DOST-ASTI Bids and Awards Committee
Invitation to Bid (Public Bidding)

IB No:	24-10-5026	**Date:**	October-15-2024
PR No:	GAA-24-09-19936	**Date:**	September-19-2024

Source of Funds:	
Total ABC:	Php 2,021,557.40
Time, Date & Venue of Pre-bid Conference:	October 24, 2024, 9:00 AM at Videoconferencing (MS Teams)
Time and Date of Submission of Bids:	November 05, 2024, 09:00 AM
Time, Date & Venue of Opening Bids:	November 05, 2024, 9:30 AM at DOST-ASTI & Videoconferencing (MS Teams)
Date of availability of Complete Set of Documents:	October 17, 2024
Deadline of Potential Bidder's Clarifications:	October 26, 2024
Deadline of ASTI's Supplemental Bid Bulletin:	October 29, 2024
Delivery Schedule:	

The *Department of Science and Technology (DOST)* - Advanced Science and Technology Institute (ASTI), through its Bids and Awards Committee (BAC), hereby invites all interested Bidders to submit their bids for the *item/s* listed below. *Section II. Instructions to Bidders (ITB) of the DOST-ASTI Bidding Documents provides information necessary for bidders to prepare responsive bids, in accordance with the requirements of DOST-ASTI. The ITB likewise provides information on bid submission, eligibility check, opening and evaluation of bids, post-qualification, and award of contract.*

Bidding will be conducted through open competitive bidding procedures *using a non-discretionary "pass/fail" criterion as specified in the 2016 revised Implementing Rules and Regulations of Republic Act No. 9184.*

A complete set of *DOST-ASTI Bidding Documents may be acquired by interested Bidders on the date and address given on this document, and upon payment of the applicable fee, pursuant to the latest Guidelines issued by the Government Procurement Policy Board. Further, the DOST-ASTI Bidding Documents may be accessed through the DOST-ASTI website (https://asti.dost.gov.ph/).*

For further inquiries, *you may contact the* ***DOST-ASTI BAC Secretariat*** *at telephone number* ***+63 2 8249-8500 / +63 2 8426-9755 local 1206/1212*** *or send your message to* ***bac-sec@asti.dost.gov.ph*** .

Respectfully,

Bayani Benjamin R. Lara Digitally signed by Bayani Benjamin R. Lara

BAYANI BENJAMIN R. LARA
BAC Chairperson

NO.	TECHNICAL SPECIFICATIONS	QTY	UNIT	UNIT PRICE(Php)	TOTAL PRICE(Php)
1	**PROCUREMENT OF SOFTWARE LICENSE SUBSCRIPTION TO SOFTWARE PLATFORM FOR ONLINE MEETING, WEBINAR, EVENTS** 1. GENERAL OVERVIEW 1.1. DOST-ASTI is seeking qualified and competent bidders for the supply and delivery of software license subscription to software platform for online meeting, webinar, events. 1.2. The Approved Budget for the Contract (ABC) is inclusive of all applicable government taxes and service charges. 2. TECHNICAL SPECIFICATIONS.	1	lot	254441.60	254,441.60

Postal Address : ASTI Bldg., U.P Technology Park Complex, C.P. Garcia Ave., Diliman, Quezon City 1101
Website : www.asti.dost.gov.ph
Email : info@asti.dost.gov.ph
Tel No. : +632 8249-8500 +632 8426-9755
Fax No. : +632 8426-9764

2.1. Quantity
2.1.1. Online Meetings
2.1.1.1. 4 licenses
2.1.1.2. Host up to 100 participants per license
2.1.2. Online Webinars
2.1.2.1. 1 license
2.1.2.2. Host up to 500 participants per license
2.1.3. Online Sessions
2.1.3.1. Pay per attendee
2.1.3.2. Host up to 600 attendees
2.1.4. Online Events
2.1.4.1. 1 license
2.1.4.2. Host up to 100 attendees per license
2.2. License Type: Software subscription
2.3. Licensee Account Name: Advanced Science and Technology Institute
2.4. Licenses should be natively compatible with existing Online Meeting, Webinar, and Event Platform account (Zoom)
2.5. License(s) will be loaded under said account
2.6. Subscription Period
2.6.1. Maximum Subscription Period per License: 12 months
2.6.2. Actual contract and/or billing will be pro-rated monthly starting on actual license activation date and ending on account anniversary date
2.6.3. Proposal should indicate cost of each license (or will otherwise be computed based on total proposal amount)
2.7. License Management
2.7.1. License(s) must be centrally deployed and assignable by DOST-ASTI to its personnel through an administrative account console.

