



Republic of the Philippines
SOCIAL SECURITY SYSTEM

East Avenue, Diliman Quezon City * Trunkline Number: (+632) 8709 7198
 Email: ussaptayo@sss.gov.ph * Website: www.sss.gov.ph



BIDS AND AWARDS COMMITTEE (BAC) III

PROJECT : APPLICATION DEVELOPMENT PLATFORM
ITB NO. : ITB-NGPA-SSS-GOODS-2026-024
SUBJECT : BID BULLETIN NO. 2
DATE : 08 APRIL 2026

Details of the bidding, as advertised:

Advertisement:	Posting at PhilGEPS & SSS Website & Conspicuous Places 12 March 2026 to 19 March 2026
Approved Budget for the Contract (ABC) and Source of Fund	₱231,000,000.00 Approved 2026 Corporate Operating Budget with Code PAP 2026-0219 of the Annual Procurement Plan (APP)
Price of BD (non-refundable)	₱35,000.00
Delivery/Completion Period	Within One Hundred Eighty (180) calendar days from receipt of Notice to Proceed and Signed Contract.

This addendum/Bid Bulletin **No. 2** is issued to clarify, modify or amend items in the Bidding Documents (BD) as a result of the Pre-bid Conference on **25 March 2026**. This shall form an integral part of the BD.

Under Section 51.5.3 of the IRR of RA 12009, it shall be the responsibility of all those who have properly secured the BD to inquire and secure Supplemental/Bid Bulletins that may be issued by the BAC.

1. Schedule of activities as discussed in the Pre-bidding Conference:

- Deadline for the submission of written queries: **Friday, 27 March 2026**
- Issuance of Bid Bulletin No. 1–reply to queries: **Wednesday, 08 April 2026**
- Pre-Screening of Documents: **Friday, 10 April 2026**
- Submission and opening of two (2) envelopes: **Wednesday, 15 April 2026, 2:00 p.m. at the 2nd Floor Bidding Room, SSS Main Building, East Avenue, Diliman, Quezon City**

2. Amendments/Clarifications – “Annex A”

3. Documentary Requirements

a. 1st Envelope

- a.1 PhilGEPS Certificate of Registration (Platinum Membership).**

In case of uploaded document/s, which validity period had already expired, submit the updated document/s.

- a.2 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;

For projects with Non-Disclosure Agreement, bidders are required to disclose the projects and its details using Form-05 of the Bidding Documents.

- a.3 Bidders should have completed, within the period of five (5) years from the date of submission and receipt of bids, any of the following:

a.3.1 A Single Largest Completed Contract (SLCC) that is similar to the procurement project to be bid, and whose value, adjusted to current prices using the Philippine Statistics Authority (PSA) consumer price indices, must be at least fifty percent (50%) of the ABC; or

a.3.2 A combination of contracts completed within the same period, provided their total value is at least fifty percent (50%) of the ABC, to wit:

- i. The bidder should have completed at least one (1) similar contract amounting to at least 25% of the ABC; and
- ii. The bidder should have completed other contracts, whether similar or not, with an aggregate amount of at least 25% of the ABC.

For this purpose, contracts similar to the Projects shall be: ICT Project with software/system development component.

SLCC should be a project without a Non-Disclosure Agreement.

- a.4 Net Financial Contracting Capacity (NFCC) computation or Committed Line of Credit (form supplied)

- a.5 Joint Venture Agreement (JVA), in case of Joint Venture – Class “B” Documents (Each partner of the joint venture shall submit the legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance)

- a.6 Bid Security

a.6.1 Cash or Cashier’s/Manager’s Check - 2% of the ABC or

a.6.2 Surety Bond - 5% of the ABC or

a.6.3 Bid Securing Declaration

- a.7 Technical Documents – project requirement

a.7.1 Section VI – Schedule of Requirements (pages 76-78)

a.7.2 Section VII – Statement of Compliance with the Technical Specifications (pages 80-88)

- a.8 Omnibus Sworn Statement.

- a.9 Foreign ownership limited to those allowed under the rules may participate in this Project, provided must submit any of the following:

a.9.1 Copy of Treaty, International or Executive Agreement; Or

a.9.2 Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.

a.9.3 Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.

b. 2nd envelope

- b.1 Bid Form (form supplied) – pages 91 to 92
- b.2 Bid Breakdown (form supplied) – page 93


c. Additional Requirements to be submitted by the bidder with the Lowest Calculated Bid

