



TECHNICAL SPECIFICATIONS

SUPPLY, DELIVERY, INSTALLATION, AND CONFIGURATION/TESTING OF VARIOUS ICT SOFTWARE SUBSCRIPTION UNDER THE DIGITAL AGRICULTURE PROJECT (SUB-PROJECT: ENHANCED FARM-TO-MARKET ROAD (FMR) AND AGRI-COMMODITY GEODATABASE)

A. RATIONALE

The Agricultural and Biosystems Engineering Management Information System (ABEMIS) and the Geographic Information System for Agricultural and Fisheries Machinery and Infrastructure (GEOAGRI) has been adopted as the planning and implementation tool of the Department in terms of infrastructure and mechanization interventions. As supplementary to their features and requirements, the following systems are necessary:

- **Cyber Security Subscription - Cyber Security Subscription** - With the increasing volume and sophistication of cyber threats, organizations, and government agencies must take measures to protect themselves. This includes securing endpoints such as workstations and servers.

In line with the Department of Information and Communication Technology (DICT) recommendation on cyber protection, the endpoint protection platform is one of its underlying security fundamentals. This endpoint protection platform is designed to enhance BAFE's services by providing additional safeguards on an endpoint level. Its primary goal is to provide an additional layer of defense to improve the overall security posture of critical government information.

Recognizing the importance of endpoint security, the Bureau has decided to strengthen its defenses further. This strategic move will empower the agency to exercise greater control over the security of its user nodes and effectively block threats and unauthorized access attempts. This will benefit the Bureau with enhanced protection, streamlined incident response, and improved coordination in managing cybersecurity incidents. This project aligns with the BAFE's commitment to government regulatory compliance, including adherence to the Data Privacy Act and the Cybercrime Prevention Act.

B. SCOPE OF WORK



The following scope of work shall be delivered by the supplier:

ITEM/DESCRIPTION	SCOPE OF WORK
<p>1. Cyber Security Subscription</p>	<p>Warranty shall provide 24x7 managed detection and response services to its server farms for at least Three (3) Years.</p> <p>The manufacturer shall send endpoint security reports monthly to ensure the safety of server farms based on organizational security policies.</p> <p>The winning bidder will also include training, configuration, as well as on-site maintenance</p>

C. APPROVED BUDGET FOR THE CONTRACT

The ABC is **Five Million One Hundred Ninety-One Thousand Pesos Only** (Php 5,191,000.00) aggregate by lot. The aggregate and total ABC is inclusive of all applicable government taxes and charges, professional fees, and other costs.

D. TECHNICAL SPECIFICATIONS

PARTICULAR AND TECHNICAL SPECIFICATIONS	QUANTITY	UNIT COST (in PH Pesos)	TOTAL AMOUNT
<p>Cyber Security Subscription (3 years)</p> <ul style="list-style-type: none"> The solution and service must be provided to at least 200 endpoints. The solution could provide both a local and cloud management platform. The solution should support collecting endpoint information of operating systems, service ports, users, applications, database applications, websites, web frameworks, web services, and web applications to help you learn the status of your server assets and improve asset management efficiency. 	1	4,000,000.00	4,000,000.00



PARTICULAR AND TECHNICAL SPECIFICATIONS	QUANTITY	UNIT COST (in PH Pesos)	TOTAL AMOUNT
<ul style="list-style-type: none">• The solution should support P2P installation and upgrade, an endpoint with the agent deployed or upgraded can distribute resource packages to other endpoints in the subnet for agent deployment and upgrade, significantly improving the efficiency of deploying and upgrading the agent on endpoints.• The solution must protect end-of-support systems including Windows XP, Windows 7, Windows Server 2003, Windows Server 2008, and Linux.• The solution should have Artificial Intelligence capabilities that allow the identification and blocking of previously unknown malware based on malware family classification.• The solution should provide a forced scan channel for stubborn viruses.• The solution should have application control that prevents applications from performing actions that may be dangerous for the system.• The solution should provide a secondary authentication capability for RDP (Remote Desktop Protocol) sessions.• The solution should have real-time ransomware protection to detect and block encryption of endpoints and shared folders.• The solution should support a honeypot to detect ransomware.• The solution should provide a visual representation of allowed/unauthorized/suspicious communications between endpoint and other network and internet devices.• The solution should support blocking of specific applications or alerting			





PARTICULAR AND TECHNICAL SPECIFICATIONS	QUANTITY	UNIT COST (in PH Pesos)	TOTAL AMOUNT
when specified applications are executed on the endpoints. The list of applications should be configurable by the administrator. <ul style="list-style-type: none">• The solution should provide anti-brute force for SMB, and RDP sessions.• The solution should support endpoint CPU restriction to make scanning more lightweight, which can reduce performance impacts on legacy systems, virtual desktops, and overloaded systems.• The solution should have capabilities to allow administrators to mitigate infections and attacks across multiple targets with minimal effort from the management console.• The solution should provide full visibility into an attack event via the process chain.			
		TOTAL	4,000,000.00

E. INSPECTION AND TEST PROCEDURE

- a) The Inspector and/or Supply Officer can reject any software or part thereof that fails to pass any installation, test, and/or inspection or does not conform to the technical specifications.
- b) The Inspector and/or Supply Officer will issue an Inspection and Acceptance Report (IAR) upon determining that the installed computer software is usable and in good working condition.

F. PRODUCTION AND/OR DELIVERY SCHEDULE

Goods and services shall be delivered within sixty (60) calendar days from the receipt of the Notice to Proceed (NTP). The delivery and installation date must fall within weekdays from Monday to Friday only and shall be delivered at the BAFE Office, Sugar Center Compound, Annex II Building Extension, North Avenue, Diliman, Quezon City.



G. BIDDERS ADDITIONAL REQUIREMENTS

To ensure the quality of the products offered and assurance for immediate and competent after-sales technical support:

1. The prospective bidder must submit the following:
 - a. Manufacturer (Principal) certification stating that the bidder is an authorized partner or reseller of the product offered for the endpoint Security.
 - b. Prospective bidder to submit proof of at least one (1) similar project implementation for the Years 2019-2024 on Cyber security
Note: The bidder shall submit the following documents: A copy of the Contract, PO, and Certificate of Acceptance as proof of similar project implementation
 - c. The Manufacture must have Satisfaction Performance from previous clients either from Government or Private sector (must submit copy of certifications)
 - d. Must submit a Manufacturer's Authorization Form (MAF) from the Manufacturer, indicating the project title and the product offered.
Note: Certified certifications will form part of the eligibility documents.

G. AFTER-SALES SERVICES

ITEM/DESCRIPTION	AFTER-SALES SERVICES
<p>Cyber Security Subscription</p>	<p>The winning bidder shall provide One (1) Day of Hybrid, Online, or Face to Face Knowledge Transfer session on endpoint security, involving at least Five (5) personnel responsible for managing the data center.</p> <p>For Warranty Requirements, the Winning Bidder shall service render for at least 8 x 5 Technical support On-Site or Off-Site (Remotely) for the First Layer Support.</p> <p>The Manufacturer must have a local office and direct local support in the Philippines to offer 8 x 5 support either remotely or on-site as needed.</p> <p>The Manufacturer must have the capability to provide incident response in case ransomware attacks happen within the installed endpoints.</p>

H. PAYMENT TERMS AND CONDITIONS





One-time payment shall be made upon completion of the Supply, Delivery, Installation, Configuration/Testing, and Acceptance of Various ICT Software Subscriptions to submission of the following documents:

- a. Certificate of Warranty for all equipment; and
- b. Sales Invoice/Delivery Receipt.

I. MODE OF PROCUREMENT / AWARDING

The supply, delivery, installation, and configuration of various ICT software subscriptions will be procured through Public Bidding. The awarding of this project shall be done by lot.

J. LIQUIDATED DAMAGES

Liquidated damages are equivalent to one-tenth of one percent (0.1%) of the value of the goods and services not delivered within the prescribed delivery period shall be imposed per day of the delay. The DA-BAFE shall rescind the contract once the cumulative amount of liquidated damages reaches 10 percent (10%) of the amount of the contract, without prejudice to other courses of action and remedies open to it.

Prepared by:

JULIUS ABE S. PERALTA

Permanent Procurement Coordinator, Interim PKMDD

Noted by:

ENGR. ARNEL L. TENORIO, EnP.

Interim Division Chief, PKMDD