2.8. Online Meeting Platform
2.8.1. Unlimited meetings
2.8.2. Meeting Duration: 30 hours minimum
2.8.3. Technical Support: Ticket and live chat
2.8.4. Recording: Local and 5 GB cloud (per license)
2.8.5. Telephone Dial-in: Toll-based
2.8.6. Screen sharing
2.8.7. Breakout rooms
2.8.8. Virtual background
2.8.9. Personal Meeting ID
2.8.10. Team Chat
2.8.11. Host controls
2.8.12. Co-Annotation on screen share
2.8.13. Remote keyboard and mouse control
2.8.14. Multi-share
2.8.15. End-to-end encryption for meetings
2.8.16. Enterprise-grade security
2.8.17. Waiting room
2.8.18. Pin multiple people
2.8.19. Spotlight multiple people
2.8.20. Filters
2.8.21. Polling
2.8.22. Co-host and alternate host
2.8.23. Assign meeting scheduler
2.8.24. REST API
2.8.25. Streaming
2.8.26. Reporting

2.8.27. User management
2.8.28. Automated Captions
2.8.29. Whiteboards: 3
2.8.30. Mail client in app
2.8.31. Calendar client in app

2.9. Webinar Platform
2.9.1. Session Type: Webinar
2.9.2. Event Attributes
2.9.3. Duration per Session: 30 hours minimum
2.9.4. Video Panelists: 100 (49 viewable on screen at one time)
2.9.5. Event registration
2.9.6. Session branding
2.9.7. Event setup
2.9.8. Customizable pre and post event email reminders
2.9.9. Customizable registration
2.9.10. Ticketing: Basic
2.9.11. Production tools
2.9.12. Practice session
2.9.13. Audience engagement
2.9.14. Session chat
2.9.15. Live polling and results
2.9.16. Question and answer
2.9.17. Session surveys
2.9.18. Live transcription
2.9.19. Language interpreter support
2.9.20. Cloud recordings and text transcripts
2.9.21. Analytics
2.9.21.1. Performance and audience engagement reports
2.9.22. Payments and Billing
2.9.22.1. Payment Provider: PayPal
2.9.23. Post Event Features.
2.9.23.1. Recording: Cloud, Local
2.9.23.2. On-demand recording available post-event
2.9.24. Other
2.9.24.1. Attendee Networking: In-Webinar chat

2.10. Online Sessions Platform
2.10.1. Session Type: Webinar or meetings
2.10.1.1. Single session
2.10.2. Event Attributes
2.10.2.1. Duration per Session: 30 hours minimum
2.10.2.2. Video Panelists: 100 (49 viewable on screen at one time)
2.10.2.3. Event registration
2.10.2.4. Event management platform
2.10.2.5. Event information
2.10.2.6. Speaker list
2.10.2.7. Registration
2.10.2.8. Session branding
2.10.2.9. Speaker bio information
2.10.2.10. Event branding
2.10.3. Hub / Collaboration
2.10.3.1. Associated with an event hub (per license)
2.10.4. Event Setup
2.10.4.1. Customizable pre and post event email reminders
2.10.4.2. Customizable registration

2.10.5. Production Tools
2.10.5.1. Practice session
2.10.5.2. Backstage
2.10.5.3. Simulated Live Event: Pre-recorded content that starts and ends automatically
2.10.5.4. Session Resources: Allow audience to view and download documents during a session
2.10.6. Audience Engagement
2.10.6.1. Session chat
2.10.6.2. Live polling and results
2.10.6.3. Question and answer
2.10.6.4. Session surveys
2.10.6.5. Live transcription
2.10.6.6. Language interpreter support
2.10.6.7. Cloud recordings and text transcripts
2.10.7. Analytics
2.10.7.1. Performance and audience engagement reports
2.10.7.2. Detailed analytics dashboard and reporting
2.10.8. Payments and Billing
2.10.8.1. Billing management account level and hub level
2.10.8.2. Payment Provider: Stripe, PayPal
2.10.8.3. Taxation
2.10.9. Post Event Features
2.10.9.1. Recording: Cloud, Local
2.10.9.2. On-demand recording available post-event
2.10.9.3. Post event survey
2.10.10. Other
2.10.10.1. Attendee networking
2.10.10.2. In-session chat

