of various priorities, SLA monitoring, etc. as well as reporting and monitoring, and other requirements.

(iv) The helpdesk agent must have good understanding of the project, the technical, functional and operational details of the technologies involved, including a very good understanding of the application software.

(v) Track each incident / call to resolution.

(vi) Escalate the calls, to the appropriate levels, if necessary, as per the escalation matrix agreed upon.

(vii) Coordinate with respective O&M for closure of calls.

(viii) In case of L3 ticket, the following process will be adopted:

- PSA will classify the issue as Critical or Non-Critical;
- BioSP will undertake troubleshooting and communicate the estimated resolution time to the PSA;
- PSA shall approve the estimated resolution time;
- For critical issues, the BioSP will provide a work around as soon as possible in agreed timeline; and
- For all L3 issues, the BioSP will provide a resolution in timeline approved by the PSA.

(ix) Analyse the incident / call statistics and provide monthly reports;

- Type of incidents / calls logged
- Incidents / calls resolved
- Incidents / calls open

15.6 Business Continuity Support

(i) BioSP must plan to create a resilient environment/system, which can be recovered in case of a Disaster. The following measures must be observed to ensure business continuity:

- Primary Site and Disaster Recovery site shall be configured in 1:1 capacity mode.
- ABIS solution in Primary Site and Disaster Recovery site will be maintained Active-Passive.
- There shall be no Zero data loss while switching from Primary Site to Disaster Recovery site.
- Seamless switching from Primary Site to Disaster Recovery site (and vice-versa).

(ii) The BioSP will be responsible for the purpose of replication of ABIS related data between sites.

(iii) BioSP shall ensure recovery/backup to ensure business continuity even in the event of disaster. The BioSP will also be responsible for resuming (including rolling back to Primary Site) the biometric solution and associated data. Thus, BioSP will be responsible for managing the recovery time objective (RTO) and recovery point objective (RPO). The BioSP shall also be responsible for coordinating with OEM(s) of ABIS infrastructure.

15.7 Warranty and Annual Technical Support (ATS)

BioSP should ensure availability of Warranty and ATS with all the OEMs for proposed software and hardware components including biometrics algorithms, if required. This Warranty and ATS shall cover the entire duration of the contract. BioSP should track the Warranty and ATS for all the components of Biometric Solution and initiate procedure for renewal of the same at appropriate point in time.

16. Project Management

16.1 Project Status Monitoring and Reporting

The BioSP shall circulate written progress reports each week to PSA and other stakeholders. Project status report shall include Progress vis-à-vis the Project Plan, status of all risks and issues, exceptions and issues along with recommended resolution etc. This project status report shall be discussed each week during the weekly project status meeting. The progress of the project shall be accessible in the online dashboard. The project status report shall be made available online in a dynamic manner, and a weekly snapshot of which shall be also made available online.

Other than the planned meetings, in exceptional cases, special project status meeting may be called with prior notice to all parties concerned. PSA reserves the right to ask the BioSP for the project review reports other than the weekly status review report.

All reports shall be made available online with managed access.

16.2 Risk and Issue Management

The BioSP shall develop a Risk Management Plan and a Risk Register for this project. BioSP shall identify project risks, analyse and prioritize the risk, identify mitigation plans and document the risks and their mitigation strategy in the risk register, which shall be made available online.

The BioSP must also prepare an issue management procedure to identify, track, and resolve all issues of the project. BioSP must prepare an issue register to document all key project issues, their impact on the engagement and their resolution plans.

BioSP should periodically update risk and issue registers and present them as part of the weekly project review reports. The project risks and issues shall also be discussed with the PSA in the weekly PMO meetings in order to discuss and identify mitigation plans.

All registers described herein shall be made available online with managed access.

16.3 Change Control Management

Due to the evolving nature of the project requirements and the complexity of the project, changes may be required before, during, and after rollout of the PhilSys solution. These changes may require modification to the software, infrastructure, and underlying processes and may thus have a financial impact.

BioSP is required to work with the PSA to ensure that all changes are discussed, managed, and implemented in a constructive manner.

One of the key requirements is that the BioSP will be responsible for providing system availability according to defined service levels. This includes responsibility to implement upgrades, enhancements, extensions, and other changes to the software application in order to maintain and extend reliable information systems, services, and service delivery mechanism. It is important that changes to the computing environment and underlying infrastructure are executed in a standardized and controlled manner in order to mitigate the risk of interruptions to the services and to maintain an online repository of knowledge about the current and changed configurations, as well as the status of the computing environment at all times.

The BioSP shall propose to PSA change control procedures covering any proposed change to the scope of work and SLAs. The PSA shall review and approve the proposed change control procedures. Such change shall include:

- Requests for requirements change (additions, deletions, modifications, deferrals) in Scope of Work (including software)
- Requests for resolving the problems in current production systems
- Requests for enhancements in current production systems
- Requests for new development projects

The Change Control procedure applies to baselined work products created or managed by the members of the PhilSys solution. The Change Control process excludes any work products that are still under development.
All change control management requests and reports shall be made available online with managed access.

16.4 Transition and Migration to new Data Center sites

BioSP shall be responsible for transition and migration of ABIS system to the new Primary Data Center and Disaster Recovery site, as required. The BioSP shall provide an overall strategy and approach for migration of sites (including data) as part of their technical scope. The BioSP should carry out the transition and migration exercise in a manner, which reduces service outage.

The BioSP shall undertake the transfer of biometric solution and associated infrastructure to another Data Center facility. BioSP, on prior notice from PSA, shall deploy required personnel to undertake the migration and in setting up installation, configuration and commissioning of the solution at the new sites.

For overall transition and migration, the BioSP shall:

- Prepare a detailed strategy and approach for migration
- Obtain approval on the strategy and approach from PSA
- Undertake transition and migration as per the approved strategy and approach
- Ensure no physical damage is done to the systems during the migration
- Ensure that there is minimal downtime of PhilSys during migration
- Ensure that there is no data loss during the migration activity
- Test the success of migration
- Prepare a report detailing the migration activities including testing and its results to PSA
- Conduct DR drill as part of successful completion of the site set up

16.5 Training

(i) The BioSP shall impart training, to staff of PSA and its appointed party (a maximum of 40 participants), on the ABIS solution related to configuration, usage, API, performance tuning and measurement and technical reports. The training program shall involve both in-class and online training sessions. The BioSP shall develop the required training materials.

(ii) The venue for training will be provided by the BioSP.

(iii) The BioSP shall prepare the training curriculum and materials covering, but not limited to, the following topics:

- ABIS System Configuration and Administration (including backup and restoration)
- Manual Adjudication - Configuration, Integration and Adjudication Operation
- Forensic biometric matching analysis and evaluation/Forensic science training
- SDK tool kit libraries , Development, Configuration and Integration
- ABIS quality and accuracy management
- Data Quality Monitoring
- Performance Measurement and SLA monitoring

(iv) The following are the deliverables for the above-mentioned training:

- Training Calendar and Curriculum
- Training Material, Training Manual(s)
- Training Sessions
- Training Effectiveness Evaluation

16.6 Reporting

(i) The BioSP will report to PSA on various aspects of the project. The BioSP will prepare a reporting plan indicating reporting area, type of reports, mode of circulation, and reporting frequency. Upon PSA's approval, the recipients of these reports will be identified.

(ii) For the reports having an impact on the payment, service levels and penalties, the BioSP will submit a signed hard copy of the reports. The other reports can be sent through email to the recipients decided by the PSA.

(iii) The BioSP will be required to broadly prepare and submit reports under the four (4) categories: (i) ABIS, (ii) Data Quality, (iii) Incident and Issues, and (iv) SLA.

(iv) The details about these categories are provided below:

16.6.1 ABIS Reports

The ABIS reports will be on a daily basis and will be used to ascertain the need to improve the performance of ABIS on a continuous basis. These reports shall be made available online with managed access.

16.6.2 Data Quality Monitoring & Reporting

(i) The quality of captured data is related with accuracy of matching. It is therefore very important that the BioSP should continuously monitor the data quality and publish reports, generate exceptions in case quality goes below the threshold levels. Data quality monitoring is complementary to benchmarking and helps to analyze and correct the issues in the registration process. The primary objective is to identify the sources of the problems in quality and to take the corrective actions. The functionality will be implemented in the analytics module.

