BIDS AND AWARDS COMMITTEE

Supplemental/Bid Bulletin No. 1

PROCUREMENT OF CODE REVIEW APPLICATION FOR THE DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES (DENR)

Bid Ref. No. DENR-CO-2024-042

Approved Budget for the Contract: ₱ 11,000,000.00

This **Supplemental/Bid Bulletin No. 1** is being issued to revise provisions/specifications in the Bidding Documents in response to clarifications/requests raised by prospective bidders during the Pre-Bid Conference conducted on 23 July 2024 for the aforecited project:

A. Revision to provisions/specifications in the Bidding Documents

FROM		TO	
SECTION III. BID DATA SHEET			
5.3	For this purpose, contracts similar to the Project shall be: a. "Software Tools/Application" and b. Completed within the last five (5) years prior to the deadline for the submission and receipt of bids.	**5.3**	For this purpose, contracts similar to the Project shall be: a. "**ICT Solutions"** and b. Completed within the last five (5) years prior to the deadline for the submission and receipt of bids.
20.2	Post-Qualification Documents (e.g., SEC Registration Certificate, PO, Contract, or any equivalent Document) to prove that the bidder has a proven track record with experience in providing Software tools/applications of at least five (5) years within the Philippines;	**20.2**	**Post-Qualification** **SEC Registration Certificate to prove that the bidder has a proven track record with experience in providing ICT Solutions of at least fifteen (15) years within the Philippines;**
SECTION VI. SCHEDULE OF REQUIREMENTS			
Section VI. Schedule of Requirements (Terms of Reference as of 11 June 2024)		**Revised Section VI. Schedule of Requirements (Terms of Reference as of 01 August 2024)**	

B. Reply to Queries/Clarifications	
Queries/Clarifications	**DENR Response**
1. To modify the experience requirement from 5 years to at least 15 years	**Request Granted.** After careful consideration, we concur with the first request regarding the qualifications of prospective bidders. This aligns with our standards for proven capability and reliability, ensuring that the ICT solutions provider has a minimum of fifteen (15) years of experience in the Philippine market, along with the submission of SEC registration.
2. To Modify the requirements for the provision of knowledge transfer and provision of technical support	**Request Denied.** We respectfully do not concur with the request concerning providing competency training to identified ten (10) DENR personnel in voucher form. The provision of training and the conduct of knowledge transfer are the same. The training voucher is a signed document that states the training or knowledge transfer activity that the supplier will provide to the end user The voucher shall also be used to complete the required documents for processing payments, ensuring that all deliverables are met satisfactorily within the stipulated period.
3. Clarification on the proper filling out of the form for Section VI. Schedule of Requirements.	Bidders are not required to indicate the word “comply” per line item in the Terms of Reference. However, bidders are required to sign the Bidder’s Undertaking on the last page of the Revised Section VI. Schedule of Requirements (Terms of Reference as of 01 August 2024) to signify compliance.

Bidders are advised to use the **Revised Section VI. Schedule of Requirements** and submit together with all the other required documents for the submission of bids on **08 August 2024 at 9:00 AM:**

Also, please use the **Revised Checklist of Technical and Financial Documents** as a guide/reference.

This Supplemental/Bid Bulletin No. 1 shall form part of the Bidding Documents. Any provisions in the Bidding Documents inconsistent herewith are amended, modified, and superseded accordingly.

For guidance and information of all concerned.

Issued this 1st August 2024 in Quezon City.

Approved by:

(sgd.)

EVELYN G. NILLOSAN
Chief, Management Division &
Alternate Vice Chairperson, Bids and Awards Committee

Received by:		
_____	_____	_____
SIGNATURE OVER PRINTED NAME	**DATE**	**NAME OF COMPANY**
(PLEASE RETURN OR FAX THIS PAGE ONLY TO THE DENR BAC OFFICE @ 8926-2675)		

PLEASE USE THIS BID FORM. DO NOT RETYPE OR ALTER.

