PHILIPPINE ECONOMIC ZONE AUTHORITY

RFQ No.	2021-07-00013
Date	02 July 2021

REQUEST FOR QUOTATION
Alternative-Small Value Procurement

Name of Company:

_____

_____

Address: _____

_____

The Philippine Economic Zone Authority (PEZA), through its Bids and Awards Committee (BAC) will undertake **Alternative/Small Value Procurement** in accordance with Sec. 53.9 ofthe 2016 Revised Implementing Rules and Regulations of the Republic Act No. 9184.

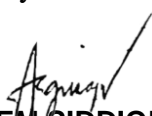|	
Name of Project	**Procurement of Isolation Platform Licenses**
Description/Specifications	**Attached Annex "A"**
Approved Budget for the Contract (ABC)	**PhP 600,000.00**
Deadline of Submission of Bid	**08 July 2021**

Interested bidders may submit their duly accomplished Price Quotation Form (Annex A) on orbefore the deadline of submission of bids to the BAC Secretariat at the PEZA Head Office, 10th Floor, Double Dragon Center, West Building, Macapagal Blvd., Pasay City.

Bidders must submit sealed quotation/s in the address given above together with the followingdocumentary requirements:

1) PhilGEPS Registration Number;
2) Valid and Current Mayor's/Business Permit 2021; and
3) Omnibus Sworn Statement (OSS).
4) BIR eFPS, Quarterly Income Tax Return (ITR)-(previous 2 quarters, BIR Form No.1701Q) (with proof of payment); and
5) BIR eFPS, Monthly VAT Declaration (last 6mos, BIR Form No. 2550-M) (with proofof payment).

Award of contract shall be given to the lowest calculated bidder which complies with the technical specifications (Annex A), and General Terms and Conditions (Annex B).

For any clarification, you may email bacsec@peza.gov.ph.

ALEEM SIDDIQUI M. GUIAPAL
BAC, Chair

10th Floor, DoubleDragon Center West Building
DD Meridian Park, Macapagal Avenue, Pasay City, 1302
Trunklines: (632) 8551-3451 · 8551-3435 to 37 · Facsimile (632) 8891-6380
E-mails: odgcbp@peza.gov.ph · info@peza.gov.ph

ISO 9001:2015 Certified Organization
with Certificate Nos AJA 08/13114 and AJA 08-009
Direct lines: (632) 8551-3432 · 8551-3454 to 55
Website: www.peza.gov.ph

Annex "A"
PRICE QUOTATION FORM
(Financial Bid)

GM ALEEM SIDDIQUI M. GUIAPAL
Chairperson, Bids and Awards Committee
Philippine Economic Zone Authority (PEZA)
8Floor, DoubleDragon Center, West Building
DD Meridian Park, Macapagal Avenue, Pasay City

Thru: BAC Secretariat

Dear Sir:

After having carefully read and accepted the Terms and Conditions of this RFQ and followed Instructions to Bidders, hereunder is our quotation/s for the items as follows:

Quantity	Specifications	Bid Price (PHP)
1 lot	**Isolation Platform License** • **Support Services** On-site deployment of isolation solution 7x24 Helpdesk including weekends and holidays Technical training for PEZA technical personnel (please see Annex B for complete technical specifications)	

*Bid Price should be inclusive of government tax

_____
Signature over Printed Name

_____
Office Telephone No. / Mobile Telephone No.

_____
Email address/es

INSTRUCTIONS:

(1) Accomplish this RFQ correctly and accurately.
(2) Do not alter the contents of this form in any way.
(3) Failure to comply with any of the mandatory requirements will disqualify your quotation.
(4) Failure to follow these instructions will disqualify your entire quotation.

QTY	Specification	
1 Lot	**Browser Isolation Platform**	
	ISO Certification	Solution must be from an ISO certified company
	Solution Server	Will be provided by bidder for on-prem implementation
	Internet Connection	25Mbps Internet connection will be provided by bidder for duration of the contract
	Description	The proposed solution must be using signature less threat Isolation technique as its core technology without relying on any form of detection based technologies to eliminate the risk of web-borne malware reaching user devices via compromised or malicious web sites.
		Fetch, execute & rendering must all be isolated and must never take place at any given time at endpoint.
		Protect against zero day and known exploits, malware, including fileless malware that are web borne.
		Protect against potential Ransomware attacks emanating through compromised websites.
		Scanning against malicious code delivery that comes by cross site scripting.
		Render additional protection by providing protection against potentially malicious URL's by opening them in Safe Mode.
		The solution shall have capability to disable user credential input while accessing the unknown risky websites.
		Protect any Malvertising attacks impacting the end user systems.
		Must be capable of handling multiple users browsing sessions with complete isolation.
		Ability to render documents in read-only mode to ensure any harmful macros contained within them are isolated.
		End user web sessions and all active content (e.g. JavaScript, Flash, etc.), whether good or bad, shall be fully executed and contained in an Isolation Platform
		Proposed solution must be able to co-exists with client's firewall and proxy solutions. System and security events can also be consumed by SIEM solutions for reporting and event management.
		The solution must render the entire web page remotely to ensure none of the code from original website can enter the organization network.