(ii) The BioSP will report on the following:

- **Quality of Data Capture and Matching**: Analysis on the quality of data in registration and accuracy of matching, and 1:N deduplications on a daily basis.
- **Data Mix-up**: Weekly reports regarding duplicates both False Positive and False Negative.
- **Quality of Performance of Operators and Devices**: The quality of data is also dependent upon the operator's training. Thus, to ensure the good quality of registration, the BioSP should submit a statistical and quality analysis report on the performance of operators and devices.

(iii) In summary, the BioSP should provision for following scope of work related with data quality monitoring and reporting:

- The BioSP should centrally administer image level quality checks and thresholds.
- The BioSP should implement a process that generates automated exception for image captures that do not meet quality standards. The BioSP should design and implement mechanism which would provide direct feedback of quality and capture related shortfalls to operators.
- The PSA may ask BioSP to enable or implement image enhancements feature to enhance biometric feature extraction to acceptable levels.
- The BioSP would present the statistical data to PSA on a weekly basis. This will help PSA to take a decision, in case threshold value of quality needs to be adjusted.

16.6.3 Incident and Issue Reporting

The incident and issue reporting shall be done by BioSP with respect to ABIS solution. The scope of these reports will include:

(i) Log of preventive / break-fix maintenance undertaken;

(ii) Summary of changes undertaken like configuration changes, application of patches, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.;

(iii) Summary of incidents reported like application down, components down, overall downtime, security vulnerabilities detected, hacker attacks / security threats, peaking of utilization, abnormal operation, etc.;

(iv) Bug/defect resolution reports including the analysis of defects resolved, pending, completion time, responsiveness, concern areas, etc.;

(v) Change Request Logs with their resolution status;

(vi) Incident Reporting (as and when it occurs)

- Complete system down – with root cause analysis;
- Peaking of resource utilization on any component;
- Bottlenecks observed in the system and the possible solutions and workarounds.

(vii) Security Incident Reporting (as and when it occurs)

- Detection of security vulnerability and available solutions / workarounds for fixing; and
- Hacker attacks, virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.

All incident and issue reports shall be made available online with managed access.

16.6.4 SLA Reporting

(i) BioSP shall be responsible for delivering the services described in the scope of work, as per the Service Levels given in this PBD. BioSP is also responsible for periodic monitoring and reporting of the Service Levels. BioSP should submit an SLA compliance report each month. BioSP shall also be responsible for providing early warning of any organizational, functional or technical changes that might affect BioSP's ability to deliver the services described in the Service Levels. Immediate actions should be taken to mitigate the risks or issues, if any.

(ii) To the extent possible, Service Level reporting should be undertaken using automated tools and should be done using the automated logs with minimal manual intervention. BioSP shall define and implement a process for those SLAs that require manual intervention for measurement and reporting.

(iii) BioSP shall prepare the reporting templates for Service Levels in compliance reports and obtain approvals from PSA. These reports should include "actual versus target" SLA performance, a variance analysis, and discussion of appropriate issues or significant events, if any.

17. Implementation Schedule

The implementation timeline for the BioSP in alignment with the program milestones are as follows:

Table 12. Implementation Schedule

No.	Key Activities of BioSP in alignment with program milestone	Timeline (in Months)
1	Issuance of Notice to Proceed	T
2	Mobilization of team and commencement of work	T + 0.5
3	Supply necessary licenses	T + 1.5
4	Delivery of sandbox and Multimodal SDKs with technical documentation	T + 2
5	Supply, implement and commissioning of IT hardware & system software data center and disaster recovery site	T + 3
6	Supply and customization/development of biometric solution (incl. integration)	T + 4
7	Deployment of manpower for helpdesk to address technical queries	T + 4
8	Benchmarking of Biometric Solution	T + 5
9	Acceptance of Biometric Solution	T + 5
10	Go-Live of ABIS Solution	T + 5.25

18. Knowledge Transfer & Exit Management

18.1 Knowledge Transfer

The BioSP must include a Knowledge Transfer milestone in its scope to ensure that on expiry of the engagement, PSA and its appointed party has the benefit of knowledge transfer. During the exit management process the following key activities shall be required to be performed by the BioSP:

(i) **Transfer of Assets:** The BioSP ensure transfer of assets to PSA three months before the date of expiry of contract/termination of contract.

(ii) **Co-operation and Provision of Information**: During the exit management period, BioSP shall allow PSA the access to information reasonably required to define the existing services being delivered.

(iii) **Confidential Information, Security and Data**: The BioSP will promptly, on the commencement of the exit management period, supply to the PSA and its appointed party the following:

- Latest documentation relating to project and any other data and all relevant information related to project;
- Project data for transitioning of the services to PSA in an agreed format;

- The BioSP is obliged to provide an access to PSA and any third party agency nominated by PSA in order to make an inventory of the assets (including hardware / Software / Active / Passive), layouts, diagrams, schematics, documentations, manuals, catalogue, archive data, IP addressing, live data, policy documents or any other material related to the Project; and
- All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable the PSA and its appointed party to carry out due diligence in order to transition the provision of the services.

18.2 Exit Management Plan

BioSP shall create an "Exit Management Plan" which shall deal with the following aspects:

(i) A detailed program of the transfer to be used to ensure continuation of the services throughout the transfer process;

(ii) The BioSP shall submit an inventory of assets to be turned over to the PSA;

(iii) Plans for provision of contingent support to PSA and third-party agency nominated by PSA during the transfer;

(iv) The Exit Management Plan shall be approved by PSA;

(v) The terms of payment as stated in the PBD Volume-I include the costs of the BioSP in complying with its obligations under this Section;

(vi) In the event of termination or expiry of SLA, Project Implementation, Operation and Management or Scope of Work each Party shall comply with the Exit Management Plan;

(vii) During the exit management period, the BioSP shall deliver the services based on the SLA;

(viii) Payments during the Exit Management period shall be made in accordance with the payment terms; and

(ix) This Exit Management plan shall be furnished in writing to PSA within 15 days from the receipt of notice of termination or three months prior to the expiry of the Contract.

The BioSP needs to ensure that the strategic control of entire biometric solution (including generated data/information) is transferred to PSA and its appointed party in a usable, operable and unrestricted manner.

19. Service Level Agreement

19.1 Service Levels

Service Levels defines services to be provided by BioSP to PSA for the duration of this contract. The SLA details are given below.

19.2 Definition of Terms

(i) **Registration Transactions** - refers to the transactions subject for de-duplication to determine if there exist any duplicate(s) in the gallery for the citizen or resident registered.

(ii) **False Positive Identification** - A term applying to de-duplication transactions only. An incorrect decision of a biometric system that an applicant for a PSN has previously been registered in the PhilSys, when in fact they have not been registered in the PhilSys.

(iii) **False Positive Identification Rate (FPIR)** - This applies to de-duplication transactions only. This is the ratio of number of false positive identification decisions to the total number of enrolled transactions by unenrolled individuals.

(iv) **False Negative Identification** - A term applying to de-duplication transactions only. An incorrect decision of a biometric system that an applicant for a PSN, not attempting to avoid recognition, has not previously been enrolled in the system, when in fact they have.

(v) **False Negative Identification Rate (FNIR)** - A term applying to de-duplication transactions only. This is the ratio of number of false negative identification decisions to the total number of enrollment transactions by enrolled individuals.

(vi) **False Acceptance** - A term applying to authentication transactions only. The decision of a biometric system that submitted biometric samples match enrollment data from a different data subject.

(vii) **False Match Rate (FMR)** - A term applying to authentication transactions only. This is the ratio of number of verification transactions conducted by data subjects resulting in a false match to the total number of transactions.

(viii) **False Rejection** - A term applying to authentication transactions only. The decision of a biometric system that submitted biometric samples do not match enrollment data of the same data subject.

(ix) **False Non Match Rate (FNMR)** - A term applying to authentication transactions only. This is the ratio of number of authentication transactions conducted by data subjects resulting in a false non match to the total number of transactions.