Revised Section VI. Schedule of Requirements

Instruction to Bidders: ***Please fill up the form accordingly and sign the Bidder's Undertaking. Failure to conform will result in a rating of "FAILED".***

A. TERMS OF REFERENCE AS OF 01 August 2024

TERMS OF REFERENCE
(as of August 1, 2024)

Procurement of Code Review Application

I. RATIONALE:

DENR recognizes the increasing importance of maintaining high software quality and security standards within its various digital initiatives and public service applications. With the rapid advancement in technology and the growing reliance on software solutions, ensuring that all code deployed is robust, secure, and adheres to best practices is critical. The acquisition of a comprehensive code review tool/application will significantly enhance the ability of DENR developers to identify and rectify potential vulnerabilities, improve code quality, and ensure compliance with established coding standards. This initiative aligns with DENR's commitment to digital transformation, cybersecurity, and the efficient delivery of public services.

II. OBJECTIVE/S:

The primary objective of acquiring a code review tool/application is to establish a systematic and efficient process for evaluating the quality and security of code developed by DENR. This tool will facilitate automated code reviews, thereby reducing the manual effort required and increasing the accuracy of code assessments. It aims to support developers by providing actionable insights, ensuring that all code meets predefined standards and best practices. Additionally, the tool will aid in the early detection of potential security flaws, thus preventing vulnerabilities from being introduced into live environments. The overarching goal is to enhance the overall reliability, security, and maintainability of DENR software applications.

III. SCOPE OF WORK / DELIVERABLES:

1. Bidders' Scope of Work / Deliverables
   - Minimum Requirements / Specifications / Features

     Mode of Operation

     1) Deployment
        a) High Availability
        b) SaaS
     2) IDE Integration
        a) Microsoft Visual Studio
        b) Eclipse
        c) IntelliJ
        d) PHP Storm
        e) Android Studio
        f) Microsoft Visual Studio Code
        g) py Charm
     3) Build Server / Repository / CI / CD integration
        a) Jenkins
        b) Bamboo

c) Microsoft VSTS
d) GitLab
e) GitHub
f) Microsoft Team Foundation Server
g) BitBucket
h) Azure DevOps
i) AWS Code Pipeline

4) Defect tracking System Integration
   a) Jira
   b) Bugzilla
   c) Team City
   d) Service Now
   e) Microsoft (VSTS)
   f) Redmine

Scanning Technologies

1) Static Scanning
   a) Scan source code
   b) Scan binaries
   c) Security Unit Testing
   d) Identify permission required in mobile applications
   e) Scan hybrid applications
2) Software Components
   a) Identify known vulnerabilities in software components
   b) Identify known vulnerabilities in software components without rescanning
   c) Identify vulnerabilities not in the CVE list
   d) Identify if a vulnerable function is used in the code
   e) Identify the license used by an Open Source Component
3) Container Scanning
   a) Scan docker images
   b) Scan headless docker images
   c) Identify known vulnerabilities in the 3rd party components used.
   d) Generate SBOM in CyclonDX, SPDIX, and SPDIW format
   e) Scan docker directories
   f) Identify secrets stored on the docker images
   g) Provide CIS Benchmark information
4) IaC Scanning
   a) Scan Terraform files
   b) Scan Helm chart files
   c) Scan CloudFormation files
   d) Scan Kubernetes Manifests
5) Dynamic Scanning
   a) Scan standard web apps
   b) Scan single-page apps
   c) Batch scanning
   d) Authenticate to run a full application scan
   e) Scan API's dynamically
6) Web Application Perimeter Vulnerability Assessment

a) Identify Web Applications running on my perimeter
b) Continuously monitoring web applications running on my perimeter
c) Batch scan all identified web applications
d) Authenticate to run a full application scan

