DEVELOPMENT BANK OF THE PHILIPPINES
Head Office: Sen. Gil J. Puyat Avenue corner
Makati Avenue, Makati City, Philippines

SUPPLEMENTAL BID BULLETIN NO. 1

25 September 2024

Attention: **All prospective bidders for the project**

BID REFERENCE NO. G-2024-31: ONE LOT DELIVERY, INSTALLATION, CONFIGURATION, TESTING AND COMMISSIONING INCLUDING MAINTENANCE AND AFTER SALES SUPPORT FOR ONE (1) YEAR OF THE API GATEWAY/SECURITY SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
(ABC: PhP 13,268,000.00 inclusive of all applicable taxes)

Please be informed of the following:

1. **The schedule of submission and opening of bids shall proceed as follows:**

ACTIVITY	DATE AND TIME	VENUE
Submission of Eligibility, Technical, and Financial Proposals*	**2 October 2024 (Wednesday) ON OR BEFORE 10:00 AM**	6/F BAC Secretariat, DBP Head Office, Makati City
Opening of Eligibility, Technical, and Financial Proposals	**2 October 2024 (Wednesday) 11:15 AM**	6/F BAC Conference Room, DBP Head Office, Makati City

Late submissions shall not be accepted.

2. **Please refer to Section III. Bid Data Sheet (BDS) of the Philippine Bidding Documents for the detailed procedure and options for the payment of bidding documents and the submission of bids. As indicated in the Invitation to Bid, bidders must settle the required payment for the bidding documents before the deadline of the submission and receipt of bids.**

   Additionally, bidders are encouraged to submit their bid proposals at least one day prior to the deadline to avoid late submissions. Bidders may attend the bid opening through Zoom Meeting App.

3. **Please refer to the Annex A as attached in this Supplemental Bid Bulletin No. 1 for the responses to the queries or requests for clarifications.**

4. **Bidders are reminded to use as guide/reference in preparing their Bidding Documents the Checklist of Requirements.**

5. **The Eligibility, Technical Documents and Financial Proposals must be properly tabbed for easy reference and must be submitted in sequence/order per Checklist of Requirements.**

6. **The BAC shall no longer entertain any question/request for clarification after the issuance of this Bid Bulletin.**

7. **Please be advised that bids submitted after the deadline shall only be marked for recording purposes, shall not be included in the opening of bids, and shall be returned to the bidder unopened.**

For the guidance and information of all concerned.

(SIGNED)
RONALDO U. TEPORA
Senior Vice President, and
Chairperson, Bids and Awards Committee

ANNEX A

Responses to the Queries or Request for Clarifications

Bidder No. 1

TITLE	DESCRIPTION	EXIST CLARIFICATION QUESTIONS	RESPONSE
III. Scope of Services and Deliverables	a) Delivery, Installation, Configuration, Testing and Commissioning including maintenance and after sales support for 1 year	Delivery, Installation, Configuration, Testing and Commissioning - Should be completed within 30 calendar days.	
		1 year support and maintenance will commence after.	The one-year support and maintenance period will begin upon the Go-live date, which will be determined by the successful launch of the first application.
		Is there any possibility for an extension of the 30-calendar-day completion period for the delivery, installation, configuration, if needed?	No, because we need to adhere to the 30-day timeline to meet the project's deadline.
	1.The service provider shall provide the API Gateway/Security Solution, adhering to the following technical specifications, with a guarantee that it **can handle the projected 20 million calls per month, and no extra fees will be charged if the monthly assessed API calls exceed 20 million.**	**1.Can you provide more details about your expected peak traffic loads and any anticipated growth?**	Peak traffic happens during the 12th-15th and 27th-31st of the Month with approximately 500k calls per peak time.
		1.1 Where are the systems deployed currently? Are they already on-cloud?	The systems are currently hosted on-premises and at test environment. not yet on-cloud.
	a. Equipped with Web Application and API Protection (WAAP) services, and Distributed Denial of Service (DDoS) defenses to counteract automated bot attacks.	**Letter A. Any specific threats you've faced? answered with bot attacks**	not yet since the WebApps is not yet launched hence we anticipate facing attacks from common bot attack vectors, including DDoS, brute force, scraping, and various others.
	b. It had the ability for data encryption, application of Transport Layer Security, and execution of data masking	**Letter B. Any specific rules to follow aside from Memorandum No. M2022-016?**	None