(x) **Successful De-Duplication** - means assurance through biometric comparisons that no enrolled person has been assigned more than one PSN.

19.3 Service Levels and Targets

This section provides the key performance indicator for this engagement. According to the procedures detailed in Section 19.4.3 SLA Change Process, the service levels may be reviewed and revised. The following section reflects the measurements to be used to track and report system performance on a regular basis. The targets shown in the following tables are for the period of contract.

19.4 SLA Framework

This section describes the SLA framework for this contract comprising of the following:

(i) Responsibilities of parties
(ii) Reporting procedures
(iii) SLA change process
(iv) Liquidated damages

19.4.1 Responsibilities of Parties

(i) PSA shall:

- Report defects and problems to the BioSP's representative at the earliest time possible.
- Assist BioSP in managing the SLA.
- Provide early warning of any organizational, functional or technical changes that might affect BioSP's ability to deliver the services described in the SLA.
- Assist BioSP in resolving production incidents.

(ii) BioSP shall:

- Be responsible in the delivery of services based on the performance targets detailed in this document.
- Be responsible in:
    - Reporting problems to PSA management at the earliest time possible;
    - Assisting PSA in managing the SLA;
    - Providing early warning of any organizational, functional or technical changes that might affect BioSP's ability to deliver the services described in the SLA; and
    - Assisting PSA in a timely manner in resolving production incidents.
- Immediately act to identify problems and take the appropriate action to fix them as quickly as possible.

19.4.2 Reporting Procedures

The BioSP shall prepare and submit SLA performance reports in an agreed format by the 10th working day of subsequent month of the reporting period. The reports will include "actual versus target" SLA performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports will be submitted to PSA.

19.4.3 SLA Change Process

The Parties may amend this SLA by mutual agreement in writing by either Party. The BioSP will initiate an SLA review at least bi-annually. Normally, the forum for negotiating SLA changes will be during BioSP's monthly meetings with the PSA. All negotiated SLA changes will require changing the version of the SLA control number. As appropriate, minor changes may be accumulated for periodic release (e.g. every quarter) or for release when a critical threshold of change has occurred.

19.4.4 Liquidated Damages

A maximum level of performance penalties is established and described below. The framework for performance penalties as a result of not meeting the Service Level Targets are detailed below:

(i) A quarterly performance evaluation will be conducted using the monthly reports covering that quarter.

(ii) Performance penalties shall be levied for not meeting each of the severity levels of performance as per the following table:

Severity Level	Penalty as a percentage of the contract price
9	Event of default and termination as per Contract
8	8.0 %
7	4.0 %
6	2.0 %
5	1.0 %
4	0.5 %
3	0.4 %
2	0.3 %
1	0.2 %

(iii) Performance Penalty for not meeting a measurement parameter for two consecutive quarters shall result in twice the penalty percentage of that respective measurement parameter.

(iv) Maximum Penalty applicable for any quarter shall not exceed 10% of the contract price for the respective quarter.

(v) Two consecutive quarterly deductions of 10% of the quarterly revenues on account of any reason will be deemed to be an event of default and may lead to termination of the contract.

19.4.5 Category of Service Levels

The Service Level Agreement (SLA) have been logically segregated in the following categories:

S. No.	Category Description	SLA Effectivity
A.	Implementation Phase	SLA Category before Go-Live
B.	Solution related performance levels (ABIS)	SLA Category after Go-Live
C.	Operations	SLA Category after Go-Live
D.	Troubleshooting / Issue Resolution	SLA Category after Go-Live

19.4.6 Service Levels and Targets

Category-I: Implementation Phase

#	Service Level	Definition	Target	Consequence / Severity in case of Penalty
A1	Team mobilization and commencement of work	The BioSP is expected to mobilize the team for commencement of work for this project. The commencement of work would mean deployment of BioSP resources at the designated PSA location for project & implementation planning, design.	Within 0.5 month from the date of release of Notice to Proceed	For each fortnight (or part thereof) of delay, sum equivalent to 0.5% of the contract price
A2	Supply of licenses for integration with PhilSys	Delivery of licenses, SDKs components required for the integration with PhilSys	Within 6 weeks from the date of release of Notice to Proceed	For each fortnight (or part thereof) of delay, sum equivalent to 0.5% of the contract price
A3	Delivery of sandbox	Delivery of end-to-end sandbox environment that can cater to one million records	Within 2 months from the date of release of Notice to Proceed	For each fortnight (or part thereof) of delay, sum equivalent to 0.25% of the contract price
A4	Installation and Commissioning of Hardware at Primary and Disaster Recovery sites for production environment	Delivery, installation, integration, testing of all components / equipment required for the system, to the satisfaction of the PSA	Within 3 months from the date of release of Notice to Proceed	For each fortnight (or part thereof) of delay, sum equivalent to 0.5% of the contract price

#	Service Level	Definition	Target	Consequence / Severity in case of Penalty
A5	Installation and Commissioning of Biometric Solution in production environment at Primary and Disaster Recovery sites	Delivery, installation, integration, testing of all components / equipment required for the solution	Within 4 months from the date of release of Notice to Proceed	For each fortnight (or part thereof) of delay, sum equivalent to 0.5% of the contract price
A6	Completion of acceptance and Go-Live of the ABIS Solution at both Primary and Disaster Recovery sites	Completion of acceptance testing and Go-Live of the ABIS solution	Within 5.25 months from the date of release of Notice to Proceed	For each fortnight (or part thereof) of delay, sum equivalent to 0.5% of the contract price

Category-II: ABIS Solution-Related Performance Levels

The performance targets for the service level measurements during any period of assessment may be revised to align with the international benchmarks. May be revise upon consultation between PSA and BioSP.

#	Service Level	Definition	Target	Consequence / Severity in case of Penalty
B1	False Positive Identification Rate (FPIR)	FPIR = (Number of false positive identification decisions for the month) / (total number of enrollment transactions by unenrolled individuals for the month).	<= 0.1% measured per month	None
			> 0.1% and <= 2% measured per month	Penalty of severity level: 7
			> 2% measured per month	Penalty of severity level: 8; Penalty of severity level: 9 (if breach occurred for two consecutive cycles)
B2	False Negative Identification Rate (FNIR)	FNIR = [(Number of false negative identification decisions for the month) / (total number of enrollment transactions by unenrolled individuals for the month)] @ FPIR <= 0.1%. FNIR @ FPIR <= 0.1%	<= 1% measured per month	None
			> 1% and<= 2% measured per month	Penalty of severity level: 7
			> 2% measured per month	Penalty of severity level: 8; Penalty of severity level: 9 (if breach occurred for two consecutive cycles)
B3			=< 24 hours	None

#	Service Level	Definition	Target	Consequence / Severity in case of Penalty
	Response Time per De-duplication check	Response Time = Average elapsed time between submission of a registration request to Biometric Solution and generation of response (Success or failure of de-duplication)	>24 hours to <=30 hours	Penalty of severity level: 5
			>30 hours to <=36 hours	Penalty of severity level: 6
			>36 hours to <=48 hours	Penalty of severity level: 7
			>48 hours	Penalty of severity level: 8
B4	Uptime	Uptime = {1 - [(Downtime) / (Total Time – Maintenance Time)]}	Minimum 99.5% up time measured on a monthly basis	None
			>= 99% to <99.5% up time measured on a monthly basis	Penalty of severity level: 4
			<99% up time measured on a monthly basis	Penalty of severity level: 6

Category-III: Operations

#	Service Level	Definition	Target	Consequence / Severity in case of Penalty
C1	Resource availability for Support and Maintenance of ABIS	No. of shift days (8 hours per shift day) for which resource present at the designated location / Total no. of shift days	• 99% averaged over all resources designated for BioSP services and calculated on a monthly basis	None
			• >=97 % to < 99% averaged over all resources designated for BioSP services and calculated on a monthly basis	Penalty of severity level: 6
			• >=95 % to < 97% averaged over all resources designated for BioSP services and calculated on a monthly basis	Penalty of severity level: 7
			• < 95 % averaged over all resources designated for BioSP services and calculated on a monthly basis	Penalty of severity level: 8
C2	Resource availability for Helpdesk	No. of shift days (8 hours per shift day) for which resource present at the designated location / Total no. of shift days	• 99% averaged over all resources designated for BioSP services and calculated on a monthly basis	None
			• >=97 % to < 99% averaged over all resources designated for BioSP services and calculated on a monthly basis	Penalty of severity level: 1