Enterprise Readiness

1) User Management
   a) Effectiveness of RBAC for User Segregation of Duties
   b) Effectiveness of user provisioning process
   c) Ability to support configuration options for user SSO via SAML 2.0
   d) Ability to restrict access based on the IP of the user
   e) Ability to administer Users through API rather than UI
   f) Ability to create users in bulk via API or through SAML Assertions
   g) Ability to support Two Factor Authentication - e.g., RSA SecurID
2) Policy Management
   a) Ability to change application security 'must-fix' scan policies retrospectively without the need to rescan
   b) Ability to define custom policies for each application
   c) Ability to define grace periods within policy - time for teams to fix before failing policy
   d) Ability to set custom Severities for flaw categories
   e) Ability to apply a policy at any level of the enterprise - for 1 team, business unit, or across the entire organization
   f) Ability to define flaw severities, categories, CWEs, and standards that comprise the policy
   g) Ability to assign a policy for different types of assessment such as SAST, DAST, and Manual Pen Testing
   h) Ability to administer Policies via API rather than UI
3) Scan Support
   a) Ability to obtain vendor assistance during application On-boarding, Uploading, and Results publication phases
4) Scan Operations
   a) Ability to support multiple scans concurrently
   b) Ability of service to cope with immediate demand for scan requests
   c) Ability to receive email notifications to prompt user action
   d) Ability to scan applications statically
   e) Ability to scan Applications dynamically (external and internal facing)
   f) Ability to scan applications manually
5) Operations
   a) Ability to start scanning without any local installation
   b) Ability to onboard new team members in a one-hour training (developers, security teams, application owners, and others)
   c) Automatic, monthly, or faster updates without enterprise intervention

d) Ability to scale to whatever amount of applications without new hardware required
e) Operate at almost no maintenance or operations costs

6) Application Security Program Operations
   a) Ability to participate in application security program management services
   b) Ability to run an application security program with the least effort and manpower

Remediation Coaching

1) On-Demand Expertise
   a) Ability to request tel/video conference with a vendor Application Security expert on flaws found in the application from within the platform
   b) Systematic approach to promoting dev teams to follow remediation path - i.e., not just left to the developers to make progress
   c) Likelihood that technology and service wrapper will affect the business outcome - reduced risk rather than risk identification
2) Product In-built Guidance
   a) Useful guidance around which flaws to fix first
   b) Effectiveness of flaw description & guidance
   c) Effectiveness of help center within SaaS platform - relevant information, documentation
   d) Clear identification of Policy-failing flaws - those that must be addressed for compliance
3) AI-assisted fix recommendations
   a) AI-assisted fix recommendations
   b) AI-assisted fix recommendations on developer IDEs
   c) AI-assisted fix recommendations as a command-line tool
   d) Batch fixing
   e) AI model not trained on open-source
   f) AI model not prone to Model Poisoning or Prompt Injections
   g) Fix recommendations, not recommending new flaws
   h) The solution supports the major languages

Results Quality

1) False Positives
   a) Average False Positives is below 10% - prior to scan configuration changes
   b) Ability to report only flaws in 3rd party components that are involved in the function of the application
   c) Out-of-the-box optimization for False Positives without requiring users to configure to reduce noise
2) True Positives
   a) The engine detects various CWEs and CVEs and displays them in a single platform.
3) Noise Levels
   a) Signal-to-noise ratio: actionable or correct findings vs total number of results

b) How well does the vendor limit unnecessarily large flaw counts in the 1st scan, e.g., the same issue or a different line of code?

