Republic of the Philippines
Office of the President

BCDA
Bases Conversion and
Development Authority

BAGONG PILIPINAS

*Bids and Awards Committee for Goods (BAC-G)*

## *PROCUREMENT OF DATA SECURITY AND ANALYTICS (ANNUAL SUBSCRIPTION)*

## BID BULLETIN NO. 2

This Bid Bulletin refers to the updated Technical Specifications and changes in the schedule of the bidding activities relative to the project.

### A. Additional Items in the Technical Specifications:

| DESCRIPTION |
|---|
| Reference:<br>**Section VII. Technical Specifications** |
| Inclusion: |
| **Password Management (300 licenses)** |
| The solution should create, store, and protect user credentials locally on devices, and centrally manage passwords. Credentials should be able to sync between devices in an end-to-end encrypted way. |
| The solution should use these secrets to auto-fill a user's username, password, and 2FA token to log into an application, significantly streamlining the authentication process, and it can detect when a user inputs a new password and offer to save it for next time either from the browser or desktop app. |
| The solution should be capable of password sharing for granular control over users' access levels to shared folders while providing admins with full visibility and the capacity to assign user groups to shared folders. |
| The solution should allow users to generate secure, complex passwords of up to 200 characters, removing the burden of creating and remembering them. |
| The solution should allow IT to easily view and track user access to non-SSO accounts, monitor for password best practices and password health (including checking for weak passwords), view and log activity, manage shared user folders, and see a list of users' devices from the console. |
| The solution should have a password health score that scans all passwords stored in the vault and checks its vulnerability. |
| The solution should support multiple browsers and systems. It should include a desktop application supported by Mac, Linux, Windows, iOS, and Android and a multi-browser extension. |

Attached is the updated Section VII. Technical Specification of the Bidding Document ***(Annex A)***

**B. Changes in the Schedule of Bidding Documents:**

| ACTIVITY | FROM | TO |
|---|---|---|
| **Deadline of Submission and Receipt of Bids** | **9:00 AM, 22 November 2024** | **12:00 PM, 25 November 2024** |
| **Opening of Bids** | **2:30 PM, 22 November 2024** | **1:00 PM, 25 November 2024** |

The above changes further amend the bidding documents accordingly. **The Submission and Opening of Bids will be conducted face-to-face** at the **BCDA Corporate Center, 2nd Floor, Bonifacio Technology Center, 31st St. corner 2nd Ave, Bonifacio Global City, Taguig City.** Alternatively, bidders may opt to attend online via Zoom. The meeting link will be provided upon request by the prospective bidders to the BAC-G Secretariat through the email address: bacgsecretariat@bcda.gov.ph.

1. For those attending in person, please consider the following guidelines:
   - Attendees to the Pre-bid Conference and Opening of Bids are expected to follow the BCDA Health protocols; and
   - Observers/representatives who show signs of COVID-19-related symptoms are advised to join online and will not be allowed to enter the BCDA premises.

This Bid Bulletin is being issued pursuant to Sections 22.5.2 and 22.5.3 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184.

Issued on **18 November 2024 (MONDAY).**

**BIDS AND AWARDS COMMITTEE FOR GOODS**

By: [redacted]

**RICHARD BRIAN M. CEPE**
*Chairperson*

ANNEX A

# *Section VII. Technical Specifications*

## *Procurement of Data Security and Analytics (Annual Subscription)*

| TERMS OF REFERENCE / TECHNICAL COMPLIANCE FORM | | | |
|---|---|---|---|
| **1 Lot** | **Description** | **Compliance** | |
| | | **Compliant** | **Non-compliant** |
| | **Data Security and Analytics (400 Licenses Annual Subscription)** | | |
| | The solution should have capabilities of Zero Trust for connectivity and Security Service Edge for security into a single unified service that protects all transactions to enterprise-owned resources and the public Internet. | | |
| | The solution should be a Zero Trust Security Service Edge that allows users to securely connect to any applications from any location. | | |
| | The solution must have these security features in a single platform to provide comprehensive protection to all users regardless of their location: | | |
| | 1. Centralized Management Console | | |
| | 2. Network DLP | | |
| | 3. Outbound Firewall Protection with Threat Prevention/IPS | | |
| | 4. Malware Defense | | |
| | 5. URL Filtering/controls | | |
| | 6. Malware Sandboxing | | |
| | 7. SSL Traffic Management | | |
| | 8. CASB | | |
| | 9. DNS Security | | |
| | 10. Secure Access to Private Resource | | |
| | 11. Zero Trust Features based on NIST 800-207 | | |
| | 12. Reporting and Analytics | | |
| | The solution should provide full native support for Windows, iOS, MacOS, Android, Chrome OS and Linux OS. | | |
| | The solution should have a unified and native single service edge for both Private and Public Access and does not require any third-party solution. | | |
| | The solution should support deployment architectures such as Full Cloud, Hybrid or Full On-prem Architecture. | | |
| | The solution should provide containerized architecture, having dedicated cloud gateways and reporters with dedicated/exclusive/static Public IP Addresses from the principal. | | |
| | The solution should provide a containerized architecture/dedicated data plane that allows full session inspection. | | |

[redacted]

| | | | |
|---|---|---|---|
| | The solution should provide a containerized architecture/dedicated data plane that provides SSL traffic visibility for both proxy and dynamic analysis engines. | | |
| | The solution should provide dedicated Public IPs from the product owner to allow tenant restriction controls or conditional access for external services or public SaaS applications (e.g. O365, Azure, Google etc) | | |
| | The solution should provide complete data isolation for each customer allowing for complete isolation of HTTPS decryption keys, log data and geo-zoning for GDPR. | | |
| | The solution should provide full control and customer separation for data processing and log retention for data sovereignty and compliance | | |
| | The solution should be capable of supporting a hybrid architecture, having a cloud SaaS service and appliance on-premise which provide 100% features parity and any policies or controls configured within the cloud service should be automatically extended into the on-prem appliance. | | |
| | The solution must have a principal's local presence in the Philippines which includes locally based sales, implementation, and support team | | |
| | **Features:** | | |
| | **Complete Web/URL Filtering** | | |
| | The solution must support forward proxy HTTP/HTTPS traffic flows including other TCP ports. | | |
| | The solution should support protocols beyond HTTP/HTTPS and inspect at the application layer (L7 FWaaS). | | |
| | The solution should have the capability to support transparent proxy type application flows. | | |
| | The solution should have the capability to direct traffic via explicit proxy. | | |
| | The solution should be able to support these data traffic redirection or connectivity methods below for on-site and mobile users: | | |
| | 1. Agent - Typically used on managed devices to redirect data traffic to the solution whether onsite or remote. | | |
| | 2. Proxy – Settings configured and locked in the web browser | | |
| | 3. DNS – DNS settings configured on the endpoint to point to the service | | |
| | 4. GRE Tunnels – The tunnel is established between a router or firewall to the solution | | |
| | 5. IPSec Tunnels – The tunnel is established between a router or firewall to the solution | | |
| | 6. Network Connector - It can be deployed in two formats(Virtual Machine in OVF format and Docker Image format) that provide a path to private resources for remote users and can also be used to automatically route outbound data to the solution from a location. | | |
| | 7. WCCP/ITD – Typically used on routers to redirect traffic to on-premise appliance | | |
| | The solution must have the ability to steer traffic directly from a managed endpoint to the associated secure web gateway. | | |
| | The solution must provide a complete list of web categories which can be used to protect users against threats, unsuitable content, and unproductive sites. | | |
| | The solution must provide auto-categorization of new web sites. | | |
| | The solution must have the capability to identify uncategorized sites and take action based on the policy. | | |

[redacted]