#	Service Level	Definition	Target	Consequence / Severity in case of Penalty
			• >=95 % to < 97% averaged over all resources designated for BioSP services and calculated on a monthly basis	Penalty of severity level: 2
			• < 95 % averaged over all resources designated for BioSP services and calculated on a monthly basis	Penalty of severity level: 3
C3	Data Quality Monitoring & Reporting	Weekly reports	• Less than 100% adherence to timelines specified in Scope of Work	Penalty of severity level: 6
	SLA reporting	Monthly reports	• Less than 100% adherence to timelines in Scope of Work	Penalty of severity level: 6
	ABIS reporting	Daily Reports	• Less than 100% adherence to timelines in Scope of Work	Penalty of severity level: 6
	Incident and Issue Reporting	As and when it occurs	Less than 100% incidents to be provided to PSA along with appropriate notification within 2 hours with the cause, action and remedy	Penalty of severity level: 5

Category-IV: Troubleshooting / Issue Resolution

"Resolution Time" means time taken (after the incident call has been logged on the helpdesk) in resolving (diagnosing, troubleshooting and fixing) or escalating to the second level to respective O&M, getting the confirmatory details about the same from the O&M and resolving the same. Provisioning of standby resources, if required, should be done along with associated data being restored, services reinitiated, and SLA conditions being met. Final Resolution shall be deemed complete only after the original equipment is replaced / reinitiated along with data being restored to the correct state and services are resumed.

#	Service Level	Definition	Target	Consequence / Severity in case of Penalty
D1	Resolution Time (120 minutes) for Level 1 (L1) issues	• Time taken (after the call has been logged on the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level to respective O&Ms, getting the confirmatory details about the same from the O&M and resolving the same)	• Resolution of 98% of the total calls within the specified limit	None
			• Resolution of >= 97 to < 98 % of the total calls within the specified limit	Penalty of severity level: 4
			• Resolution of >= 96 to < 97 % of the total calls within the specified limit	Penalty of severity level: 5
			• Resolution of >= 95 to < 96 % of the total calls within the specified limit	Penalty of severity level: 6

#	Service Level	Definition	Target	Consequence / Severity in case of Penalty
		Provisioning of standby resources, if required, should be done along with associated data being restored, services re-initiated and SLA conditions being met. Final Resolution shall be deemed to be complete only after the original equipment is replaced / reinitiated along with data being restored to the correct state and services are resumed.	• Resolution of < 95 % of the total calls within the specified limit	Penalty of severity level: 7
D2	Resolution Time (8 hours) for Level 2 (L2) issues	• Time taken (after the call has been logged on the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level to respective O&Ms, getting the confirmatory details about the same from the O&M and resolving the same) Provisioning of standby resources, if required, should be	• Resolution of 98% of the total calls within the specified limit	None
			• Resolution of >= 97 to < 98 % of the total calls within the specified limit	Penalty of severity level: 4
			• Resolution of >= 96 to < 97 % of the total calls within the specified limit	Penalty of severity level: 5
			• Resolution of >= 95 to < 96 % of the total calls within the specified limit	Penalty of severity level: 6

#	Service Level	Definition	Target	Consequence / Severity in case of Penalty
		done along with associated data being restored, services re-initiated and SLA conditions being met. Final Resolution shall be deemed to be complete only after the original equipment is replaced / reinitiated along with data being restored to the correct state and services are resumed	• Resolution of < 95 % of the total calls within the specified limit	Penalty of severity level: 7
D3	Resolution Time (7 days) for Level 3 (L3) issues	• Time taken (after the call has been logged on the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the highest level of technical resources of the BioSP). Final Resolution shall be deemed to be complete only after a successful fix has been applied and documented.	• Resolution of 98% of the total calls within the specified limit.	None
			• Resolution of < 98 % of the total calls within the specified limit	Penalty of severity level: 6

Note:

Level 1 (L1) support means basic help-desk resolution and service desk delivery. L1 employs entry-level technical personnel, trained to solve known problems and fulfill service requests by following scripts, and escalate to L2 if no known solution is available.

Level 2 (L2) support is an in-depth technical support. Experienced and knowledgeable technicians assess issues and provide solutions for problems that cannot be resolved by Level-1. If no solution is available, Level-2 support escalates the incident to Level-3. L2 employs support personnel with deep knowledge of the product or service. L2 support can be provided remotely by BioSP off-site within the Philippines.

Level 3 (L3) involves support access to the highest technical resources available for problem resolution or new feature creation. Level-3 technicians are experts who attempt to duplicate problems and define root causes. Once a cause is identified, the engineer decides whether to create a new fix. New fixes are documented for use by L1 and L2 personnel. Level-3 specialists may include chief architects, or engineers who created the product or service. L3 support can be provided offsite from outside Philippines.

Appendices

20. Appendix A - MOSIP Tools and Technology

PSA will use the Modular Open Source Identity Platform (MOSIP) as its identity platform for the PhilSys solution. The MOSIP overview can be referenced at https://www.mosip.io/ and the MOSIP specifications can be referenced at https://github.com/mosip/.

21. Appendix B - Minimum Technical Requirement Specifications

(PSA to provide Data Center specifications as a Supplemental Bid Bulletin)

22. Appendix C – Compliance Statement

Technical Specification Requirements	**Specification (refer to page of Volume 2: Technical Specifications)**	**Statement of Compliance**
10. Biometric Solution	28	
10.1 ABIS solution design principles	28	
10.2 Biometric standards	29	
10.3 Interoperability Standards	29	
10.4 System Architecture Requirements	30	
10.5 Biometric Components	34	
10.6 ABIS Biometric Matcher	34	
11. Functional and Technical Requirements	35	
11.1 Enrollment	35	
11.2 Management	35	
11.3 Verification	36	
11.4 Data storage requirement	36	
11.5 Logging and monitoring	36	
11.5.1 ABIS Log	37	
11.5.2 Verification Log	37	
11.5.3 Management Functions Log	37	
11.6 Security Requirements	37	
11.7 Operator Interface Requirements	38	
11.8 Biometric Middleware	38	
11.9 Multimodal SDK	39	
11.9.1 Fingerprint	39	
11.9.2 Iris	39	
11.9.3 Face Photo	40	

Technical Specification Requirements	Specification (refer to page of Volume 2: Technical Specifications)	Statement of Compliance
11.10 Standards requirements	40	
11.11 Reliability Requirements	40	
11.12 Security Requirements	41	
11.13 User Interface Requirements	41	
11.14 Platform requirements	41	
11.15 Biometric Middleware	42	
11.16 Authentication Solution (SDKs and Integration Support)	42	
11.17 Biometric Manual Adjudication Solution	43	
11.18 Licensing Requirements	44	
11.19 Load Requirement	45	
12. Scope of Work	46	
12.1 Overview of scope of work	46	
12.2 Project Planning and Initiation	49	
12.3 Capacity Planning	50	
12.4 Requirements Analysis	51	
12.5 Solution Design	51	
12.6 Supply, Customization and Implementation of Biometric Solution	52	
12.7 Set up of Biometric Solution	52	
12.8 Integration Requirements	52	
12.8.1 Integration Requirements for PSA or its appointed party	52	
12.8.2 Integration Requirements for BioSP	53	
12.9 User Acceptance Testing (UAT)	53	
12.10 Roll out of Biometric Solution - ABIS Go-Live	53	