- c.1 Registration Certificate from Security Exchange Commission, for corporation including Articles of Incorporation and General Information Sheet, Department of Trade and Industry for sole proprietorship, or Cooperative Development Authority for cooperatives or its equivalent documents.
 - c.2 2026 Mayor's or Business permit issued by the city or municipality where the principal place of business of the prospective bidder is located, or the equivalent document for Exclusive Economic Zones or Areas.
 - c.3 Valid Tax Clearance per E.O. No. 398, s2005, as finally reviewed and approved by the Bureau of Internal Revenue (BIR).
 - c.4 Latest Audited Financial Statement filed through Electronic Filing and Payment System (EFPS)
 - c.5 Latest Income Tax Return filed through EFPS corresponding to the submitted Audited Financial Statement
 - c.6 Quarterly VAT (business tax returns) per Revenue Regulations 3-2005 for the last (6) months prior to the submission and opening of bids filed through EFPS.
4. Secretary's Certificate/Special Power of Attorney must clearly specify the name and position of the authorized representative who will:
- a. submit its bid; and
 - b. sign the contract (in case of award)
5. The award shall be issued to the bidder whose offer has been determined as the Lowest Calculated and Responsive Bid (LCRB).
6. All documents requiring notarization must be notarized by the Notary Public personally, who is duly commissioned and authorized to perform notarial acts for the current year.


Prepared by:


ROSALYN AZUL-CONDAT
Department Manager III
BAC Secretariat Department

Concurred by:


ISSACHAR PERALTA
Chairperson
Technical Working Group

Approved by:


VP EDWIN B. DINCOG, JR.
Vice Chairperson
Bids and Awards Committee III

"Annex A"

BB No.2026-027
dated 08 April 2026

PROJECT: Application Development Platform

QUERIES/CLARIFICATIONS RAISED DURING THE PRE-BID CONFERENCE:

No queries/response during the Pre-Bid Conference.

WRITTEN QUERIES:

	Query/Clarifications	TWG/BAC Reply
Secure Metric Technology		
1	<p>Page 82, 1.4.1.1. Data Locality - All platform data, logs, and configurations must be hosted and processed exclusively within Philippine or ASEAN regional data centers or the local Hybrid Cloud infrastructure.</p> <p>Page 63, Section 5 Item 8 Utilization of Existing SSS Infrastructure - The proposed Application Development solution shall be deployed and operated using the existing SSS Hyper-Converged Infrastructure (HCI) to leverage current compute, storage, and network resources, ensuring efficient utilization and simplified management.</p> <p>Question: For compliance with the Data Locality (1.4.1.1) and Utilization of Existing SSS Infrastructure requirements, may we confirm if it is acceptable that all core components are deployed within the SSS HCI environment, while non-core or auxiliary features may be integrated externally provided that no sensitive or regulated data is stored outside SSS-managed infrastructure and data locality requirements are maintained?</p>	<p>Yes, all core components should be deployed within the SSS HCI environment, while non-core or auxiliary features may be integrated externally provided that no sensitive or regulated data is stored outside SSS-managed infrastructure and data locality requirements are maintained</p>
2	<p>II. Page 82, 1.4.1.3. Data Encryption - All data must be protected using AES-256 encryption at rest and TLS 1.2 or higher in transit</p> <p>Question: For the Data Encryption (1.4.1.3) requirement, may we clarify if SSS accepts a layered implementation approach, where encryption in transit is enforced using TLS 1.2/1.3 and mutual TLS, enabled by an internal private CA platform with HSM-backed key management in a single hardware and encryption at rest should be implemented using AES-256 at the infrastructure, database, and storage levels within the SSS existing HCI environment,</p>	<p>Yes. The proposed solution must ensure full compliance with data encryption requirements through a layered security architecture. Encryption in transit is enforced using TLS 1.2/1.3 and mutual TLS, enabled by an internal private CA platform with HSM-backed key management in a single hardware. Encryption at rest should be implemented using AES-256 at the infrastructure, database, and storage levels within the SSS existing HCI environment.</p>

	ensuring that all application data, logs, and configurations across application development platform and API management tool are fully protected in accordance with RA 10173 and SSS security policies?	
3	<p>Page 83, 1.4.2.1. Certificate-Based Signing – Must support certificate-based code signing for binaries, executables, and containers to ensure authenticity and integrity.</p> <p>Page 63, Section 5 Item 7 Implementation of a Certificate-Based Code Signing Platform – Deploy a secure, certificate-based code signing platform to ensure the integrity and authenticity of software, applications, and code artifacts developed for SSS. The platform must enable issuance, management, and revocation of X.509 certificates for signing binaries, executables, and containers, while supporting trusted delivery pipelines aligned with industry best practices. The solution must be hardware-backed with a certified HSM, integrate with DevOps toolchains (e.g., CI/CD pipelines), and provide APIs for seamless embedding into development workflows, with full support for audit logging and timestamping to maintain complete lifecycle traceability.</p> <p>Question: For the Certificate-Based Signing (1.4.2.1) requirement, may we clarify if SSS expects the solution to include a centralized, certificate-based code signing platform supported by an internal private CA for certificate issuance, management, and revocation wherein, the internal Private CA should be an entry level hardware based with HSM and must be complemented by a dedicated signing component capable of securely signing binaries, executables, and containers, integrated with DevOps pipelines and secure key storage shall be implemented using a hardware-backed HSM that is FIPS 140-2 compliant as per Section 5 Item 7. Implementation of a Certificate-Based Code Signing Platform?</p>	<p>Yes, the solution is expected to include a centralized, certificate-based code signing platform supported by an internal Private CA for certificate issuance, management, and revocation. The internal Private CA should be an entry-level hardware based with HSM and must be complemented by a dedicated signing component capable of securely signing binaries, executables, and containers, integrated with DevOps pipelines. Secure key storage shall be implemented using a hardware-backed HSM that is FIPS 140-2 compliant as per Section 5 Item 7. Implementation of a Certificate-Based Code Signing Platform. The overall solution must support audit logging, timestamping, and full lifecycle traceability in accordance with industry best practices.</p>
4	<p>Page 83, 1.4.2.2. HSM Key Security – Keys used for code signing must be secured by an onboard FIPS 140-2 Level 3 Hardware Security Module (HSM)</p> <p>Question: For the HSM Key Security (1.4.2.2) requirement, may we clarify if the HSM is expected to be integrated within the overall certificate-based platform, including the internal private CA and code signing components, to ensure secure key</p>	<p>Yes, the HSM is expected to be integrated within the overall certificate-based platform, including the internal Private CA and code signing components, to ensure secure key generation, storage, and usage. The HSM must be hardware-based and embedded within</p>