	c. Enables the setting of a threshold or rare-limit to regulate the number of times an API can e accessed by a user within a specific timeframe	**Letter C. Could you specify the rate-limiting rules you need? For example, how many API requests should be allowed per user or IP address within a given timeframe?**	Rate Limiting Headers, approximately 25 API calls per user/IP address for every transaction/timeframe
	d. Capable of granular access controls and authentication mechanisms.	**Letter D. Are there any particular access control levels /restrictions that you prefer?**	we currently employ JWT, API keys, IP whitelisting, and Rate Limiting, hence we require flexible capability
	e. Can integrate Multi-Factor Authentication (MFA) for a layered defense and identity access management.	**Letter E: Do you require any specific MFA (eg. OTP, Biometrics etc.)**	we currently employ SMS-based MFA, hence we prefer a service capable of supporting multiple MFA methods.
	3. The Solution shall provide a real-time dashboard for administration for monitoring API traffic, activity, and security events.	**Aside from monitoring the API Traffic, activity and security events, do you have other data that you would like to see in the dashboard?**	yes, such as events, traffic peaks, statistics reports, and typical solution/system are providing.
	6. Can provide comprehensive reporting capabilities to track security incidents and compliance status, including but not limited to:	**1.How frequently would you like reports to be generated (e.g., daily, weekly, or monthly)?**	Monthly report generation is standard, however the system should be capable of generating reports for custom date ranges as needed.
		2.Considering the sensitivity of data in Letter D of Item No. 1, will access to report generation be restricted to specific personnel?	Yes, report generation access should be limited to authorized personnel, such as analysts or supervisors.
		3.Do you require any additional customizable reports beyond those already mentioned?	Yes, as mentioned "not limited to"
	- Volume of API traffic calls processed.		
	- Number of protected APIs Calls		
	- Threats assessed and blocked.		
	- Detailed Security incident reports.		
	- Audit trail and Compliance Status reports.		

	Reports can be exported and made readable in widely used formats such as excel, PDF, among others.		
	7. It comes with continuous updates of enhanced threat detection and monitoring stay abreadt of merging threats.	**1.Would you prefer an announcement on the upcoming updates?**	Yes
		2. Is it possible to provide a point of contact that has the authority to decide on the go or no go of the critical activities? For example zero-day threat. **A zero-day is a vulnerability in software or hardware that is typically unknown to the vendor and for which no patch or other fix is available. The vendor has zero days to prepare a patch as the vulnerability has already been described or exploited**	Yes, but we will provide the point of contact during the operation/ implementation phase.
	1. For monitoring purposes, the service must include alert capabilities notofying DBP for when API calls exceed 90% or 18 million calls.	**Who should be notified in DBP if this occurs?**	We will provide the DBP Representative/name during the operation/ implementation phase.
	2. In the case where DBP Head Office application interface is down, the solution must be able to automatically switch to DR Site for business continuity purposes.	**What is your SLA preference on this?** **Can we assume that cloud management is also part of the 1 year support and maintenance?**	Same - Stated SLA should apply in production as well as in DR. Yes, management for control adjustments or reconfigurations in cloud are included in the 1 year support and maintenance.
	3. In case DBP conducts BCP activity, the Service provider's support Engineer shall be on standby and ready to assist on any necessary configuration to ensure that the APi Gateway Securiy Solution is operational.	**Will the assistance be provided onsite or remotely? Will there be prior notice (date and activity details) to ensure that the appropriate Engineer deployed based on the specific activity**	can be made onsite/online as needed, depending on the situation. Yes, BCP activity details shall be provided
		Do you require 24/7 support?	no, but available when needed

	4. In case a security breach involving the service provider or its API service product, it is mandatory for the service provider to notify DBP within a span of 30 minutes.	**Who should be notified in DBP if this occurs?**	Specific names will be provided during the implementation phase.
V. Implementation Activity	**3. Security Functionality Testing:**	**Are there any specific tools or methodologies required for the Security Functionality Testing, and who will be responsible for this?**	Tools for Security Functionality Testing shall be provided by the Service-provider to simulate protection measures.
	Security functional Testing should be done right after configuration Activity and should be executed within 5 calendar days.		
	- Access control and security testing (applicable testing includes, but is not limited to, port scanning, DDoS testing, and penetration testing.)		
	- Error handling and offline Testing (server and telco offline testing)		
	The User Acceptance Testing Certificate will be issued by DBP following the activity.		
	4. Commissioning (go-live):		
	Cloud Gateway/Security and Tier-2 blocker should be set operational right after the Security Functionality testing or training and should be executed within 10 calendar days. The Service Provider must provide a 'WebApp Operational Status Verification Document', which should be signed by both parties.	**1.What are the exact criteria for the 'WebApp Operational Status Verification Document'?**	Criteria, - Porting Documents, UAT Certificate and the Site is evidently online/live.
	At the conclusion of each activity, DBP will provide a completion certificate, which will serve as the basis for milestone payments.	**2.How will the completion certificates be issued, and what documentation is needed to receive them?**	DBP Shall provide the completion Certificate right after completion of every activity, documents needed are also stated in the payment terms
VI. Training/ Kowledge Transfer	Training certificates should be issued to all DBP training attendees within 2 calendar days after the training.	**How many attendees are we expecting to participate in this training?**	around 10 participants