Technical Specification Requirements	Specification (refer to page of Volume 2: Technical Specifications)	Statement of Compliance
12.11 Conditions for re-templatization	54	
12.12 Setup of Data Center sites	55	
12.12.1 Data Center Strategy	55	
12.12.2 DC/DR set up in the interim	55	
12.12.3 Permanent DC/DR set up	55	
12.13 Transition and Migration of Data Center	56	
12.14 Biometric Solution Hosting Requirements	56	
12.14.1 Supply of Hardware	56	
12.14.2 Environment Creation	58	
13. Benchmarking, Acceptance and Go-Live	58	
13.1 Benchmarking	58	
13.2 Commissioning	61	
13.3 Acceptance	61	
13.4 Go-Live	61	
14. Manpower Requirement	61	
14.1 Guidelines for staffing and provisioning of manpower	61	
14.2 BioSP functions that can be performed off-site	62	
14.3 Replacement of Personnel	62	
14.4 Removal of Personnel	63	
14.5 Logistics requirements of the Personnel	63	
14.6 Escalation Matrix	63	
14.7 Deployment of Resources	63	
14.8 Profile Qualifications	64	
14.9 Indicative deployment schedule	66	

Technical Specification Requirements	Specification (refer to page of Volume 2: Technical Specifications)	Statement of Compliance
15. Ongoing Maintenance	66	
15.1 Maintenance Management	66	
15.2 Biometric Solution Management	67	
15.3 Infrastructure Management	68	
15.4 Information Security	69	
15.4.1 ISO certification readiness for Information Security Management	69	
15.4.2 Responsibility for the overall security of the biometric solution	69	
15.5 Help desk Support	69	
15.6 Business Continuity Support	70	
15.7 Warranty and Annual Technical Support (ATS)	71	
16. Project Management	71	
16.1 Project Status Monitoring and Reporting	71	
16.2 Risk and Issue Management	71	
16.3 Change Control Management	72	
16.4 Transition and Migration to new Data Center sites	72	
16.5 Training	73	
16.6 Reporting	74	
16.6.1 ABIS Reports	74	
16.6.2 Data Quality Monitoring & Reporting	74	
16.6.3 Incident and Issue Reporting	75	
16.6.4 SLA Reporting	75	
17. Implementation Schedule	77	
18. Knowledge Transfer & Exit Management	77	
18.1 Knowledge Transfer	77	

Technical Specification Requirements	Specification (refer to page of Volume 2: Technical Specifications)	Statement of Compliance
18.2 Exit Management Plan	78	
19. Service Level Agreement	79	
19.1 Service Levels	79	
19.2 Definition of Terms	79	
19.3 Service Levels and Targets	80	
19.4 SLA Framework	80	
19.4.1 Responsibilities of Parties	80	
19.4.2 Reporting Procedures	81	
19.4.3 SLA Change Process	81	
19.4.4 Liquidated Damages	81	
19.4.5 Category of Service Levels	82	
19.4.6 Service Levels and Targets	83	

Conforme:

____

Name of Company

____

Name and Signature of Company Authorized Representative

____

Date

23. Appendix D – Use Cases for PhilSys

A. Priority use cases

This section elaborates on use cases that are of immediate importance for the PhilSys. The exact timing for the implementation of these use cases will depend on the readiness of relying parties and the final registration strategy.

1) Targeting and delivery of the Pantawid Pamilyang Pilipino Program (4Ps)

The cornerstone of social protection in the Philippines is the *Pantawid Pamilyang Pilipino* Program (4Ps; Bridging Program for the Filipino Family), which is implemented by the Department of Social Welfare and Development (DSWD). Through 4Ps, poor households with three (3) children in high school can receive a maximum conditional cash transfer of up to PHP 6,900 every two months for complying with a range of health and education conditions. 4Ps is anchored on the paradigm of breaking the intergenerational cycle of poverty by keeping children in school and healthy. Cash is primarily delivered to an eligible grantee, usually the female head of household, through a cash card from Land Bank. In areas where ATMs are less accessible, off-site cash payments are scheduled or payments are made over-the-counter through rural banks, cooperatives and NGOs.

As of 30 June 2019, 4Ps is being implemented in 144 cities and 1,483 municipalities in 80 provinces, with a total of 4,893,346 registered households since the program started in 2008. Out of the total number of registered households, 4,123,829 are active households or 93.72% of this year’s target of 4.4 million households.

4Ps uses a national household targeting system known as Listahanan to identify the poor households to benefit the program. Listahanan is an information management system that identifies who and where the poor are, which is created through a survey of over 15 million households every five years (last in 2015; to be carried out in 2019), covering approximately 75% of the Philippine population. A proxy means test (PMT) is used to determine which households are poor. No unique identifier is collected at the time of the Listahanan survey, and no deduplication takes place. Each household in the Listahanan is assigned a 16-digit number, which has a logic based on its geographic location. There is no unique identifier for individual household members.

4Ps operates three major information systems: Beneficiary Update System (BUS), Compliance Verification System (CVS), and Grievance Redress System (GRS). The BUS records changes on the status or condition of households. It captures recent information about household members to serve as basis in monitoring compliance of beneficiaries. Updating is a continuous process to ensure that the beneficiaries are availing the maximum health and education grants. The CVS monitors the compliance of households with the conditions of the program as basis for the provision of grants. On the other hand, complaints were encoded and recorded in the GRS through various modes such as calls, grievance forms, social networking sites, courier, and electronic mail. The 4Ps information systems are anchored on the eight major steps in the implementation of the program, namely: 1) Selection of Provinces/ Cities/ Municipalities; 2) Supply Side Assessment; 3) Selection of Households; 4) Registration and Validation of Households; 5) Family Registry; 6) Release of Initial Grants; 7) Compliance Verification; and 8) Release of Succeeding Cash Grants.

Beneficiary registration / community assembly serves as a beneficiary entry point into the Program. It is conducted to gather identified potentially eligible beneficiaries for validation and registration/ enrollment and to orient enrolled beneficiaries about the program. DSWD considers validation of potentially eligible households as the most important activity of the community assembly, because it is through it that the information on eligible households and their members is checked, corrected and updated and their program eligibility is verified. To be deemed eligible for the program, the households should be a resident in the area selected for the program roll-out, should be identified as poor by *Listahanan*, and must have a pregnant member or at least one child 0-18 years old. Once the household is positively validated and verified, it is registered with the program and called a "*Pantawid Pamilya* beneficiary household".

At the registration, the grantee of the registered household is identified. The program design stipulates that a grantee should be a mother in the household. If there is no mother in the household, than an adult household member is authorized to receive and withdraw the grants. Grantees must be included in the household roster. Once the grantee is identified, she/ he chooses who from among the children in the household would be monitored for school enrollment and attendance. The maximum number of children that could be selected for education monitoring is three. To be selected for education monitoring a child should be 3-18 years of age, be a child/ grandchild in the family and included/ listed in the household roster reported to *Pantawid*.

After the registration, the grantee fills the Land Bank Cash Card Enrollment Form. The data stated in the form is verified for accuracy. All validated beneficiaries are asked to sign an *Oath of Commitment* as a confirmation of their agreement to comply with *Pantawid*'s conditions. The signing of the Oath of Commitment signals that the beneficiaries have fully understood and accepted *Pantawid*'s conditions and commit themselves to complying with them. This Oath serves as a living proof of the program acceptance. The signing of the *Oath of being a new Pantawid Pamilya beneficiary* is meant to ensure that neither a household nor any of its members had previously been registered with the program. This is expected to help minimize registration duplicates.

A photo of each grantee is taken to be attached to the Land Bank Cash Card Enrollment Form and to issue the *Pantawid* identification card (ID), which has a unique beneficiary household number, which is the same as the household's *Listahan* number. The Regional Project Management Office (RPMO), together with the Working Team is responsible for the *Pantawid* ID picture taking. Once this has been completed, the grantee signs the ID. The ID is for parent grantees, not for children. If grantees can't read or write, then grantees use their thumbmark to sign the registration documents. To the extent possible, the ID cards are handed to the grantees on the actual day of community assembly. To make sure that the grantee's identity is true, DSWD requires that an official from the LGU or barangay is present to witness the picture taking and the ID issuance and to confirm the identity of newly enrolled beneficiaries. If for some reason the IDs are not released to grantees during the assembly, they are subsequently informed about the release of the ID and Cash cards by the Municipal/City Link in coordination with the Municipal/City Social Worker.

The *Pantawid* ID is an identification (ID) card provided to all heads of households in 4Ps. The ID card can be used to establish eligibility to claim benefits, such as the monthly grants and National Health Insurance Program (NHIP) benefits. The card does not have any security features nor authentication mechanism beyond the photo and this, combined with the glued-on photo, makes it easy to forge.

