SUPPLEMENTAL BID BULLETIN #1

"Procurement of Various ICT Software Licenses for FY 2022, Procurement of Various ICT Supplies for FY 2022, and Procurement of One (1) Lot Server-Based Hosting and Backup for FY 2022"

I. Approved changes on Technical Specifications

Agreed between the Bids and Awards Committee, end-users, and prospective bidders during the Pre-bid Conference last December 23, 2021, are the following:

For the "Procurement of Various ICT Software Licenses for FY 2022"

- Total requirements for Adobe Creative cloud are twelve (12) licenses.
- Final total ABC of Two Million Two Hundred Sixty-Three Pesos (2, 263,000.00)

For the "Procurement of Various ICT Supplies for FY 2022"

- Ink cost will be based on the total amount of the Purchase Request not on their individual cost.
- Delivery schedule will be one hundred twenty (120) calendar days (CD).
- Approved specification for the monitor:
  - Response time: 1ms – 5ms
  - Refresh: 60hz – 144Hz
  - Contrast Ratio: 1000:1 - 10000000:1
  - Port: should consist of HDMI plus VGA or DVI.

For the "Procurement of One (1) Lot Server-Based Hosting and Backup for FY 2022"

- 99.95% is approved for the SLA requirement of standard storage and as a whole end-user is looking for 99.99% SLA for uptime.
- Prospective bidder may submit their recommended specification for the Web Application Firewall (WAF).
- Following are the approved criteria in choosing the correct and needed specification for the WAF:
  - Protection
    - Protect your web applications from web vulnerabilities and attacks without modification to back-end code
  - Monitoring
    - Monitor attacks against your web applications by using a real-time WAF log.
  - Customization

  - Customize WAF rules and rule groups to suit your application requirements and eliminate false positives.
- Features
  - SQL-injection protection.
  - Cross-site scripting protection.
  - Protection against other common web attacks, such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion.
  - Protection against HTTP protocol violations.
  - Protection against HTTP protocol anomalies, such as missing host user-agent and accept headers.
  - Protection against crawlers and scanners.
  - Detection of common application misconfigurations (for example, Apache and IIS).
  - Configurable request size limits with lower and upper bounds.
  - Exclusion lists let you omit certain request attributes from a WAF evaluation. A common example is Active Directory-inserted tokens that are used for authentication or password fields.
  - Create custom rules to suit the specific needs of your applications.
  - Geo-filter traffic to allow or block certain countries/regions from gaining access to your applications.
  - Protect your applications from bots with the bot mitigation ruleset.
  - Inspect JSON and XML in the request body.
- WAF policy and rules
  - Core rule sets
    - Application Gateway supports three rule sets: CRS 3.1, CRS 3.0, and CRS 2.2.9. These rules protect your web applications from malicious activity.
  - Custom rules
    - Application Gateway also supports custom rules. With custom rules, you can create your own rules, which are evaluated for each request that passes through WAF. These rules hold a higher priority than the rest of the rules in the managed rule sets. If a set of conditions is met, an action is taken to allow or block.
  - Bot Mitigation
    - A managed Bot protection rule set can be enabled for your WAF to block or log requests

from known malicious IP addresses, alongside the managed ruleset

- WAF modes
  - The Application Gateway WAF can be configured to run in the following two modes:
    - Detection mode: Monitors and logs all threat alerts. You turn on logging diagnostics for Application Gateway in the Diagnostics section. You must also make sure that the WAF log is selected and turned on. Web application firewall doesn't block incoming requests when it's operating in Detection mode.
    - Prevention mode: Blocks intrusions and attacks that the rules detect. The attacker receives a "403 unauthorized access" exception, and the connection is closed. Prevention mode records such attacks in the WAF logs.

II. Bidding Document Forms

Kindly refer to this link https://gppb.gov.ph/downloadables.php for the editable versions of Bid Securing Declaration and Omnibus Sworn Statement.

Prepared by:

LEOD MARTIN B. PRESADO
BAC Secretariat

Approved by:

Ruby Raterta
Digitally signed by RUBY RATERTA
Date: 2021.12.28 15:20:14 +08'00'

DR. RUBY RATERTA
Chairperson, BAC