2.11. Online Event Platform
2.11.1. Session Type: Webinar and meetings
2.11.1.1. Multi-day
2.11.1.2. Multi-track
2.11.1.3. Concurrent sessions
2.11.2. Event Attributes
2.11.2.1. Duration per Session: 30 hours minimum
2.11.2.2. Video Panelists: 100 (49 viewable on screen at one time)
2.11.2.3. Event registration
2.11.2.4. Event management platform
2.11.2.4.1. Event information
2.11.2.4.2. Speaker list
2.11.2.4.3. Registration
2.11.2.5. Session branding
2.11.2.6. Event branding
2.11.2.7. Speaker bio information
2.11.2.8. Session video previews
2.11.2.9. Streaming sessions in event lobby
2.11.2.10. Event sponsors
2.11.2.11. Expo floor
2.11.3. Hub / Collaboration
2.11.3.1. Associated with an event hub (per license)
2.11.4. Event Setup
2.11.4.1. Customizable pre and post event email reminders
2.11.4.2. Customizable registration
2.11.4.3. Ticketing: Paid, Free
2.11.5. Production Tools

	2.11.5.1. Practice session 2.11.5.2. Backstage 2.11.5.3. Simulated Live Event: Pre-recorded content that starts and ends automatically. 2.11.5.4. Session Resources: Allow audience to view and download documents during a session 2.11.6. Audience Engagement 2.11.6.1. Session chat 2.11.6.2. Lobby chat 2.11.6.3. Live polling and results 2.11.6.4. Question and answer 2.11.6.5. Session surveys 2.11.6.6. Event surveys 2.11.6.7. Live transcription 2.11.6.8. Language interpreter support 2.11.6.9. Cloud recordings and text transcripts 2.11.7. Analytics 2.11.7.1. Performance and audience engagement reports. 2.11.7.2. Detailed analytics dashboard and reporting 2.11.8. Payments and Billing 2.11.8.1. Billing management account level and hub level 2.11.8.2. Payment Provider: Stripe, PayPal 2.11.8.3. Taxation 2.11.9. Post Event Features 2.11.9.1. Recording: Cloud, Local 2.11.9.2. On-demand recording available post-event 2.11.9.3. Post event survey 2.11.10. Other 2.11.10.1. Attendee networking 2.11.10.1.1. Attendee profile creation 2.11.10.1.2. One-on-one chat 3. TECHNICAL SUPPORT SERVICE 3.1. Technical support should be available at least eight (8) hours from Monday to Friday and has the following response times: 3.1.1. Application is Down: Two (2) business hours 3.1.2. Serious Degradation: Six (6) business hours 3.1.3. Moderate Impact: One (1) business day 3.1.4. Low Impact: One (1) - Two (2) business days 3.2. End-user must be able to request technical support by phone, email, or through a website. 3.3. Access to version upgrades, new releases, bug fixes, and critical security patches, if any, must be made available during the duration of the subscription. 4. DELIVERY AND PAYMENT 4.1. License activation within fifteen (15) calendar days from issuance of Notice to Proceed (NTP). 4.2. Price shall be inclusive of all taxes, delivery, and all other related charges and fees 4.3. Payment Terms: Prescribed government terms. 4.4. It is the sole responsibility of the External Provider/Supplier/Contractor to monitor and ensure that payment methods it uses to activate the subscription (e.g., credit card, etc.) are not inadvertently charged beyond what is contracted by DOST-ASTI per issued Purchase Order (PO).				