The Oath of Commitment of Pantawid program signifies the co-responsibilities between the government and the beneficiaries to strengthen the commitment to invest in human capital and to improve lives of the family-beneficiaries and their children. The oath is signed by the beneficiary upon registration into the program to signify his/her duty to comply with the conditionalities that are anchored on health and education.

Encoding and approval of registered households: City/Municipal Linkss check and clean collected beneficiary information prior to encoding it into the Community Assembly Registration System (CARS) by checking completeness, accuracy and validity of the CA update forms. The RPMO spot checks beneficiary information as part of the final quality audit. Once the quality check is completed, the Regional Director approves the encoded registered households. There are online and offline versions of CARS.

Based on anecdotal evidence and according to Beneficiary Data Management Division (BDMD), it takes about 6-7 months for the registration and validation process to be completed.

The 16-digit household number issued by the *Listahanan* is also used for the administration of the 4Ps, and this number is displayed on the card.

Following the completion of the 2019 *Listahanan* survey and 4Ps targeting process, the use cases of the PhilSys for the 4Ps will be:

- **Unique identifying all beneficiaries and seeding PSNs or PSN tokens:** PSNs and/or PSN tokens should be over time validated and seeded in the 4Ps information systems to help DSWD ensure that each beneficiary is recorded only once and in only one household. This process should involve obtaining the informed consent of beneficiaries, including on behalf of minors. Minors younger than five are unlikely to be registered by PhilSys for some time (e.g. 2022) so they will not have a PSN. The process for resolving potential duplicates will be separate and the responsibility of DSWD, and should not involve gaining access to the PhilSys registry. This use case is likely to involve substantial process and system re-engineering on the side of DSWD, as well as the procurement of hardware to carry out authentication.
- **Verifying the identity of beneficiaries at payment and grievance redressal:** DSWD should have the capability to periodically or on-demand verify the identity of the grantee (head of household) or their designees before or at the time of payment to help

ensure that the right person is receiving the payment (e.g. that the funds are not being intercepted) or when they are reporting a grievance in a DSWD office at the city or municipality level. This use case is likely to involve substantial process and system re-engineering on the side of DSWD, as well as the procurement of hardware to carry out authentication.

- **In the longer-term, using the PSN or PSN tokens to validate compliance:** Systems to check compliance with the health and education conditions are organized at the city and municipal level. For example, local schools and health facilities will manually report compliance to the local DSWD office, using the 16-digit household number or beneficiary names as a reference. Once the PSNs or PSN tokens are seeded into relevant information systems, opportunities to streamline compliance reporting, using the PSNs or PSN tokens, should be explored (e.g. automated reports by local health facilitates and schools sent to local DSWD offices).

Any solution for the 4Ps use cases must take into account that these beneficiaries are the poorest and among the most vulnerable segment of Philippine society. Of upmost importance is ensuring inclusion, not creating new barriers for accessing 4Ps benefits, and having readily available exception handling mechanisms. Many households are in remote and far-flung areas with limited or no reliable connectivity and beneficiaries are likely to have limited literacy and means and capability to use technology (e.g. no mobile phone or no smartphone). Households are known to share mobile phones within and among themselves. Furthermore, their biometrics are likely to be of worse quality than others in the Philippines, which could lead to increased error rates for fingerprint matching.

2) Financial account opening

The 2017 Global Findex Survey found that only 34% of Filipinos aged 15 and older had an account with a financial institution, which was only a modest increase from 31% in 2014 and no increase among the poorest 40% of the population. This translates to approximately 48 million Filipinos aged 15 and older without a financial account. By comparison, the rate of account ownership among all economies in East Asia and the Pacific was 74% in 2017, and among all lower-middle income economies worldwide it was 58%.

According to the BSP dashboard on financial inclusion in the Philippines for the first quarter of 2019, there were 12,378 bank offices and branches (including 1,892 branch-lites). 1,101 cities and municipalities have a banking presence, while 465 have some other kind of financial access point and 68 have no access point.

Customer Due Diligence (CDD) (or Know Your Customer (KYC)) regulatory requirements for identity verification are a major constraint to financial inclusion, deepening and integrity in the Philippines. In the Philippines, these requirements are set by the BSP through the Implementing Rules and Regulations of Republic Act No. 9160 (or the Anti Money Laundering Act), which were last amended in 2016. While the BSP has introduced simplified CDD regulatory requirements for low-value accounts, many financial institutions decide to still require one specific or two or more identification documents as part of the customer onboarding process because of the perceived risks, and the issues around the quality of existing identification noted in the background section of this document. A ‘lack of necessary documentation' (45%) was the third most cited barrier by those who do not have a financial (following 'insufficient funds' at 69% and 'too expensive' at 53%), which is also the third highest rate of any economy behind Madagascar (50%) and Zimbabwe (49%). In addition, 41% cited that financial services were too far away.

The PhilSys will help directly address the 'lack of necessary documentation barrier' because its universally-accessible credentials, by themselves and following authentication, should allow all Filipinos and resident aliens to meet the CDD regulatory requirements for identity verification (but not other requirements, such as beneficial ownership and sources of funds). The PhilSys will also provide a valid proof of address. Furthermore, by reducing paperwork and manual processes by financial institutions as part of the identity verification part of the onboarding process, the PhilSys will contribute to reducing the cost for financial institutions to onboard customers, which will hopefully lead to reduced fees for opening and maintaining accounts. Finally, the PhilSys will also contribute to expanding the delivery of financial services by allowing agents to go to underserved communities (e.g. because they do not have brick-and-mortar branches) with equipment (e.g. tablets or point of sale devices) that can leverage the PhilSys for customer onboarding.

The use case of the PhilSys for financial inclusion will be:

- **Verifying the identity of customers as part of Customer Due Diligence (CDD) requirements for financial account opening:** The PhilSys, by itself, should facilitate various methods of reliable verification of the identity of customers to comply with the IRRs of R.A. 9160. As an 'e-KYC' verification, this process, following consent, should also facilitate the secure transmission of specific data attributes required under the IRRs in a standardized and machine-readable format (e.g. XML) to pre-fill the financial institutions electronic forms. The level of assurance provided should be enough to not require the financial institution to require other documents for the purposes of identity verification. There should be different methods of authentication offered for both online and offline contexts, including without the need for a face-to-face interaction. This use case is likely to involve substantial process and system re-engineering on the side of participating financial institutions, and may require enabling amendments to the IRRs or circulars by the BSP.

Any solution for the financial inclusion use case must comply with relevant laws and regulations, as well as best practices in terms of data protection and privacy. Furthermore, any solution must minimize costs to financial institutions for adopting the PhilSys as part of their customer onboarding process.

3) Management of social insurance

The Social Security System (SSS) and Government Social Insurance System (GSIS) are government-owned and controlled corporations that provide social insurance (e.g. pensions and health insurance) and related financial services to non-government and government workers respectively. The SSS has more than 35 million members (of which 15 million were paying members during the period January to June 2019) and the GSIS has 1.8 million active members. The SSS operates 291 branches across the country and GSIS has 42 branches. Both organizations also provide services through their website, call center and smartphone apps. GSIS operates self-service kiosks in its branches and major government buildings.

The SSS and GSIS operate their own information systems to manage their registry of members and service delivery. Both also use the Unified Multi-purpose Identification (UMID) smartcard and the Central Verification System (CVS) to deduplicate and authenticate their members and, in the case of GSIS, as a cash card (e.g. for accessing advances and loans). The CVS is operated by the PSA, based on data submitted separately by SSS and GSIS, which includes four fingerprints for deduplication. Each unique registrant is assigned a Customer Reference Number (CRN), which becomes their member number and is used for portability between these schemes and with others such as the H. After being processed in the CVS, SSS and GSIS will have their private partner produce the contactless UMID smartcard, including fingerprints for authentication in branches and at kiosks. As of July 2019, there were 21 million records in the CVS and 12 million UMID smartcards have been issued.

The precise relationship between the PhilSys and the UMID/CVS will be subject to the transition plan that PSA will develop in collaboration with SSS and GSIS.