		Protect against email threats, HTTP and HTTPS attacks. Ensure coverage of SSL threat surface while preserving user experience.
	User Experience	The solution must not have any or minimal latency on image loading time, keypress such as typing and scrolling, mouse scrolling, java script execution and video streaming.
		The solution shall preserve native end user web browsing experience and avoid disruption to work flow operations such as continue support of copy-paste, find-replace, and printing functionality.
		The solution must be able to support various commercial available browsers such as IE, Edge, Safari, Chrome and Firefox.
		The solution shall support browser running on Windows, Mac & Linux OS.
	Administration and Reporting	Should provide a single portal to manage the entire deployment including policy creation, reporting, monitoring and system health check.
		Ability to block certain category of URL's to provide additional control and security.
		The solution shall provide configurable policy options which can be applied at the organization or group or at user level.
		The solution shall provide a single view of the user session and browsing activity details. System should provide the details of activity such as file downloads and related information.
		Should provide rich dashboards related to the browsing threats, user behavior, categories of website being visited.
	General	Solution should be provided as a software which can be deployed on existing hardware infrastructure. Vendor should provide the required specifications based on understanding of existing environment and setup.
		Provide details on solution's architecture, and indicate how each component communicates (software, virtual appliance, agents, etc.).
		Proposed solution must be able to provide a multi-tenant central dashboard for remote visibility into security threats as well as policy management to ensure protection. In addition, administrators can also generate periodic reports.
	Security	Solution should comply to Vulnerability Assessment Testing.

		Granular segregation of user roles and access rights within the system shall be enforced.
		Only designated users should have direct access to database, log files or any other critical information.
		Any communication initiated by the system to external sites should be documented with business justifications.
		System shall be able to define the TCP/UDP ports required for its communication.
		The solution shall support data encryption between the user endpoint and system host.
	Training/Knowledge transfer	Vendor shall provide the required training and technology transfer to the Systems and Security team at client for effective operation of the proposed solution.
		Vendor to provide basic troubleshooting guide and a detailed walkthrough of the same.
		Concerned teams to be informed of any major security patches or updates and related trainings if any.
	Deployment	Vendor should provide detailed deployment plan and ensure timely adherence to the process.
		Proposed solution can be deployed as a cloud service or as on-premise physical or virtual deployment for a single customer or as a multi-tenant solution.
		Vendor to propose the onboarding process for various teams and come up with a joint plan after working with concerned prospect's teams
		Vendor should have deployment team working within the prospect's premises in the initial deployment phase.
		Agentless deployment with standard browsers to cover managed and unmanaged endpoints.
		Local (in-country) hosting to adhere to regulatory guidelines
	Integrations	Proxy: Co-exist with a 3rd party proxy solution to continue enforcing acceptable use policy at the proxy while ensuring stronger security with isolation. Can also be used to selectively isolate users and/or specific websites.
		Sandbox: Leverage existing investment to ensure downloaded files are scanned for zero-day threats.
		LDAP: Integrate with identity and access management systems, e.g. Active Directory / LDAP, SAML, etc. to ensure seamless user management
		SIEM: Provide a single point of monitoring and troubleshooting with SIEM integration to ingest and

		analyze browser isolation information
	System and support Maintenance	The Vendor is required to implement, maintain and support the solution for the duration of contract term.
		Vendor should provide a detailed support model of the proposed solution with standard SLA terms and conditions.
		The proposed Web Browser Isolation Platform shall allow prospect's team to submit support request through the following means: Phone, E-mail and Customer Online Support Portal.
		Proposed solution must be able to reduce administrative complexity and overhead by eliminating the need to detect threats, instead relying on a Zero Trust model to remotely render all content.
		The Vendor should assure zero impact on end user's browsing session during maintenance/downtime.
		Vendor to provide details on how the upgrade and maintenance activities would be carried out with minimum user impact.
	Bidder's Qualification	1. Must have Certified Engineers who are regular and locally based employees.
		2. Bidder must be an authorized reseller and support provider in the Philippines
		3. Must have a Helpdesk Support System in place to accommodate PEZA technical request.
		4. Helpdesk system will provide ticket for each technical request or issues and will provide continues status and report until the resolution.
		5. Helpdesk must be available 7x24 including Saturday, Sunday and Holidays.
		6. Helpdesk system should be available for site visit.
		7. The principal must have a locally based office.
	Delivery and Project Completion Period	45 Days
	Warranty	1 Year-Parts, Service, and On-site

(Annex C)

- Bidder shall type or write in "Ink" the following on the **<u>sealed envelope</u>**:
  - his/her name or business name;
  - address; and
  - identification of the item/s being quoted.

- Delivery period: 30 calendar days upon receipt of NTP/Contract.

- Terms of payment: Through Cheque/15 working days upon receipt of original invoice.

- Winning bidder must deliver the item/s to the following address: