

**BIDS AND AWARDS COMMITTEE**

July 18, 2022

**SUPPLEMENTAL / BID BULLETIN NO. 001**

***Procurement of Supply, Delivery and Installation of Cloud-Based Web Application Firewall (WAF) License with Anti-Distribute Denial of Service (DDoS)***

***(ITB-ITD-004-11-07-2022)***

This Bid Bulletin No. 1 dated July 18, 2022, issued to clarify, modify or amend items in the Bidding Documents. Accordingly, this shall form an integral part of the said Documents.

The modifications, amendments or clarifications are as follows:

1. Queries / Questions by the prospective bidders during Pre-Bid Conference held on 15 July 2022 (Friday):

Particulars / Requirements	Prospective Bidder's Queries / Clarifications	BAC / BAC Sec / TWG Replies
1. Bid Submission	For consideration to move the submission from July 21, 2022(Thursday) to <b><u>July 29, 2022 (Friday)</u></b>	In consultation with Project Owner/s, the BAC agreed to extend bid submission until <b><u>July 25, 2022 (Monday) at 3:00pm only.</u></b>  Due to extension of bid submission, the bid opening will be moved from July 22,2022 (Friday) to <b><u>July 28, 2022 (Thursday) at 2:30pm.</u></b>
2. Section VI. Schedule of Requirements	For consideration to increase the delivery and installation period from five (5) calendar days to fifteen (15) calendar days upon receipt of Notice to Proceed	Yes
3. Supplier's Qualification, item no.7	Can we submit the "Performance Evaluation for 2021 (period: Jan - Dec 2021)	Yes
4. Section 3 - Scope of Works and Deliverables	1.1.a.3 Protocol Anomaly Attacks Protection  Please clarify on this requirement. Is this IPS monitoring?	Yes
	1.1.a.4 L3/4 Protection  Is this to protect HTTP/s applications or L3/4 applications?	Yes
	1.1.a.7 Behavior Detection  What kind of behavior detection is required?	Can be signature based or based on parameters
	1.1.a.11 Internet Services Protection	None at the moment



**BIDS AND AWARDS COMMITTEE**

July 18, 2022

**SUPPLEMENTAL / BID BULLETIN NO. 001**

***Procurement of Supply, Delivery and Installation of Cloud-Based Web Application Firewall (WAF) License with Anti-Distribute Denial of Service (DDoS)***

***(ITB-ITD-004-11-07-2022)***

	Do you have non-http applications in SFTP/SNMP/SMTP/POP-3/IMAP/CHARGEN/MIME? Are they individual applications available on hostnames?	
	1.1.a.11 Internet Services Protection  With reference to SMTP, IMAP, POP-3, what applications are you protecting? If it is your mail server, will it have an out-of-band connection? i.e. will you be proxying MX domains in Cloudflare?	Disregard for mail related protocols
	1.1.a.11 Internet Services Protection  With reference to DNS protection, what is the DNS setup you would like to achieve?  Will Cloudflare be your authoritative DNS? If not, will you want to use a hidden-primary or primary-secondary DNS setup? Or do you want Cloudflare to protect your authoritative DNS via a Firewall.  Cloudflare has the following DNS protections: (1) Authoritative DNS – this comes with DNSSEC and uses the full Cloudflare network capacity to protect from DDoS attacks (2) Secondary DNS – Cloudflare acts as the secondary DNS to maintain a copy of your primary DNS records to respond to queries on your behalf. This can support a hidden-primary or primary-secondary setup. Hidden primary will hide where your primary DNS actually is and Primary-secondary provides greater redundancy in case one of your DNS providers go down. (3) DNS firewall – helps protect your nameservers from DDoS	As your expert recommendation

WSP

**BIDS AND AWARDS COMMITTEE**

July 18, 2022

**SUPPLEMENTAL / BID BULLETIN NO. 001**

***Procurement of Supply, Delivery and Installation of Cloud-Based Web Application Firewall (WAF) License with Anti-Distribute Denial of Service (DDoS)***