The use cases of the PhilSys for social insurance delivery by SSS and GSIS will be:

- **Uniquely identifying all members and seeding PSNs or PSN tokens:** PSNs and/or PSN tokens should be over time validated and seeded in the SSS and GSIS information systems as well as the CVS to help ensure that each beneficiary is recorded only once. This process should involve obtaining the informed consent of beneficiaries. The process for resolving potential duplicates will be separate and the responsibility of SSS and GSIS, and should not involve gaining access to the PhilSys registry. This use case may involve substantial process and system re-engineering on the side of SSS and GSIS, as well as the procurement of hardware to carry out authentication.
- **Verifying the identity of members:** SSS and GSIS should have the capability to periodically or on-demand verify the identity of members or their designees before or at the time of registration, service delivery (e.g. loan application), payment, and grievance. This use case is likely to involve substantial process and system re-engineering on the side of SSS and GSIS, as well as the procurement of hardware to carry out authentication.
- **Proof of life for pensioners:** SSS and GSIS should have the capability to periodically or on-demand verify the identity of pension beneficiaries to ensure that they are still alive and thus still eligible to receiving benefits.

4) Universal health coverage

The Philippines has long had a policy to implement universal health coverage. The main insurers are the Philippine Health Insurance Corporation (PhilHealth), a government-owned and controlled corporation attached to the Department of Health, SSS, GSIS and private insurers. According to the 2017 National Demographic Health Survey, 66% of the population receive health insurance through PhilHealth, 22% through SSS, 3% through GSIS, and 2% through private insurers. Meanwhile, 31% of the population reported having no health insurance coverage. Currently PhilHealth operates eight programs and its own registry of more than 90 million records, which are not deduplicated. PhilHealth provides a very basic paper-card for its members but also offers a voluntary PVC-plastic cards for a fee.

A significant reform is underway. The landmark Republic Act No. 11223 (or the Universal Health Care Act), signed into law in February 2019, guarantees for all Filipinos the full range of high-quality health care services – from preventive to promotive, curative, rehabilitative, and palliative – at affordable cost. Implementation of the Universal Health Care Act will involve automatically including all Filipino citizens into the National Health Insurance Program (NHIP) to be administered by PhilHealth, which will also have a greater role in purchasing health goods and services and improving health facilitates. Beneficiaries will not have to provide identification when accessing health services.

Beneficiaries will be split into Direct Contributors (e.g. formal workers, migrant workers, and lifetime members) and Indirect Contributors (e.g. indigents and senior citizens) who will be subsidized by the Government. The new model for health insurance delivery will therefore require accurate and efficient data sharing between PhilHealth, SSS, GSIS and other insurers, as well as other information systems (e.g. *Listahanan*) to target Indirect Contributors and to prevent fraud and leakages. The PhilSys will play a key role in facilitating this, drawing on the experiences of other countries, such as Thailand, who have used their foundational identification system to enable reliable data sharing across public and private health insurance programs.

The use cases of the PhilSys for universal health insurance delivery will be:

- **Uniquely identifying all benefciaries and seeding PSNs or PSN tokens:** PSNs and/or PSN tokens should be over time validated and seeded in PhilHealth, SSS, GSIS and private health insurer information systems as well to help ensure that each member is classified correctly as Direct or Indirect Contributors in the NHIP, including movement between different health insurance programs. This process should involve obtaining the informed consent of beneficiaries, including on behalf of minors. Minors younger than five are unlikely to be registered by PhilSys for some time (e.g. 2022) so they will not have a PSN. The process for resolving potential duplicates will be separate and the responsibility of DSWD, and should not involve gaining access to the PhilSys registry. The process for resolving potential duplicates will be separate and the responsibility of respective insurers, and should not involve gaining access to the PhilSys registry. This use case may involve substantial process and system re-engineering on the side of PhilHealth, SSS, GSIS, private health insurers and health facilitates.
- **Verifying the identity of members:** Health insurers and service providers should have the capability to periodically or on-demand verify the identity of members or their designees before or at the time of registration, service delivery, payment, and grievance. This use case is likely to involve substantial process and system re-engineering on the side of health insurers and health facilities, as well as the procurement of hardware to carry out authentication. Critically, failed authentication should never lead to a denial of health service, which necessitates the existence of exception handling mechanisms.

5) Obtaining authenticated civil registration certificates

The PSA's central civil registration repository, the Civil Registry System (CRS), contains more than 166 million digital civil registration records, including more than 115 million birth registration records. Records from before 2002 were digitized through optical character recognition (OCR) and manual data entry on demand, after requested have been made for certificates related to those records. While the actual act of registration is carried out by Local Civil Registration Offices (LCROs) in each city or municipality (and reporting to the mayor), this data is reported to the CRS, usually within 4-6 weeks. Each birth registration record is assigned a Birth Registration Number (BReN) when it reaches the CRS, and this BReN is included on any 'authenticated' birth certificate issued by the PSA.

The 'authenticated' civil registration certificates issued by the PSA are typically what service providers will require if they need evidence of identity or of a birth, marriage, death or other vital event. They can be purchased through a website (www.ecensus.gov.ph), by phone or through 40 service points (known as '*Serbilis* Centers') in urban centers. The CRS IT system is developed and maintained by a private partner through a public-private partnership (PPP), which goes through 2029. The private partner also manages the website, call center, *Serbilis* Centers, and distribution of 'authenticated' certificates.

The PSA receives 60,000-80,000 requests for 'authenticated' certificates per day (or around 10.5 million per year). Customers have their identity verified by providing exact details on the record for which they are requesting an 'authenticated' certificate. This is prone to potential identity theft and there is therefore an opportunity to improve the speed, accuracy and integrity of this verification process.

The use case of the PhilSys for civil registration certificates will be:

- **Verifying the identity of customers for purchasing civil registration certificates:** The PhilSys, by itself, should facilitate various methods of reliable verification of the identity of customers requesting a civil registration certificate from the PSA either through the website, by phone, or at *Serbilis* Centers.

In the medium-run, the PSA plans to seed the PSN into each person's civil registration records, including for their birth, death, marriage and other vital events. For future vital events, this will happen as they are registered. For past vital events, this will be done gradually, as people request copies of their certificates, so that consent can be obtained and to ensure that the right PSN is being seeded into the right records.

6) Passport renewals

The Department of Foreign Affairs (DFA) issues approximately three million passports every year. Roughly 15 million passports are active at any given time. Each application involves the collection of four fingerprints, which are used for deduplication purposes, as well as authentication for renewals. New applications undergo a rigorous identity proofing procedure (including nationality verification) that involves multiple identification documents and an 'authenticated' birth certificate. Renewal applications have a simplified procedure, with just one identification document required, as the identity verification uses existing data at the back-end (i.e. not at the time of applying). Applicants typically have to book an appointment at a

DFA office (or mission abroad). The standard processing period for new and renewal applications is 10-15 days. For an additional fee, a customer can expedite this process.

The use case of the PhilSys for passport renewals is:

- **Verifying the identity of customers for passport renewals:** The PhilSys, by itself, should facilitate various methods of reliable verification of the identity of customers and facilitate matching against their existing passport record (using their old passport number). As an ‘e-KYC’ verification, this process, following consent, should also facilitate the secure transmission of specific data attributes required for the passport application to carry out the matching. The level of assurance provided should be enough to not require DFA to require other documents for the purposes of identity verification.

In the medium-run, the DFA should have the opportunity to move passport renewal applications to online channels, potentially without the need for any face-to-face interaction.

B. Other important use cases

1) Electronic signatures

Republic Act No. 8792 (the Electronic Commerce Act) provides that no electronic document or message, regardless of technology type, shall be denied legal effect because it is in electronic form. Like a ‘wet’ or handwritten signature on a physical document, an electronic signature (or e-signature) verifies a person or legal entity’s acceptance of the content of a document or a collection of data linked to that signature, but in a digital format (e.g. through a website or smartphone app). Electronic signatures, which are a service typically offered by Governments and/or private sector ‘trust service’ providers, can provide greater assurance than ‘wet’ signatures because technology can more easily allow relevant parties to see if a signature or the document or data it is linked to has been modified. Furthermore, by linking electronic signatures to a national digital ID system such as the PhilSys, relevant parties can more reliably link the electronic signature with the signee. If a digital ID system answers the questions “who are you?” and “are you who you say you are?”, electronic signatures answer the question “do you commit or agree to this transaction, service or terms and conditions?”.