2	**PROCUREMENT OF SOFTWARE LICENSE SUBSCRIPTION TO ENDPOINT SECURITY SOLUTION** 1. GENERAL OVERVIEW 1.1. DOST-ASTI is seeking qualified and competent bidders for the Supply and Delivery of One (1) Lot of Endpoint Security Solution. The contract's duration shall be for twelve (12) months. 1.2. The ABC is inclusive of all applicable government taxes and service charges. 2. TECHNICAL SPECIFICATIONS 2.1. The solution should offer a holistic approach in security with purpose-built XDR, Attack Surface Risk Management, and Zero Trust capabilities. 2.2. The solution must have participated with strong performance and impressive results in MITRE Engenuity ATT&CK® Evaluations 2.3. Prevention Requirements 2.3.1. The solution should offer comprehensive protection against known and unknown threats. 2.3.2. The proposed solution should have but not limited to the following prevention capabilities: 2.3.2.1. Antimalware with signature/Pattern based detection 2.3.2.2. Ransomware protection 2.3.2.3. Machine learning - pre-execution and runtime 2.3.2.4. Browser exploit protection 2.3.2.5. Behavior monitoring 2.3.2. 6. Injection protection 2.3.2.7. Script protection 2.3.2.8. Anti-exploit 2.3.2.9. C&C communication prevention 2.3.2.10. Application control 2.3.2.11. File less malware prevention 2.3.2.12. File/web reputation 2.3.2.13. Vulnerability protection and virtual patching 2.3.2.14. Integrity monitoring (server and workload only) 2.3.2.15. Log inspection (server and workload only) 2.3.3. The solution should offer a combination of signature-based malware protection, behavioral analysis, and AI/machine-learning based analysis. 2.3.4. Machine learning must have pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats. 2.3.5. The solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems or on installed software's to provide additional threat protection from programs that exhibit malicious behavior. 2.3.6. The solution must have Anti-exploit module to terminate the program exhibiting abnormal behavior associated with exploit attacks. Solution must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution. 2.3.7. The solution must provide a protection mechanism against ransomware in the event of a machine becoming compromised and should have feature with documents to be protected from	1	lot	745000.00	745,000.00

unauthorized encryption or modification.

2.3.8. The solution must be able to create copies of files being encrypted by a ransomware on the endpoint and it must be able to restore the affected files back to their original state.

2.3.9. The solution must be able to identify communication over HTTP/HTTPS protocols and commonly used HTTP ports, and allow administrators to create user defined list also.

2.3.10. The solution should have a virtual patching capability and be able to deliver the most timely vulnerability protection in the industry across a variety of endpoints.

2.3.11. The solution must support host-based firewall with stateful inspection, option to create rules on the basis of Source, Destination, Port, Protocol, Application to provide stateful inspection and high performance network virus scanning

2.3.12. The solution must have an integrated Application Control module to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting (default-deny) and lockdown capabilities.

2.3.13. The solution integrated Application Control should provide global and local real-time threat intelligence based on good file reputation data correlated across a global network.

2.3.14. The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The Devices that are able to be restricted must include but not limited to the following:

2.4.14.1. USB Storage Drives (Also able to disable autorun)

2.4.14.2. CD-ROM

2.4.14.3. Floppy Disk

2.4.14.4. Network Drives

2.3.15. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, Com/LPT, Imaging Devices, Wireless Nic, Infrared devices

2.3.16. The solution must have an integrated Data Loss Prevention capability to provide data leakage prevention.

2.3.17. The solution must have damage cleanup services to provide automated cleanup of the changes made by the malware including network and file-based malicious applications, and virus and worm remnants (Trojans, registry entries, and viral files).

2.4. Detection and Correlation Requirements

2.4.1. Should be able to collect and correlate XDR activity data for one or more vectors including but not limited to — endpoints, email, servers, cloud workloads, and networks.

2.4.2. Should include predefined detection models which combine multiple rules, and filters using techniques such as machine learning and data stacking. It should be regularly updated to improve

	threat detection capabilities and reduce false positive alerts. 2.4.3. Should have the ability to enable or disable detection models and add/configure detection model exceptions based on the organization requirements. 2.4.4. Should allow the creation of custom detection models and custom event filters that define the events the model uses to trigger alerts. 2.4.5. The solution should be able to analyze and determine if certain indicators signal an ongoing attack, enabling the network security administrator to take timely prevention, investigation, and mitigation actions against targeted attack campaigns. 2.4.6. The solution should have the capability to provide recommended actions to harden the environment against future potential attacks. 2.4.7. Should list all the events that are mapped into the MITRE ATT&CK framework, the network security administrator can use these events as starting point to do further investigations. 2.4.8. Should provide more context with mapping to the MITRE ATT&CK TTPs for faster detection and higher fidelity alerts. 2.4.9. Should have the capability to write custom search queries, add the saved queries to the watchlist, and automatically execute them against the latest telemetry data on an interval basis. 2.5. Investigation and Incident Management Requirements 2.5.1. Should be able to provide consolidated investigation and response capabilities across endpoint and servers. 2.5.2. The solution should have an AI-powered chatbot to guide with the investigations and automatically provide answers to any questions related to cybersecurity. 2.5.3. Generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets. 2.5.4. The solution should provide a platform for easier investigation like visual graphical view and timeline of the attack. 2.5.5. The solution should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents. 2.5.6. The console should provide different search methods and filters to identify, categorize, and retrieve search results. 2.6. Response Requirements 2.6.1. Add or Remove indicators of compromise to block list including but not limited to File hash, URL, IP address, and Domains. 2.6.2. Automatic and manual collection of forensic evidence from specified endpoints and upload the forensic package back to the management console for further investigation. 2.6.3. Automatic and manual collection of files and objects from specified endpoints. 2.6.4. Remotely connect to an endpoint and dump process memory.					

	2.6.5. Remote isolation of an endpoint but still maintain communication with the management server to continue with investigation. 2.6.6. Ability to remotely connect and execute custom PowerShell or Bash scripts. 2.6.7. Ability to execute custom YARA rules on the specified endpoints. 2.6.8. Ability to execute SQL queries using osquery to obtain system information on the specified endpoints. 2.6.9. Remote shell session capability and be able to execute remote commands. 2.6.10. Submit selected file or object for automated analysis in a sandbox, a secure virtual environment. 2.6.11. Ability to view and terminate active processes on a specific endpoint or multiple endpoints. 2.6.12. The solution should provide a unified platform that enables security teams to take immediate response and track actions for endpoints. 2.7. Threat Intelligence Requirements 2.7.1. The solution must collect, organize, and provide an up-to-date information resource for active Threat Campaigns and Threat Actors. 2.7.2. Threat Campaign must include information such as Threat Actor profile, Infection Chain, MITRE ATT&CK mapping, Intelligence Data, and Impact Scope. 2.7.3. Campaign Intelligence Data must include - Intelligence Reports, TTPs, Tools, Malicious Software Used, Associated CVEs, and Indicators. 2.7.4. The solution must support automatic and manual sweeping based on vendor curated and third-party custom intelligence to search your environment for indicators of compromise. 2.7.5. The solution should allow you to perform sweeps identifying indicators of compromise (IoC) and indicators of attack (IoA). 2.7.6. The solution should allow the network security administrator to manually add IoCs such as File Hashes, IP Addresses, Domains, and URL's as part of the custom intelligence. 2.7.7. Shall be able to view information about suspicious objects that has been obtained by analyzing the suspicious file in a sandbox, a secure virtual environment. 2.7.8. The solution should allow the network security administrator to build custom intelligence by subscribing to third-party threat intelligence feeds. 2.8. Deployment, Management, and Operations 2.8.1. The solution must support Windows endpoints, including Windows Servers. 2.8.2. The solution must support macOS endpoints. 2.8.3. The solution must support Linux endpoints. 2.8.4. The solution must include Mobile Security capability compatible with Android, iOS/iPadOS, and ChromeOS operating systems 2.8.5. The solution must support persistent and non-persistent virtual desktop infrastructure (VDI) environments. 2.8.6. The solution must support multi-session VDI solutions without changing or limiting the functionality of your virtual desktop operating systems				

	2.8.7. The solution deployment model must support air-gapped, on- premises, and hybrid deployments. 2.8.8. The solution should have the capability to automate a variety of actions using Security Playbooks to help reduce workload and speed up security tasks and investigations. 2.8.9. The solution needs to include an ability to build security playbooks against threats and risks, such a blocking the activity of a file, shutting down an endpoint, disconnecting an endpoint from the internet, entering files into quarantine, deleting malicious files and etc. 2.8.10. The solution should have the capability to create playbooks from scratch or use built-in templates to suit the organization's specific needs. 2.8.11. Security playbook template types should include but not limited to the following XDR threat investigation actions. 2.9.12.1. Automated Response Playbook 2.9.12.2. Endpoint Response Actions 2.9.12.3. Incident Response Evidence Collection 2.8.12. Solution should be capable of integrating with a cybersecurity platform that is capable of managing the organization’s Endpoint and network in a single console. 2.8.13. Provides insights into the organization’s security posture using an Executive level dashboard. Must be able to show the company’s overall risk score, individual asset risks, a view of ongoing attacks and their contributing risk factors. 2.8.14. Highly customizable dashboard that provides widgets displaying statistics from Attack Surface, Endpoint, and XDR. 2.8.15. Solution should be able to display MITRE ATT&CK Mapping for tactics and techniques detected in the organization for the following MITRE ATT&CK matrices. 2.8.16. The solution should be able to produce manual and scheduled reports that can be customized to display company information and logo. Generated reports should at least support PDF/PPT format and can be sent to specified email recipients. 2.8.17. The solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets. 2.8.18. The solution should provide 30 days included standard of data retention period 2.8.19. The solution should provide an option to extend the retention of data for up to 365 days. 2.8.20. The solution should be cloud-delivered service with an option to deploy and manage within a private cloud. 2.9. API and Third-party Integration Requirements 2.9.1. The solution must be able to integrate with common security information and event management (SIEM) and security orchestration, automation, and response (SOAR) products. 2.9.2. The solution should provide connectors ready to integrate with supported third-party security solutions. 2.9.3. The solution should also have the capability to					

integrate with other third-party solutions via application programming interface (API)

2.9.4. The solution should be able to generate API keys utilizing role- based access control for more granular permissions. API keys should have the option to expire and disabled from the management console.

2.9.5. The solution should be able to integrate with third party identity provider (IdP) solutions for single sign-on.

2.9.6. Solution should be able to integrate with at least one third party solution in the following category.

2.9.6.1. Breach Assessment and Simulation

2.9.6.2. Cloud Services

2.9.6.3. Firewall and Network

2.9.6.3.1. IT service management (ITSM)

2.9.6.3.2. security information and event management (SIEM)

2.9.6.3.3. (security orchestration, automation and response (SOAR)

2.9.6.3.4. Threat Intel

2.9.6.3.5. Unified endpoint management (UEM)

2.9.6.3.1. Vulnerability Management

2.10. Attack Surface Management

2.10.1. The solution provides continuous risk analysis of devices, identities, content, and applications. This includes active risks such as:

• Suspicious or anomalous user activity

• Indicators of attack (IoA), behaviors, or detections

• Potential risks such as vulnerabilities, exposed identities, or risky cloud app access

2.10.2. The solution shall provide a deep insight into the risk and health level, pulled from endpoint to uncover hidden risks.

2.10.3. The proposed solution shall uncover undiscovered risks and vulnerabilities, and gain insight into what needs immediate attention. Admin may view risks by user, device, and application, or at the organization level

2.10.4. The solution must show security posture, whether it is improving or declining, and gain visibility into how it compares to peers in the industry, region, or organization size.

2.10.5. The solution must be directly integrated into the XDR platform for simpler management and visibility

2.10.6. The solution must incorporate health scores into access control solutions and make more informed automated decisions when following a zero-trust strategy

2.11. Licenses

2.11.1. At least 167 licenses for end-users' Windows and MacOS laptops security

2.11.2. At least ten (10) licenses for server security

2.11.3. At least 177 licenses for attack surface management, covering each laptop and server protected by the licenses specified in sections 2.12.1 and 2.13.2)

2.11.4. Twelve (12) months license subscription

2.12. Includes initial configuration of the administration console

2.13. With knowledge transfer for at least three (3)

	DOST-ASTI personnel as administrators 3. TECHNICAL SUPPORT SERVICE 3.1. Technical support should be available at least eight (8) hours from Monday to Friday and has the following response times: 3.1.1. Critical Severity: Within one (1) business hour 3.1.1. Issues where the service components are rendered inoperable 3.1.2. Critical impact to business operations 3.1.3. No workaround available 3.1.2. High Severity: Within four (4) business hours 3.1.2.1. The software performance or service operation components severely impaired or degraded 3.1.2.2. Significant impact to business operations 3.1.3. Medium Severity: Within one (1) business day 3.1.3.1. Software or service function impaired but operational 3.1.3.2. Minor Trend Micro product or service component function not working as documented 3.1.3.3. Medium to low business impact 3.1.3.4. Workaround available. 3.1.4. Low Severity: Within two (2) business days 3.1.4.1. Request for enhancement 3.1.4.2. Little or no business impact 3.1.4.3. No immediate resolution required 3.1.4.4. Request for general information or questions. 3.2. End-user must be able to request technical support by phone, email, or through a website. 3.3. With readily accessible documentation and/or instruction manuals. 4. DELIVERY and PAYMENT TERMS 4.1. Price must be inclusive of government taxes and all applicable fees. 4.2. Delivery and activation of the licenses and conduct of knowledge transfer shall be made by the supplier before October 31, 2024. 4.3. Full payment will only be processed once the items are completely delivered, inspected, and accepted by the end-user.				
3	**PROCUREMENT OF SOFTWARE LICENSE SUBSCRIPTION TO PDF EDITOR** 1. GENERAL OVERVIEW 1.1. DOST-ASTI is seeking qualified and competent bidders for the Supply and Delivery of Ten (10) Licenses of PDF Editor. The contract's duration shall be for twelve (12) months. 1.2. The ABC is inclusive of all applicable government taxes and service charges. 2. TECHNICAL SPECIFICATIONS 2.1. Total of 10 Foxit PDF editor licenses which comprise of: 2.1.1. Renewal of DOST-ASTI's five (5) existing licenses 2.1.2. Purchase of additional five (5) licenses 2.2. Subscription period is 12 months 2.3. Edit and modify PDF contents 2.4. Export PDF content 2.5. Standard and XFA form filling	10	lic.	12889.40	128,894.00

	2.6. OCR text recognition 2.7. Scan documents directly to PDF file 2.8. Edit scanned documents 2.9. Compare PDF documents 2.10. Design and deploy electronic forms 2.11. Content management system integration 2.12. RPA-ready PDF editor 2.13. Secure PDF documents 2.14. Sign PDF documents 2.15. With accessibility features for people with disabilities 2.16. Cloud-based PDF editor 2.17. For Windows users (32-bit & 64 bit) 3. TECHNICAL SUPPORT SERVICE 3.1. Technical support should be available at least eight (8) hours from Monday to Friday and has the following response times: 3.1.1. Critical Severity: Within one (1) business hour 3.1.1. Issues where the service components are rendered inoperable 3.1.2. Critical impact to business operations 3.1.3. No workaround available 3.1.2. High Severity: Within four (4) business hours 3.1.2.1. The software performance or service operation components severely impaired or degraded 3.1.2.2. Significant impact to business operations 3.1.3. Medium Severity: Within one (1) business day 3.1.3.1. Software or service function impaired but operational 3.1.3.2. Minor Trend Micro product or service component function not working as documented 3.1.3.3. Medium to low business impact 3.1.3.4. Workaround available. 3.1.4. Low Severity: Within two (2) business days 3.1.4.1. Request for enhancement 3.1.4.2. Little or no business impact 3.1.4.3. No immediate resolution required 3.1.4.4. Request for general information or questions. 3.2. End-user must be able to request technical support by phone, email, or through a website. 3.3. With readily accessible documentation and/or instruction manuals. 4. DELIVERY and PAYMENT TERMS 4.1. Price must be inclusive of government taxes and all applicable fees. 4.2. Subscription period should be activated before the existing subscriptions expire in October 2024. 4.3. Full payment will only be processed once the items are completely delivered, inspected, and accepted by the end-user.				
4	**PROCUREMENT OF SOFTWARE LICENSE SUBSCRIPTION TO CLOUD PLATFORM** 1. GENERAL OVERVIEW 1.1. DOST-ASTI is seeking qualified and competent bidders for the Supply and Delivery of One (1) Lot of Cloud Platform. The contract's duration shall be for twelve (12) months. 1.2. The ABC is inclusive of all applicable government taxes and service charges. 2. TECHNICAL SPECIFICATIONS	1	lot	693221.80	693,221.80