Ease of Use

1) Browser Navigation
   a) Ease of Flaw Management
   b) Easy administration of Application Profiles and Policies
   c) Easy access to reporting and analytics
   d) Ease of submitting scan for assessment
   e) Ease of marking flaws as mitigated (not to be remediated)
2) IDE Navigation
   a) Ease of Flaw Management
   b) Ease of submitting scan for assessment
   c) Ease of marking flaws as mitigated (not to be remediated)

Reporting

1) Pan Enterprise Metrics
   a) Results consolidation across multiple assessment types and policies
   b) Flaw trending information between scans
   c) Drill-down reporting from the top of the organization to individual developer-level
   d) Ability to submit additional application metadata for centralized reporting and context
   e) Ability to create customized reports in the platform
   f) Ability to export data in a variety of convenient formats
   g) Ability to integrate data in a variety of SIEM and dashboarding tools
2) Programmatic Data Access
   a) Range of data and functions available via API: Detailed Flaw, Risk Mitigations, Frameworks Used, User Activity

Use Case Support

1) Identify Publicly Known Vulnerabilities
   a) Ability to identify Common Vulnerability Exposures (CVEs) - without additional scanning - e.g., Heartbleed scenario with vuln OpenSSL
   b) Ability to identify specific locations in 1st party code that call vulnerable 3rd party component functions.
   c) Ability to identify vulnerabilities using vendor-supplied vulnerability data is not available as CVEs are available in NVD.
   d) Wide range of supported programming languages and package managers
   e) Ability to perform 3rd party analysis as part of Static Analysis with no additional scan required
   f) Fix the compatibility rating shown for the recommended 3rd party library version
   g) Ability to perform 3rd party analysis separately from Static Analysis

h) Ability to identify vulnerable libraries in multiple applications - without additional scanning
i) Ability to identify the risk related to open source licenses - without additional scanning

2) Scan Without Source Code
   a) Ability to Scan 1st and 3rd party code
   b) Ability to understand the context of flaw without the source code (inc C/C++ Applications)
3) Client Side Support
   a) Ability to view source within a Browser or IDE without sending to Service Provider
4) Support Diverse Application Landscape
   a) Extensive major language support
5) Identify Coding Weaknesses
   a) Ability to identify Common Weakness Enumerations (CWEs) - Open Standard
6) API Automation
   a) Ability to submit builds, obtain results, call stacks, mitigation data, user activity, and applications profiles via API using direct web requests or via plugins/command line tools
   b) No additional costs to use plugins, APIs, or command-line tools
   c) Publically available sample integrations for reference
7) Application Profiles
   a) Ease of Application Profile creation in UI
   b) Ability to create an Application Profile via API
   c) Ability to visualize SAST, DAST, and Manual Pen Test Results side by side in UI

Developer Workflow

1) Flaw Management
   a) Ease of applying mitigation proposals to single or multiple flaws
   b) Effectiveness of flaw and mitigation matching between scans - persistent annotation of flaws
   c) Ability to segregate mitigation approval role from mitigation proposal role
2) Tool Chain Integration
   a) Richness of data available through API or other extracts
   b) Flexibility and extensibility of API suite and SDKs
   c) Range of Plugins, e.g., Build, IDE, Defect Tracking and GRC
   d) Automatic "fail build" configuration in build server integrations without dev intervention
   e) Pipeline support in build server integration without dev intervention
   f) Private developer scanning support in build server integrations without dev intervention
   g) Scan results overview on a per-build job basis in build server integrations
   h) Security scan results trend data overview on per build job basis in build server integrations

i) Repository integration
j) Ability to automate Defect Tracking (flaw) ticket creation and closure when scan results are published without dev intervention

3) Intra-sprint Testing
   a) Ability to scan in private using multiple Sandboxes in a dev cycle - without impacting compliance assessment
   b) Ability to scan in private different branches of an application - without impacting compliance assessment
   c) Ability to scan in private parts of an application - without impacting compliance assessment
4) Real-Time Testing
   a) Ability to manually scan in private, in developer IDE while coding a single file with an immediate response - without impacting compliance assessment
   b) Ability to automatically scan in private, in developer IDE, whenever a file is opened or saved with immediate response - without impacting compliance assessment
   c) Ability to integrate with repositories to support automated single file scanning whenever new files are committed with an immediate response - without impacting compliance assessment
   d) The solution must offer real-time scan functionality, enabling developers to identify vulnerabilities introduced during the coding process immediately.