Electronic signatures are a fundamental component of the digital economy and digital government. Aside from bringing greater integrity to contracts and commerce in the Philippines, it will also enable service providers to provide even greater value-added services through online channels, such as formal notarization of documents, property transfers, and credit applications. By reducing the onboarding costs and risk to financial service providers, there is an opportunity to reduce the cost of credit.

In order to allow for the PhilSys to focus on reaching high-levels coverage and adoption, the PhilSys itself may not facilitate electronic signatures in the short-term. However, it should allow ‘trust service providers’ to onboard customers, reducing their risks, costs and time for creating electronic signature accounts. Eventually, as the market and Government policy on electronic signatures mature matures and grows, the PhilSys may itself offer electronic signature capabilities, such as through a special method of authentication.

2) Digital government services

An increasing number of departments, agencies and LGUs are shifting their Government to Citizen (G2C) and Government to Business (G2B) online. The Department of ICT (DICT) has a number of related initiatives, including development of a National Government Portal (NGP) to serve as a single-entry point and the Philippine e-Government Interoperability Framework (PeGIF) to facilitate back-end data exchange. The ability to offer many services online, without a face-to-face interaction, is dependent on being able to verify the identity of customers with a high-level of assurance, as well as to be able to accept electronic signatures that have the same legal effect as 'wet' signatures.

The use case of the PhilSys for digital government services is to facilitate verification of the identity of customers through online channels. The PhilSys should be able to be linked to electronic signature service providers (e.g. Certificate Authorities) to facilitate secure electronic transactions.

3) Developing a dynamic Listahanan National Household Targeting System and supporting future social protection programs

The *Listahanan* is a registry of over 15 million households that is compiled every five years (last in 2015; to be carried out in 2019 to 16.1 million target households), covering approximately 75% of the Philippine population, for the purposes of targeting social welfare services using a proxy means test (PMT). As of March 2018, 1,252 entities (e.g. Government departments and agencies and local government units (LGUs) were using the *Listahanan* to identify poor households, including 59 national-level programs (including the 4Ps and Sustainable Livelihoods program). No unique identifier is collected at the time of the *Listahanan* survey, and no deduplication takes place. Each household in the *Listahanan* is assigned a 16-digit number, which has a logic based on its geographic location. There is no unique identifier for individual household members.

The use case of the PhilSys for the *Listahanan* is to support the shift away from a survey every five years to a more dynamic data collection model (e.g. real time data sharing between social welfare and social security stakeholders). This will make the overall social protection system in the Philippines more responsive and adaptive as households move above and below the poverty thresholds.

Furthermore, an enhanced *Listahanan* and dynamic social registry will facilitate rapid deployment of future programs, such as the unconditional cash transfer (UCT), which was introduced through the Government's Tax Reform for Acceleration and Inclusion (TRAIN) under the Comprehensive Tax Reform Program, for the poorest 10 million households and individuals to offset the moderate but temporary increase in prices due to other measures of TRAIN. One of the challenges in delivering the UCT was targeting the right beneficiaries, which in the end comprised 4.4 million 4Ps beneficiary households, 3 million senior citizen-beneficiaries of the Social Pension Program, and 2.6 million of the next poorest households identified by *Listahanan*.

4) Credit information

The Philippines ranks relatively low in terms of credit information coverage. One of the main challenges is the inability for credit bureau to unify data from different sources because of the absence of a ubiquitous unique identifier. While the Tax Identification Number (TIN) is currently used by the credit bureaus for this purpose, the TIN is not fully deduplicated. The present situation has made it more challenging for people to access credit through formal channels. A 2017 survey by the BSP found that 40% of Filipinos with an outstanding loan obtained loans from informal sources.

The use case of the PhilSys for credit history is for financial institutions to seed PSNs and PSN tokens, and for the credit bureau to be able to use this information to uniquely identify persons and to efficiently collate relevant data on the same person from a variety of sources, including those who have defaulted.

5) Targeting and delivery of humanitarian assistance, including emergency cash transfers (ECT)

The Philippines experiences many natural disasters every year, including typhoons, earthquakes and volcano eruptions. According to the Joint Typhoon Warning Center, around 80 typhoons develop near the Philippines every year, 19 enter its territory, and six to nine make landfall. The impact of this is millions of people internally-displaced and hundreds of millions, if not billions, of dollars of damage. For instance, the Philippines was devastated in 2013 by Typhoon Haiyan, which killed at least 6,300 people, displaced 4 million and caused an estimated US$2 billion in damage. Among the damage is often the loss of personal property, including IDs and birth certificates, which can hamper the ability for the Government and relief agencies to effectively respond to such disasters. Most recently, the Government carried out a registration of internally-displaced persons from the Marawi siege, in order to profile the affected population and deliver targeted assistance, and established a management information system (MIS), but there have been challenges in implementation due to the ad-hoc nature of this project. A more systematic approach to registering affected and displaced persons is needed, which could be enabled by a foundational identification system.

DSWD recently adopted guidelines for emergency cash transfers, which are geographically targeted to affected areas along with other criteria such as 4Ps beneficiaries and certain vulnerable populations. The aim is to use information from *Listahanan*, which may be out of date in terms of the locations and composition of families and thus some affected households could be excluded when the ECT is applied while unaffected households who have moved from the location may still be counted as a beneficiary.

The use case of the PhilSys for humanitarian assistance and ECT delivery is to enable DSWD, other agencies and non-governmental organizations to reliably verify the identity of affected persons before, during and after natural disasters and other shocks to ensure that the right people are receiving the right assistance, such as the ECT. This will include the ability to quickly compile lists of affected persons, depending on PSNs to establish uniqueness. Furthermore, after a disaster, data collected (e.g. on persons who may have become disabled) can be shared, following consent, with appropriate authorities to render the necessary services. Any solution should take into account that emergency situations often result in no or low connectivity and electricity, and that many affected persons may not have any credentials with them.

C. Extended list of use cases

User	Identity authentication for transaction (e.g. to trigger a payment)	e-KYC for enrollment	Uniqueness (seeding validated PSN token)
AFP - Recruitment	X	X	
Airlines/Airports	X		
Banks - Accounts and Applications	X	X	
Barangays	X	X	X
BI - ACR-I Card	X	X	X
BIR - Customs	X		
BIR – TIN	X	X	X
CFO	X		
CHE	X	X	X
Cities and Municipalities	X	X	X
COMELEC - Voter registration		X	X
Credit bureaus			X
CSC	X		X
DA - Farm loans and subsidies	X	X	X
DepEd - Learner Reference Number	X	X	X
DFA - Passports	X	X	X
DICT - National Government Portal	X	X	
DOH - Electronic Health Records	X		X
DOJ - Access to justice	X	X	
DOLE – Alien Employment Permit,	X	X	
DSWD - Listahanan			X
DSWD - Regular programs (4Ps, Supplemental feeding)	X	X	X
DSWD - Special programs (UCT, Disaster Response	X	X	X
DTI	X		
GSIS	X	X	X
Health facilities	X		
Insurance providers - Accounts and Applications	X		
LCROs - Civil registration	X	X	
LTO	X	X	X
Mobile operators - Accounts and Applications	X	X	
NBI - Background check	X	X	X
NCDA	X		

User	Identity authentication for transaction (e.g. to trigger a payment)	e-KYC for enrollment	Uniqueness (seeding validated PSN token)
NCIP	X		
NCMF	X		
NHA	X	X	X
OWWA/POEA – Overseas Employment Certificate	X	X	X
Pag-IBIG	X	X	X
PhilHealth	X	X	X
PNP - Gun licenses	X	X	X
PRC	X	X	
PSA - Civil registration	X	X	X
SSS	X	X	X
Task Force Bangon Marawi	X	X	X
UMID	X	X	X
Universities	X	X	

PHILIPPINE STATISTICS AUTHORITY

Solid • Responsive • World-class