	2.1. Four (4) virtual machines with the following specifications: 2.1.1. RAM: At least 8 GB 2.1.2. CPU: At least 4 Cores 2.1.3. VM Class: Regular 2.1.4. Operating System / Software: Free (Preferably CentOS) 2.1.5. Three (3) VMs have assigned static public IP addresses 2.1.6. Accompanying Persistent Disk: 100GB 2.1.7. Region: Singapore 2.2. Cloud VPN 2.2.1. 3 Tunnels; 730 tunnel hours per month 2.2.2. Can be used by unlimited users 2.3. Will serve as off-site redundancy of critical ASTI information System 2.4. Subscription period is twelve (12) months 3. TECHNICAL SUPPORT SERVICE 3.1. Technical support should be available at least eight (8) hours from Monday to Friday and has the following response times: 3.1.1. Critical Severity: Within one (1) business hour 3.1.1. Issues where the service components are rendered inoperable 3.1.2. Critical impact to business operations 3.1.3. No workaround available 3.1.2. High Severity: Within four (4) business hours 3.1.2.1. The software performance or service operation components severely impaired or degraded 3.1.2.2. Significant impact to business operations 3.1.3. Medium Severity: Within one (1) business day 3.1.3.1. Software or service function impaired but operational 3.1.3.2. Minor Trend Micro product or service component function not working as documented 3.1.3.3. Medium to low business impact 3.1.3.4. Workaround available. 3.1.4. Low Severity: Within two (2) business days 3.1.4.1. Request for enhancement 3.1.4.2. Little or no business impact 3.1.4.3. No immediate resolution required 3.1.4.4. Request for general information or questions. 3.2. End-user must be able to request technical support by phone, email, or through a website. 3.3. With readily accessible documentation and/or instruction manuals. 4. DELIVERY and PAYMENT TERMS 4.1. Price must be inclusive of government taxes and all applicable fees. 4.2. Delivery will be made within thirty (30) working days following receipt of NTP or PO. 4.3. Full payment will only be processed once the items are completely delivered, inspected, and accepted by the end-user.				
5	**PROCUREMENT OF SOFTWARE LICENSE SUBSCRIPTION TO ONLINE LATEX EDITOR** 1. GENERAL OVERVIEW 1.1. DOST-ASTI is seeking qualified and competent bidders for the subscription to Online Latex Editor, to be used for generating documents, including scientific	10	lic.	20000.00	200,000.00

	and technical papers for publication, and other high-quality project-related materials under the project. 1.2. The ABC includes all applicable government taxes and services charges. 2. TECHNICAL SPECIFICATIONS 2.1. Number of Licenses: Ten (10) licenses 2.2. Duration: 12 months 2.3. Maximum Collaborators per Project: User + Ten (10) 2.4. Can compile timeout and servers 2.5. Equipped with real-time track changes 2.6. With full document history 2.7. With advanced reference search 2.8. Has git integration 3. FEATURES 3.1. Editor and real-time collaboration 3.2. Thousands of templates 3.3. Symbol palette 3.4. GitHub integration 3.5. Dropbox integration 3.6. Mendeley integration 3.7. Zotero integration 3.8. Priority support 4. WARRANTY SERVICE 4.1. Access to software features, support, version upgrades, new releases, bugfixes and critical security patches must be made available for one (1) year from the date of user acceptance. 5. DELIVERY AND PAYMENT TERMS 5.1. The winning bidder is required to deliver the subscription within ten (10) calendar days upon issuance of NTP. 6. NOTES 6.1. Charging: ASTI GAA/ IT Support				
TOTAL APPROVED BUDGET FOR THE CONTRACT (ABC):					**Php 2,021,557.40**

RESERVATION CLAUSE

The Advanced Science and Technology Institute reserves the right to accept or reject any proposal, to annul the bidding process, and to reject all proposals at any time prior to contract award, without thereby incurring any liability to the affected proponent or proponents.