***(ITB-ITD-004-11-07-2022)***

	attacks and speed up DNS answers by acting as a proxy between the client (DNS resolver) and the customer's nameservers. It sits in front of the authoritative nameservers and pretends to be the authoritative server by caching the DNS responses and blocking the nameservers from attack.	
	1.1.2.e At least 50 Mbps clean bandwidth  What is the total data transfer expected?	With provision to increase
	1.1.2.f At least 15 web application/domains to protect  Please clarify how many root domains you have. Is it 5 root domains and total 15 FQDNs?  Are settings across apps that share the same root domain very different?	yes
	1.1.2.i Rate Limiting  What are your requirements? How do you identify traffic coming from the same source and do you want to rate limit by hostname or do you need to look into additional parameters like payload and heaters?	For discussion
	1.1.2.l BGP  Please clarify on this requirement? Are you referring to BGP announcements on your behalf? Cloudflare has a L3 DDoS solution (Magic Transit) that can announce IP prefixes of at least /24 for our customers. Do you have /24 prefix to announce?  Cloudflare can announce your IP prefixes via BGP on your behalf if	As per your product expert recommendation

**BIDS AND AWARDS COMMITTEE**

July 18, 2022

**SUPPLEMENTAL / BID BULLETIN NO. 001**

***Procurement of Supply, Delivery and Installation of Cloud-Based Web Application Firewall (WAF) License with Anti-Distribute Denial of Service (DDoS)***

***(ITB-ITD-004-11-07-2022)***

	have a /24 prefix. Alternatively, we can also lease Ips for smaller prefixes.	
	1.1.2.p Deep Packet Inspection  Please provide more clarity on the expectations of the packet analytics required.	Same as packet sniffing
	1.1.3.c On-Demand  Please clarify on-demand requirement. Is this referring to on-demand BGP announcement for your IP prefixes?	For discussion / As per your expert product recommendation
	1.1.3.d Customized Mitigation Strategy  Please clarify on the expectations of the mitigation.	For discussion / As per your expert product recommendation
	1.1.4.b On-site Management  Cloudflare is a complete cloud-based solution. Any on-site work may only relate to initial router configurations to set up the GRE tunnel to Cloudflare if Magic Transit is required.  Please clarify on what other on-site management you may require.	Disregard / Not at the moment
	1.1.4.d Reports  Please clarify on what reports are required and the depth of analysis.	Historical and on demand reports
	4.1.3 Real-time Reports and Alerts  Please clarify on what reports and alerts are required and the depth of analysis.	Historical and on demand reports
	4.1.4 Forensic Capabilities  Please clarify on what forensic capabilities are expected.	Historical and on demand reports
	4.1.5 Produces reports that can be converted into different file formats (e.g. html, pdf, csv) on specified schedule. Reports generated can	Manual and custom reports, can be scheduled or on demand



**BIDS AND AWARDS COMMITTEE**

July 18, 2022

**SUPPLEMENTAL / BID BULLETIN NO. 001**

***Procurement of Supply, Delivery and Installation of Cloud-Based Web Application Firewall (WAF) License with Anti-Distribute Denial of Service (DDoS)***