	generation, storage, and usage wherein, the HSM must be hardwarebased and embedded within the internal Private CA and code signing platform components?	the internal Private CA and code signing platform components, and should be compliant with FIPS 140-2 Level 3, supporting secure and controlled code signing operations.
5	<p>V. Page 80, I. The development tools to be acquired (Application Development Platform)</p> <p>Question: May we clarify if all core components of the application development platform are expected to reside within SSS-managed infrastructure, particularly within the existing HCI environment, wherein all core components of the application development platform are expected to reside within SSS as per Section 5 Item 8. Utilization of Existing SSS Infrastructure, particularly within the existing HCI environment, to ensure security, control, and compliance with SSS policies?</p>	Yes
6	<p>VI. Page 84, II. API Management (APIM) Tool</p> <p>Question: May we clarify if all core components of the API Management Tool are expected to reside within SSSmanaged infrastructure, particularly within the existing HCI environment, wherein all core components of the API Management Tool are expected to reside within SSS as per Section 5 Item 8. Utilization of Existing SSS Infrastructure, particularly within the existing HCI environment, to ensure security, control, and compliance with SSS policies. ?</p>	Yes
7	<p>Page 87, 3.1.1.4 Certification under ISO/IEC 27701:2019 – Privacy Information Management System (PIMS)</p> <p>Question: For the certification requirement under ISO/IEC 27701:2019 (PIMS) (3.1.1.4), may we clarify if local regulatory compliance, such as registration with the National Privacy Commission (NPC) through a Certificate of Registration, may be considered an acceptable alternative?</p>	Yes, NPC Certificate of Registration is acceptable
8	<p>VIII. Page 87, 3.6 The Solution Provider must have SOC 2 Type 2: implemented procedures aligned with SOC 2 Type 2 requirements</p> <p>Question: For the SOC 2 Type 2-aligned implementation procedures (3.6), may we clarify if compliance may also be demonstrated through the proposed platform or technology components, provided these are integral to the overall solution?</p>	Yes, provided that the proposed platform or components are integral to the solution and meet SOC 2 Type 2 requirements.
9	Page 87, 3.7 The Solution Provider application security controls shall be aligned	

	<p>with OWASP Application Security Verification Standard (ASVS) Level 3</p> <p>Question: For the requirement on alignment with OWASP Application Security Verification Standard (ASVS) Level 3 (3.7), may we clarify if compliance may also be demonstrated through the proposed platform or solution components, provided these support the required security controls and practices?</p>	<p>Yes, provided that the proposed platform or components support and meet the required OWASP ASVS Level 3 controls.</p>
10	<p>Page 88, 3.8 The Solution Provider must support Financial-grade API (FAPI)-aligned security controls, including Mutual TLS (mTLS), pushed authorization requests, and Proof-of-Possession mechanisms.</p> <p>Question: For the requirement on support for Financial-grade API (FAPI)-aligned security controls (3.8), may we clarify if compliance may also be demonstrated through the proposed platform or solution components, provided these support the required security mechanisms?</p>	<p>Yes, provided that the proposed platform or components support and meet the required FAPI-aligned security controls.</p>
11	<p>Page 9, 3.a & b, Page 19, 5.5.a & b, Page 41, 5.4.i & ii, Single Largest Completed Contract</p> <p>Question: For the eligibility requirement on Single Largest Completed Contracts (SLCC), may we clarify if SSS requires bidders to demonstrate capability through a single completed project that covers any ICT related project with end-to-end scope, that independently meets at least 50% of the ABC to ensure consistency and accountability in delivery?</p>	<p>Yes. Bidders must comply with either:</p> <ul style="list-style-type: none"> (a) a Single Largest Completed Contract (SLCC) equivalent to at least 50% of the ABC; or (b) a combination of contracts, with at least one similar contract equivalent to 25% of the ABC and others totaling at least 25% of the ABC.