| | | | |
|---|---|---|---|
| | The solution should have the capability to restrict which browsers and operating systems that can be utilized by users that are connected to the platform. | | |
| | The solution must allow for customer creation of URLs and block lists. | | |
| | The solution should support registry entries and IP addresses in URL lists. | | |
| | The solution should allow customers to create a list of inappropriate keywords aside from the predefined keyword lists. | | |
| | The solution should allow customers to restrict activity over specific networking ports. | | |
| | The solution should allow customers to prevent users from downloading files that have specific extensions. | | |
| | The solution should allow for customers to prevent access to specific top-level domains (TLDs). | | |
| | The solution must support policy layering which allows advanced configurations to be applied based on multiple and potentially regularly changing user criteria like IP/Username/Geo-Location or Group/s. | | |
| | The solution must support user, group, and business unit levels for granular policy enforcement. | | |
| | The solution must have the ability to use URLs/Domains and CIDR notation in policy creation, URL lists, etc. | | |
| | The solution must have the ability to bypass URLs/Domains and IPs (as source or destination) in policy creation, URL lists, etc. | | |
| | The solution should allow for customers to create custom URL categories. | | |
| | The solution must provide access controls based on user, group, IP, or geographic location. | | |
| | The solution must have the capability to apply SSL decryption to all or selected destinations | | |
| | The solution must have the capability to support PAC file hosting. | | |
| | The solution must provide URL look up functionality against category or policy. | | |
| | The solution must be able to detect and provide appropriate action for TLS certificate issues, including, but not limited to: Expired certs, Cert Domain Mismatches, Self-Signed Certs, Untrusted Certs, Invalid CAs, Insecure ciphers, Too Long Cert Chains and etc. | | |
| | The solution should allow for XFF header modifications. | | |
| | The solution should allow for the creation of whitelist/blacklist that can be updated via API | | |
| | The solution must be capable of creating/modifying custom user block messages. | | |
| | The solution should support transparent authentication without so much reliance on directory service integration. | | |
| | **SSL traffic management** | | |
| | The solution should provide granular SSL traffic controls and options for different TLS versions and Ciphers. | | |
| | The solution should provide a broad array of selective decryption options that allow certain traffic to be decrypted while leaving other traffic untouched based on category, group, | | |

[redacted]

| | | | |
|---|---|---|---|
| | domain, app or network subnet. | | |
| | **CASB** | | |
| | The solution should natively support O365 and Google Tenant Restriction. | | |
| | The solution must support the CASB feature to apply fine grained controls on SaaS and Social Media applications. | | |
| | The solution should have the capability to enforce safe search across popular search engines such as Google, Yahoo, Bing and Youtube. | | |
| | The solution should allow for customers to manage access to any SaaS Applications via conditional access or via custom CASB rules for bespoke company's compliance requirements. | | |
| | The solution should have the capability to control file uploads to sanctioned and unsanctioned cloud services including generic websites. | | |
| | The solution must support API CASB integrations for the major SaaS applications such as Box, Google and O365. | | |
| | The solution must support out-of-band data discovery via API CASB to highlight sensitive data across SaaS applications and situations where sensitive content is shared publicly via share links. | | |
| | **Malware Defense** | | |
| | The solution should provide capabilities that include malware scanning of full content and files, including data transferred within encrypted HTTPS connections. | | |
| | The solution should support multiple engines to detect and prevent threats in all traffic processed by the platform, options include; C2 and Threat Feed Defense, Content-Based Malware Defense, Email File Types scanning,and etc. | | |
| | The solution should provide defense-in-depth and comprehensive protection by leveraging leading Cybersecurity companies and cutting edge malware defense technology. | | |
| | The solution should allow malware scanning rules to be fully configurable which include the content types, target destination/s, traffic direction, priority, action etc. | | |
| | The solution should have malware sandboxing built into the platform for further analysis of suspicious content. | | |
| | The solution must support heuristic analysis that looks at patterns within the transactions to determine whether the transaction might be malicious or risky. | | |
| | The solution must support Google Web Risk Protection that allows feeds from the Google Risk database to be ingested and applied to transactions. | | |
| | The solution should have IDS/IPS signature based capabilities. | | |
| | The solution should have IDS/IPS tuning capabilities. | | |
| | The solution must have the capability to import custom created IDS/IPS signatures. | | |
| | **Zero Trust Capabilities** | | |