***(ITB-ITD-004-11-07-2022)***

	<p>either be template based or customized.</p> <p>Is the expectation for the reports to be automatically generated or manually curated? What is the expected frequency of the reports?</p>			
	<p>6.1.1 With least 1 technical support personnel certified in the solution being offered.</p> <p>With reference to Section 6.3, suppliers are required to have at least 3 certified system support engineers on the product proposed.</p> <p>For consideration to at least one (1) technical support personnel in the solution being offered be retained.</p>	1 is acceptable		
	<p>6.1.3 Resolve issue/problem raised within 4 hours of receipt of call.</p> <p>Request to remove from the TOR. We cannot commit resolution time.</p>	If 4-hour resolution is no feasible, at least response time		
5. Section 5 – Support Coverage	<p><u>Support Coverage</u></p> <table><tr><td>Support Coverage 24x7</td><td><p>Comprehensive 12 months maintenance and support which includes:</p><ul style="list-style-type: none"><li>1. Software/Server Support<ul style="list-style-type: none"><li>• 24x7 Hardware support coverage</li><li>• 24x7 Service availability, call and on-site response time based on the severity level defined in Response Time Commitments</li><li>• Parts Warranty and Replacement</li></ul></li><li>2. Software Support<ul style="list-style-type: none"><li>• Patch and Firmware updates (provided equipment machine is still supported by manufacturer/principal)</li></ul></li><li>3. Remote Support<ul style="list-style-type: none"><li>• Technical support through electronic mail, telephonic, messaging platforms and other remote access facilities authorized by UCPBS. If unable to resolve remotely, on-site support shall be done.</li></ul></li></ul></td></tr></table> <p><u>Service Management and Reporting</u></p> <p>Supplier shall handle and manage UCPBS service request in accordance with workflow procedures approved by UCPBS.</p> <p>Quarterly reports on support requests and reported incidents shall be completed by Supplier and submitted to UCPBS. Quarterly status reports shall be discussed by the Supplier Account Service Manager with UCPBS to ensure that UCPBS is aware of possible support issues and risks faced by UCPBS.</p> <p>No. 1 &amp; 2 is not applicable for a Software as Service (SaaS) offering.</p>	Support Coverage 24x7	<p>Comprehensive 12 months maintenance and support which includes:</p> <ul style="list-style-type: none"><li>1. Software/Server Support<ul style="list-style-type: none"><li>• 24x7 Hardware support coverage</li><li>• 24x7 Service availability, call and on-site response time based on the severity level defined in Response Time Commitments</li><li>• Parts Warranty and Replacement</li></ul></li><li>2. Software Support<ul style="list-style-type: none"><li>• Patch and Firmware updates (provided equipment machine is still supported by manufacturer/principal)</li></ul></li><li>3. Remote Support<ul style="list-style-type: none"><li>• Technical support through electronic mail, telephonic, messaging platforms and other remote access facilities authorized by UCPBS. If unable to resolve remotely, on-site support shall be done.</li></ul></li></ul>	Agree, disregard
Support Coverage 24x7	<p>Comprehensive 12 months maintenance and support which includes:</p> <ul style="list-style-type: none"><li>1. Software/Server Support<ul style="list-style-type: none"><li>• 24x7 Hardware support coverage</li><li>• 24x7 Service availability, call and on-site response time based on the severity level defined in Response Time Commitments</li><li>• Parts Warranty and Replacement</li></ul></li><li>2. Software Support<ul style="list-style-type: none"><li>• Patch and Firmware updates (provided equipment machine is still supported by manufacturer/principal)</li></ul></li><li>3. Remote Support<ul style="list-style-type: none"><li>• Technical support through electronic mail, telephonic, messaging platforms and other remote access facilities authorized by UCPBS. If unable to resolve remotely, on-site support shall be done.</li></ul></li></ul>			

WSP

**BIDS AND AWARDS COMMITTEE**

July 18, 2022

**SUPPLEMENTAL / BID BULLETIN NO. 001**

***Procurement of Supply, Delivery and Installation of Cloud-Based Web Application Firewall (WAF) License with Anti-Distribute Denial of Service (DDoS)***

**(ITB-ITD-004-11-07-2022)**

	<p><u>Preventive Maintenance</u></p> <ul style="list-style-type: none"> <li>Quarterly preventive maintenance (Health Checks)</li> </ul> <p><u>Response Time Commitment</u></p> <p>Based on the assigned Severity Level (described in Annex A) of a reported incident, Supplier shall respond according to the Response Time Commitments below:</p> <table border="1"> <thead> <tr> <th>Severity Level</th><th>Maximum Response Time</th><th>Maximum Time Until Onsite</th></tr> </thead> <tbody> <tr> <td>1</td><td>30 Minutes</td><td>2 Hours</td></tr> <tr> <td>2</td><td>1 Hour</td><td>2 Hours</td></tr> <tr> <td>3</td><td>2 Hours</td><td>1 Day</td></tr> <tr> <td>4</td><td>4 Hours</td><td>2 Days</td></tr> <tr> <td>5</td><td>1 Day</td><td>Not Applicable</td></tr> </tbody> </table> <p><u>Disaster Recovery</u></p> <p>Will this cover the 2x health check that will be provided by the principal under Incidental services?</p>	Severity Level	Maximum Response Time	Maximum Time Until Onsite	1	30 Minutes	2 Hours	2	1 Hour	2 Hours	3	2 Hours	1 Day	4	4 Hours	2 Days	5	1 Day	Not Applicable	
Severity Level	Maximum Response Time	Maximum Time Until Onsite																		
1	30 Minutes	2 Hours																		
2	1 Hour	2 Hours																		
3	2 Hours	1 Day																		
4	4 Hours	2 Days																		
5	1 Day	Not Applicable																		
	<p><u>Incidental Services</u></p> <ul style="list-style-type: none"> <li>Supplier shall provide health check report conducted by the principal, at least twice (2x) over the year period. The said checks will also require validation by UCPBS IT Security Unit. <ul style="list-style-type: none"> <li>Upon turn-over</li> <li>Sixth (6<sup>th</sup>) month after turnover</li> </ul> </li> <li>Retooling and reorientation of the Information Security Administration organization on the used and administration of the technology/Solution.</li> </ul> <p>May I clarify if this 2x health check is just the same under Preventive Maintenance.</p>	No, this should be separate from the incidental services																		
6. Section 6 - Supplier Qualification	<p>1. Supplier shall provide Principal's Certification of Partnership or submit a current and valid certification from principal or manufacturer issued within the last 3 years.</p> <p>For your consideration for at least one year partnership certificate</p>	Yes, same as PM																		
	<p>2. Supplier must be a Certified Expert support provider and is trained to offer and deliver on-site replacement services.</p> <p>For your consideration to rephrase to: must be a certified support provider to offer and deliver services</p>	Agreed																		
	<p>3. Supplier shall have at least three (3) certified system support engineers on the product being proposed.</p> <p>For your consideration to at least one (1) certified system support engineer on the product being processed.</p>	Agreed, provided Product specific																		

WSP





**BIDS AND AWARDS COMMITTEE**

July 18, 2022

**SUPPLEMENTAL / BID BULLETIN NO. 001**

***Procurement of Supply, Delivery and Installation of Cloud-Based Web Application Firewall (WAF) License with Anti-Distribute Denial of Service (DDoS)***

**(ITB-ITD-004-11-07-2022)**

	<p>5. Supplier must submit at least three (3) installed bases in financial institution and government entities (provide client name, contact person, address, telephone number and email)</p> <p>For your consideration to at least one(1) installed based to any financial government entity.</p>	Yes
	<p>6. List of Similar Ongoing and Completed Projects similar in scope and at least 50% of the cost of the Project under consideration including names and contact information of the projects' proponents.</p> <p>May I clarify if the completed project refers to "Single Largest Completed Contracts"?</p> <p>For ongoing projects, it can be any IT products and solutions as basis for the NFCC computation.</p>	<p>Yes</p> <p>Yes</p>
7. Technical Specifications - Item no.3	<p>3.4.1.4a and 3.4.1.4b Cloud Management and On-Site Management</p> <p>Can this be either of the two management options instead of complying both?</p>	Yes
	<p>3.6.1.1 With at least one (1) technical support personnel who is certified for the solution being offered</p> <p>Just want to clarify that this can be a local engineer from all partners of the bidder (system integrator, distributor, or principal)</p>	Yes
	<p>3.6.1.3 Resolve issue/problem raised within four (4) hours from receipt of call</p> <p>Not all issues can be resolved within 4-hour time frame. Can this be revised from "Resolve Issue" to "Response /Update" instead.</p>	Yes
8. Single Largest Completed Contract (SLCC)	<p>Can this be a project under the systems integrator or the distributor partner with?</p>	Yes

1/05/22



**BIDS AND AWARDS COMMITTEE**

July 18, 2022

**SUPPLEMENTAL / BID BULLETIN NO. 001**

***Procurement of Supply, Delivery and Installation of Cloud-Based  
Web Application Firewall (WAF) License with Anti-Distribute Denial  
of Service (DDoS)***

***(ITB-ITD-004-11-07-2022)***

2. Reminders:

- a. The **deadline for bid submission will be on or before July 25, 2022(Monday) at 3:00pm**, at the BAC Secretariat Office located at Penthouse, UCPB Corporate Offices Building, 7907 Makati Avenue, Makati City. Late bids or those submitted after **3:00pm of July 25, 2022 shall not be accepted**.
- b. Bidders may submit their bid documents days ahead of the deadline for the submission in order to avoid late submission.
- c. **Bid Opening will be on July 28, 2022 (Thursday) at 2:30pm** via MS Teams. Bids will be opened in the virtual presence of the bidder's representatives who choose to attend.
- d. Each and every page of the Bid Form must be appropriately signed by the bidder or the bidder's authorized representative. The authorization should also be attached. Failure to do so shall be a ground for the rejection of the Bid.
- e. All licenses, permits and other required clearances should be valid at the time of submission of bids, Post-qualification Evaluation and signing of the contract.
- f. The BAC expects the bidders to exercise due diligence in going through the bidding documents so that they can prepare their bids intelligently.
- g. No queries shall be entertained after this bid bulletin.

All provisions, conditions and statements in the bidding documents inconsistent with the Bid Bulletin are either modified or rendered ineffective, as the case may be.

  
**MR. JAIME JUAN RAMON N. VALERA III**  
BAC Vice-Chairperson