	Distribution of training materials, operating manuals, admin-user guides, FAQs, software release notes and other relevant training technical documents, 2 days before the training schedule.		
VII. Payment Terms	The Cloud-Based API Gateway/Security Solution will be priced based on the ABC, irrespective of the number of WebApps enrolled, and stationed in Head Office (HO) and Disaster Recovery (DR) sites.	**Can you confirm the scope of the solution—does the ABC cover all future WebApps, or will there be a threshold limit for WebApp enrollments?**	Yes, ABC covers all future WebApps with in 1 year period, Three WebApps are anticipated this year, with the potential addition of one or two web applications if resources permit.
	Payment will be divided according to the milestones stated in the table below.		

Bidder No. 2

Clarifications	Response
1. For the required functionalities of the solution SEC III-Item 1-letter B, we want to clarify what data needs to be encrypted and mask?	The service should be compatible with encryption method implemented within the web API service, but will not perform any encryption itself.
2. For the required functionalities of the solution SEC III-item 1 letter E, What MFA solution needs to be integrated? Will the MFA provider and identity provider be provided by DBP? What is the existing identity provider and MFA provider that the solution will integrated?	We currently employ SMS-based MFA, we prefer a service capable of supporting multiple MFA methods.
3. For the required functionalities of the solution item 2, we want to clarify if this is only for API calls that will traverse on the WAF/API gateway? Or any WEB transaction is expected to be protected by the proposed solution?	If the East-West Traffic protection solution/device is proprietary to the service provider, only the APIs need to be monitored/protected. However, if an independent Web Application Firewall (WAF) is provided, we expect it to offer comprehensive web transaction protection, similar to a typical WAF.
4. What is the required DATA type for logs of DBP's SOC?	Strings, integers, timestamps, etc.
5. How many applications will be protected by the API gateway?	Three website launches are anticipated this year, with the potential addition of one or two web applications if resources permit.
6. Do we assume that the DR infrastructure of DBP will also house the API web server and backend servers similar to HO?	Yes

7. May we request for an additional 15 days extension from the original 30 days project completion to 45 days project completion in anticipation of a possible appliance delivery and customs clearance delay?	No, because we need to adhere to the 30-day timeline to meet the project's deadline.

Bidder No. 3

PARTICULARS	CLARIFICATION/SUGGESTION	RESPONSE
III. SCOPE OF SERVICES AND DELIVERABLES b. Required functionalities of the Solutions: The Services Provider shall provide the API Gateway/Security Solution, adhering to the following technical specifications, with a guarantee that it can handle the projected 20 million API calls per month, and no extra fees will we charged if the monthly assessed API calls exceed 20 million.	We would like to seek further clarification regarding the information provided for the WAAP (Web Application and API Protection) to ensure accurate alignment with your expectations. Below are the following questions need your input: 1. How many APIs hosts (or FQDNs) does DBP want to onboard to the WAAP? 2. Is the 20M API calls per month the estimated total volume of API calls to the environment? a. Based on the prebid call, the total calls also include the internal calls (which assumed a 1:1 ratio for external incoming calls generating an equivalent 1:1 internal API call) 3. Will there be other applications that is need to onboard to the WAAP? meaning additional FQDN hosting websites?	1. Three website launches are planned for this year, with the potential addition of one or two web applications if feasible. 2. Yes, We anticipate an average monthly API volume of under 20 million calls across the three web applications. a. The actual API call volume may vary depending on your technology. A 1:1 call ratio is expected if you utilize a proprietary/dedicated on-premise blocker compatible with your cloud technology. Alternatively, if an independent Web Application Firewall (WAF) is provided, only cloud API traffic will be counted. 3. The initial launch will include three web applications, with the possibility of further expansion within the year and beyond.
2. The Solution must incorporate security protection through implementing Web Application Firewall (WAF) or equivalent blocker in the Tier 2-Data Center for internal (East West Traffic) API anomalies.	1. Is the internal WAF specifically virtual appliances or hardware models to be proposed?	This is contingent on your preferences, provided the solution can execute real-time blocking.

Bidder No. 4

PARTICULAR	QUERY	RESPONSE
"A contract similar to the project refers to API Gateway/Security Solution includes the delivery installation, and/or maintenance and support.."	Could you please confirm if this refers to "|API Gateway| or |Security Solution|" or if it means "|API Gateway| or |API Security Solution|"?	This pertains to as |API Gateway| or |API Security Solution|

Bidder No. 5

TECHNICAL SPECIFICATIONS	INQUIRY	RESPONSE
Item 1	May we validate that the required solution includes Bot Defense protection that supports Multi Cloud Deployments?	It doesn't matter how your cloud service infrastructure is architected, as long as the enrolled DBP web applications in the Cloud environment are protected from common Bot attack vectors such as DDoS attacks, particularly safeguarding against API call alterations.
DBP WebApps traffic will be channeled through a Cloud Service.		
a. Equipped with Web Application and API Protection (WAAP) services, and Distributed Denial of Service (DDoS) defenses to counteract automated bot attacks.		
b. It has the ability for data encryption, application of Transport Layer Security, and execution of data masking.		
c. Enables the setting of a threshold or rate-limit to regulate the number of times an API can be accessed by a user within a specific timeframe.		
d. Capable of granular access controls and authentication mechanisms.		
e. Can integrate Multi-Factor Authentication (MFA) for a layered defense and identity access management.		
DBP Security Administrators are given access to the Service Provider or Principal's demo environment to execute and output the following:		
• Enrolling Website - provide screen shot(s).		

• Controlling/configuring security parameters both in Cloud and		
Blocker - provide screen shot(s).		
• View / extract/ print events/attacks System Generated Reports.		
Item 2	May we validate that the requirement shall include implementing on on-prem Web Application Firewall including public cloud deployments k8s, etc?	Yes, in addition to cloud-based security, an on-premises WAF or compatible proprietary solution is required to safeguard east-west traffic, ensuring API integrity (unaltered) between the DMZ API Server (Tier 1) and the Data Center API Server (Tier 2).
The solution must incorporate security protection through implementing Web Application Firewall (WAF) or equivalent blocker in Tier 2 Data Center for Internal East-West API Traffic Anomalies		
Item 3	May we validate if the solution should be capable of monitoring service health from an end-user perspective?	Yes, to ensure optimal performance and security of our web applications, monitoring their health status within your cloud domain is crucial.
The solution shall provide a real time dashboard for administration and monitoring API traffic, activity and security events	May we confirm based on the requirement that the solution shall include functions / features for web application scanning and testing?	Application scanning and testing are integral components in the security functionality testing phase.
• Control/configure security parameters.		
• View/ extract/ print API traffic related System Generated Reports.		
Item 4	Based we validate that the requirement pertains to Scanning capability that includes scheduled scan including run authenticated and unauthenticated Automated Penetration Testing	Penetration testing should be conducted during the initial/testing phase (Security Functionality Testing) to assess the solution's capabilities.
The Solution can discover and identify API for inventory of every APIs deployed across the network.		
• View/ extract/ print Listing of API servers/services through System		
Generated		
Item 5		
Must be capable of integrating logs (security and or audit trail) with the Bank's Security Operation Center for event security monitoring or orchestration.		
• System Generated Reports/Screen shots on interconnection facility of Cloud and Tier-2 Blocker with SIEM		

Item 6	May we validate that compliance requirement pertains to the capability of the solution for Vulnerability and Application Scanning ?	The system must be capable of generating incident reports that support compliance requirements. (Note: Vulnerability and application scanning are explicitly excluded from this context.)
Can provide comprehensive reporting capabilities to track security incidents and compliance status.		
• View / extract/ print System Generated Reports.		
Item 7		
It comes with continuous updates of enhanced threat detection and monitoring to stay abreast of emerging threats		
• Enhancements/update list, notifications in printable information or screen		
	Can we confirm the requirement for the technical expert and the bidder's authorized representative? Specifically, for the technical expert, will a technical certification of the proposed solution be required to verify its qualifications? To ensure clarity of requirement, can we request this certification be part of the proof as part of the submission and evaluation requirements?	Bidders must submit a Certification - confirming that the personnel's technical Certifications demonstrate expertise in API security.
BIDDING REQUIREMENTS		
Documents required for the Bid Opening:		
A certificate or training		
credentials naming the technical expert in API		
Gateway/Security, who will be assigned to the project if the contract is awarded, duly signed by the bidder's authorized representative. The product-specific API Gateway/Security certification or training certificate must demonstrate proficiency in API security installation, configuration, testing, and commissioning, and must be obtained at least one month before the bid		
A CV signed by both the technical expert and the bidder's authorized representative, which must include a list of experiences supporting at least one API gateway/security project.		

Bidder No. 6

	QUERY	RESPONSE
1	Total bandwidth for the three apps/hosts mentioned during the pre-bid	Bandwidth requirements are unavailable due to the websites/web applications are not yet launch in public, however, for projection purposes, a transactional text-based website typically utilizes approximately 5 GB per month.
2	Are they using custom ports for the apps?	Yes