[redacted]

|  |  |  |  |
|---|---|---|---|
|  | The solution should implement all of the core tenets and network requirements of the NIST 800-207 Zero Trust Architecture publication. |  |  |
|  | The solution should be a single unified Zero Trust Security Service Edge that can be used to apply consistent security policies across all resources and users, regardless of resource or user location. |  |  |
|  | The solution should have the ability to catalog all resources an enterprise needs to protect, including applications, data, and services. |  |  |
|  | The solution should have the ability to label resources to identify the type of resources present within an organization. |  |  |
|  | The solution should have the ability to categorize resources by type, functional category, and location. |  |  |
|  | The solution should have the ability to assign a risk and impact level to resources. |  |  |
|  | The solution should have the ability to catalog all assets and devices accessing sensitive resources within an organization. |  |  |
|  | The solution should have the ability to catalog all users accessing sensitive resources within an organization. |  |  |
|  | The solution should have the ability to force modern authentication, such as SAML or OIDC, for ALL resources, including resources that do not support modern authentication. |  |  |
|  | The solution should support Automatic Application & Service discovery to find shadow IT and resources that need protection. |  |  |
|  | The solution should have Advanced Trust Algorithms that adaptively and automatically score users, assets, resources, and transactions to resources in real-time. |  |  |
|  | The solution should have an Asset and Posture management to ensure assets meet minimum requirements before accessing critical resources. |  |  |
|  | The solution should have continuous adaptive access trust scoring algorithms that include scoring and adaptive access decisions based on MFA, impossible user travel, geographic location at the time of resource access, firewall and anti-malware being enabled, disk encryption, and much more. |  |  |
|  | The solution should have the capability to create resource policies according to the NIST 800-207 Zero Trust Architecture that automatically denies unauthorized users access to enterprise-owned resources while only allowing access to approved users. |  |  |
|  | The solution should have NIST 800-207 Criteria-Based access policies. |  |  |
|  | The solution should have NIST 800-207 Score-Based access policies. |  |  |
|  | The solution should have Zero Trust reporting capabilities including reports by type and category, security impact, location, and score. |  |  |
|  | The solution should have the ability to connect resources located on private networks, such as resources in an office, within Azure, AWS, or other cloud providers. |  |  |
|  | The solution should provide the capability to access private resources based on domain or IP/Subnet. |  |  |
|  | The solution should not allow users to connect directly to the private network so that other network resources are protected from unnecessary risks. |  |  |

[redacted]

| | | | |
|---|---|---|---|
| | **Data Loss Prevention** | | |
| | The solution should be able to detect, alert, and stop the transfer of sensitive data to and from the cloud. | | |
| | The solution should be capable of scanning for Credit card numbers, email addresses, and other Personally Identifiable Information (PII). | | |
| | The solution should be able to process and parse targeted files, ensuring that even compressed content within a compressed file is accessible to the detection engines. | | |
| | The solution should have a built-in content detection and content analysis engine that gives the ability to search for sensitive content with minimal configuration. | | |
| | The solution must be able to effectively detect and prevent unique identifiers using regular expression, keywords and boolean constructs. | | |
| | The solution should have the ability to set thresholds that trigger a DLP event. | | |
| | The solution should have the ability to mask captured DLP data when an event is triggered. | | |
| | The solution should have the ability to create and apply different DLP Content Analysis Rules depending on the destination. | | |
| | The solution should have the ability to prevent content transfers, including to personal destinations, based on document data labelling. | | |
| | The solution should have the ability to read labels within documents from popular data labelling platforms, including Microsoft Information Protection (MIP), Boldon James, and Stealthbits. | | |
| | The solution should have the capability to scan for content within connected applications via API CASB to find potentially risky situations, such as when sensitive documents are published via shared links with public permissions. | | |
| | **Integrations** | | |
| | The solution should support native integration with Splunk, FireEye Helix and Microsoft Sentinel for log forwarding. | | |
| | The solution should support integration with any SIEM with fully customizable log format for forwarding. This includes forwarding protocols syslog, SCP, and SFTP. | | |
| | The solution should support ICAP Service for content analysis offloading | | |
| | The solution should support Cloud IDP integration such as but not limited to Azure/Okta/Google or Any IDP via SAML/OIDC. | | |
| | The solution should support RESTFUL OPEN API which can integrate with any third party vendor. | | |
| | **Reporting** | | |
| | The solution should provide a dedicated reporter or cloud storage with dedicated Public IP Address as consolidation point of all generated events coming from users from any location. | | |
| | The solution should be equipped with an advanced report manager, capable of tracking and generating statistics for a variety of aspects of network traffic. | | |
| | The solution should provide information on all activity from any user/device anywhere in real time and also have the ability to backtrack historical events. | | |

[redacted]

| | | | |
|---|---|---|---|
| | The solution should allow the organization to generate reports on-demand or on a schedule basis. | | |
| | The solution should have the capability to provide a threat dashboard that gives the administrator an instant visibility into any infections on the network. | | |
| | Email alerts should be provided throughout the platform including alerts for Advisories, Maintenance, and Updates. | | |
| | **Management Console** | | |
| | The solution must provide single-pane-glass management that allows administrator to do all administrative tasks such as policy configurations, viewing of reports, troubleshooting including packet capture capability from the containerized gateways and etc. | | |
| | The solution must have a management console that is accessible from anywhere and every delegated administrator has the option to enable MFA as an added security layer for access. | | |
| | **Compliance and Certification** | | |
| | The solution should support and committed to security standards and compliance: | | |
| | SOC 1 Type II | | |
| | SOC 2 Type II | | |
| | ISO-9001 | | |
| | ISO-27001 | | |
| | FedRAMP | | |
| | Cloud Security Alliance STAR Level 1 | | |
| | Cloud Security Alliance STAR Level 2 | | |
| | StateRAMP | | |
| | **Qualifications** | | |
| | Bidders should have completed within five (5) years from the date of submission and receipt of bids, a contract similar to the Project.<br>Bidder must be an authorized Partner of the product owner that the bidder is offering to ensure that support / services will be provided to BCDA. The bidder must show proof of partnership with the product owner such as certification, etc. to be submitted during the Post Qualification<br>Bidders must have a certified engineer of the product that they are offering and will directly handle/manage the deployment. The Engineer must show proof of certification during post-qualification. | | |
| | **Scope of Services** | | |
| | Installation, configuration, testing, and maintenance of the Data Security and Analytics Solution. | | |
| | **Implementation Period** | | |
| | The installation, configuration, and testing of 350 devices should be completed within ninety (90) days upon receipt of NTP. | | |

[redacted]

| | | | |
|---|---|---|---|
| | The subscription period is twelve (12) months starting from the initial installation to devices. | | |
| | **Training/ Knowledge Transfer** | | |
| | Should provide knowledge transfer/refresher training min for 10 pax | | |
| | **Support Services** | | |
| | Should provide 24/7 support with onsite assistance depending on severity as determined by the BCDA team to be provided by a local provider | | |
| | **Payment Terms** | | |
| | BCDA agrees to pay the total amount inclusive of all applicable taxes and fees upon issuance of Certificate of Completion and Acceptance. | | |
| | **Inclusion:** | | |
| | **Password Management (300 licenses)** | | |
| | The solution should create, store, and protect user credentials locally on devices, and centrally manage passwords. Credentials should be able to sync between devices in an end-to-end encrypted way. | | |
| | The solution should use these secrets to auto-fill a user's username, password, and 2FA token to log into an application, significantly streamlining the authentication process, and it can detect when a user inputs a new password and offer to save it for next time either from the browser or desktop app. | | |
| | The solution should be capable of password sharing for granular control over users' access levels to shared folders while providing admins with full visibility and the capacity to assign user groups to shared folders. | | |
| | The solution should allow users to generate secure, complex passwords of up to 200 characters, removing the burden of creating and remembering them. | | |
| | The solution should allow IT to easily view and track user access to non-SSO accounts, monitor for password best practices and password health (including checking for weak passwords), view and log activity, manage shared user folders, and see a list of users' devices from the console. | | |
| | The solution should have a password health score that scans all passwords stored in the vault and checks its vulnerability. | | |
| | The solution should support multiple browsers and systems. It should include a desktop application supported by Mac, Linux, Windows, iOS, and Android and a multi-browser extension. | | |
| | | | |

**Notes to bidders:**

- All specifications are minimum requirements. Proponents may propose equivalent or higher specifications.
- The obligation for the warranty shall be covered by Retention money in an amount equivalent to at least one percent (1%) of the total contract price. The said amount shall only be released after the lapse of the warranty period.

***Bidder's Authorized Representative:***
Name: ____________________
Legal capacity: ____________________
Signature: ____________________
Duly authorized to sign the Bid for and on behalf of: ____________________
Date: ____________

[redacted]