Developer Training

1) Secure Coding Courses
   a) The ability for developers to attend self-running or instructor lead trainings
   b) Ability to see and launch eLearning courses related to specific flaws in SAST or DAST
   c) Ability to integrate with ILM systems
   d) Ability to track eLearning results

User Experience Feedback

1) Aggregated Developer Responses (avg)
   a) The results obtained from the Vendor solution were largely accurate, even if mitigating controls were already in place.
   b) Human advice and support are available from the vendor to help understand the flaws in the results.
   c) This tool helps the organization produce more secure software with the lowest tax on the developer's time.
2) Aggregated Security IT Responses (avg)
   a) Vendor provides this organization with a solution that offers an enterprise-wide view of application security.
   b) The Vendor helps teams focus both on risk identification and affecting change.
   c) On balance, this organization will be most successful with this Vendor.

2. QUALIFICATIONS AND RESPONSIBILITIES OF THE WINNING BIDDER
   a. Qualification Requirements
      i. The bidder should have a proven track record with experience in providing ICT Solutions of at least (15) fifteen years within the Philippines.
      ii. The bidder must have at least two (2) completed or ongoing contracts on provision of ICT Solutions projects from any recognized Government Agency in the Philippines or a Registered Private Company, the value of which is equivalent to at least thirty-five percent (35%) of the ABC (Approved Budget for the Contract). The Bidder must provide project details such as a description of the Project, its scope, etc.

   b. Duties and Responsibilities of The Winning Bidder
      i. Shall coordinate primarily with the KISS in terms of Project requirements, timelines, and deliverables
      ii. Shall be responsible for the timely delivery of outputs as indicated in this TOR.
      iii. The Contractor shall provide competency training to identified DENR personnel in voucher form, which DENR personnel could utilize.
      iv. Shall provide learning tools and materials accessible online and facilitated by a Certified Engineer or Trainer. The Certified Engineer or Trainer shall provide a training evaluation report post-training. The Certified Engineer or Trainer shall either come from the Vendor, Distributor, or Reseller.
      v. The training logistics shall be composed of but not limited to the following:
      vi. Electronic files on Training Manuals (user manual, administration manual, training handouts)
      vii. Certificates of Completion
      viii. Shall turn over complete documentation of the user guide and technical manual in electronic form.

   c. Duties and Responsibilities of DENR
      i. Ensure the availability of required information and other details in support of the implementation.
      ii. Facilitate/manage/organize the participation of the office's personnel in user testing and training.
      iii. Pay the winning bidder for its services based on the contract and follow existing government accounting and auditing rules and regulations. (DENR)

IV. TIMELINES:

The winning bidder shall complete the delivery within thirty (30) calendar days.

V. WARRANTY:

Any error or fault in any of the products or services delivered, accepted, and signed off shall be acted upon, resolved, and/or replaced accordingly by the winning bidder at no cost within the one (1) year duration of the subscription from the date of the acceptance, sign-off and the start of full implementation.

VI. APPROVED BUDGET FOR THE CONTRACT:

The approved budget for the contract is Eleven Million Pesos (P11,000,000.00).

VII. MODE OF PAYMENTS:

The payment for the services shall be made as stated in the table below:

TIMELINE	PROJECT DELIVERABLE/S	% Amount of contract rice to be released as payment	DOCUMENTARY REQUIREMENT/S
Within thirty (30) calendar days from receipt of Notice to Proceed (NTP)	Installation / Setup of Code Review Tool / Application User / Admin Accounts and set other requirements Training vouchers	100%	Certificate of Acceptance issued by the DENR Billing Statement

Approved by:

ARLENE A. ROMASANTA
Director, Knowledge and Information Systems Service

PLEASE USE THIS BID FORM. DO NOT RETYPE OR ALTER.

B. OTHER REQUIREMENTS

1. Bidder has no overdue deliveries or unperformed services intended for DENR.
2. Bidder did not participate as a consultant in the preparation of the design or technical specification of the GOODS/SERVICES subject of the bid.

BIDDER'S UNDERTAKING

I/We, the undersigned bidder, having examined the Bidding Documents including Bid Bulletins, as applicable, hereby BID to (supply/deliver/perform/comply) the above Terms of Reference

I/We undertake, if our bid is accepted, to deliver the goods/services in accordance with the terms and conditions contained in the bid documents, including the posting of the required performance security within ten (10) calendar days from receipt of the Notice of Award.

Until a formal contract/order confirmation is prepared and signed, this Bid is binding on us.

_____

Name of Company (in print)

_____

Signature of Authorized Representative

_____

Name of Authorized Representative (in print)

_____

Designation (in print)

DENR BIDS AND AWARDS COMMITTEE

REVISED CHECKLIST OF TECHNICAL AND FINANCIAL DOCUMENTS

Project: **PROCUREMENT OF CODE REVIEW APPLICATION FOR THE DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES (DENR)**

Bid Ref. No. **DENR-CO-2024-042**

APPROVED BUDGET FOR THE CONTRACT: ₱11,000,000.00

ENVELOPE 1: TECHNICAL COMPONENT

CLASS "A" DOCUMENTS

A. LEGAL DOCUMENTS

☐ (a) Valid and current **Certificate of PhilGEPS Registration (Platinum Membership)** (all pages) ***in accordance with Section 8.5.2 of the IRR*** (pursuant to GPPB Resolution No. 15-2021, dated 14 October 2021);

B. TECHNICAL DOCUMENTS

☐ (b) 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 (per **Annex I**);

☐ (c) Statement of the Bidder's Single Largest Completed Contract (SLCC) of similar nature within the last five (5) years from date of submission and receipt of bids equivalent to at least fifty (50%) of the total ABC (per **Annex I-A**)

*Similar in nature shall mean "**ICT Solutions**"*.

Any of the following documents must be submitted/attached corresponding to listed completed largest contracts per Annex I-A:

i) Copy of End User's Acceptance; or
ii) Copy of Official Receipt/s or Sales Invoice or Collection Receipt/s

☐ (d) Original Bid Security must be issued in favor of the **DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES (DENR)** (must be valid for at least 120 calendar days from the date of bid opening); any one of the following forms:

Project ABC (₱)	Bid Security: Cash, Cashier's/ Manager's Check, Bank Draft / Guarantee, Irrevocable Letter of Credit (2%) (₱)	Bid Security: Surety Bond (5%) (₱)	Original Bid Securing Declaration
11,000,000.00	220,000.00	550,000.00	No required Amount

1. Bid Securing Declaration per **Annex II**;
2. The Cashier's/Manager's Check shall be issued by a Local, Universal or Commercial Bank
3. The Bank Draft/Guarantee or Irrevocable Letter of Credit shall be issued by a Local Universal or Commercial Bank; or
4. Should bidder opt to submit a Surety Bond as Bid Security, the surety bond must be callable on demand and must be issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such bond. Together with the surety bond, a certification from Insurance Commission must be submitted by the bidder which must state that the surety or insurance company is specifically authorized to issue surety bonds.
5. For submission of Bank Draft/Guarantee or Irrevocable Letter of Credit or Surety Bond, the following must be stated/specified in the Bid Security pursuant to Section III, ITB Clause 18.5, to wit:

☐	*The following are the grounds for forfeiture of Bid Security* ▪ **IF A BIDDER:** a) Withdraws its bid during the period of bid validity. b) Does not accept the correction of errors pursuant to Section 32.2.1 of the IRR of RA 9184. c) Fails to submit the Post Qualification requirements within the prescribed period or a finding against their veracity thereof. d) Submission of eligibility requirements containing false information or falsified documents. e) 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. f) Allowing the use of one's name, or using the name of another for purposes of public bidding. g) 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 Lowest Calculated and Responsive Bid. h) Refusal or failure to post the required performance security within the prescribed time. i) 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. j) Any documented unsolicited attempt by a bidder to unduly influence the outcome of the bidding in his favor. k) Failure of the potential joint venture partners to enter into the joint venture after the bid is declared as successful. l) 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. ▪ **IF THE SUCCESSFUL BIDDER:** a) fails to sign the contract in accordance with Section 40 of the Revised IRR of RA 9184; or b) fails to furnish performance security in accordance with Section 40 of the Revised IRR of RA 9184.
☐	(e) Conformity with **Revised Section VI. Schedule of Requirements (Terms of Reference as of 01 August 2024)as enumerated and specified in the Supplemental/Bid Bulletin No. 1** (**all pages**) and Section VII. Technical Specifications (all pages) of the Bidding Documents.
☐	(f) Original duly signed **Omnibus Sworn Statement** in accordance with Section 25.3 of the IRR of RA 9184 and using the prescribed form attached as **Annex III** with attached **Proof of Authority of the bidder's authorized representative/s**: i. **FOR SOLE PROPRIETORSHIP (IF OWNER OPTS TO APPOINT A REPRESENTATIVE):** Notarized Special Power of Attorney. ii. **FOR CORPORATIONS, COOPERATIVE OR THE MEMBERS OF THE JOINT VENTURE:** Notarized Secretary's Certificate evidencing the authority of the designated representative/s. ***Note:*** ***Should there be more than one (1) appointed authorized representatives, use the word "any of the following" or "OR", otherwise, all authorized representatives must sign/initial the bid submission*** **IN THE CASE OF UNINCORPORATED JOINT VENTURE:** Each member shall submit a separate Special Power of Attorney and/or Secretary's Certificate evidencing the authority of the designated representative/s.

C. FINANCIAL DOCUMENTS	
☐	(g) Net Financial Contracting Capacity (NFCC) computation**,** in accordance with ITB Clause 5.5, (per **Annex IV).** The NFCC computation must at least be equal to the ABC of this project. The detailed computation using the required formula must be provided. **OR** Original copy of Committed Line of Credit (CLC) per **Annex IV-A** issued by a Local Universal or Local Commercial Bank at least equal to ten percent (10%) of the ABC of this project. **In case of Joint Venture, the partner responsible to submit the NFCC shall likewise submit the Statement of all its ongoing contracts and the Latest Audited Financial Statements.**
Class "B" Document: (For Joint Venture)	
☐	**If applicable, For Joint Ventures, Bidder to submit either:** (i) Copy of the JOINT VENTURE AGREEMENT (JVA) in case the joint venture is already in existence, or (ii) Copy of Protocol/Undertaking of Agreement to Enter into Joint Venture (**Annex V**) signed by all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful and must be in accordance with Section 23.1 (b) of the IRR In case the joint venture is not yet in existence, the submission of a valid JVA shall be within ten (10) calendar days from receipt by the bidder of the notice from the BAC that the bidder is the Lowest Calculated and Responsive Bid [Sec 37.1.4 (a) (i)] (h) **The JVA or the Protocol/Undertaking of Agreement to Enter into Joint Venture (**per **Annex V) must include/specify the company/partner and the name of the office designated as authorized representative of the Joint Venture.**
ENVELOPE 2: FINANCIAL COMPONENT	
☐	(a) Completed and signed Financial Bid Form. Bidder must use, accomplish and submit Bid Form **(Annex VI); and** (b) Original of duly signed and accomplished Price Schedule(s) (**Annex VI-A or VI-B**). The ABC is inclusive of VAT. Any proposal with a financial component exceeding the ABC shall not be accepted.