Bid Bulletin No. 2

"Supply and Delivery of Various ICT Equipment and License Software for the Department of Trade and Industry"
Bidding No. 21-050

December 3, 2021

This Bid Bulletin No. 2 is hereby issued to modify or amend the Bidding Documents.

Section I: Invitation to Bid

Lot No.	Item No.	Description	Approved Budget of the Contract (ABC)
1	1	Executive Laptop (76 units)	PhP6,030,600.00
	2	Laptop Computer – HIGH END (25 units)	PhP2,500,000.00
	3	Desktop Computer – High End (14 units)	PhP1,400,000.00
	4	Desktop Computer – Midrange (20 units)	PhP1,600,000.00
2	1	Internet Kiosk (Self Serving Nook) (16 units)	PhP4,800,000.00
3	1	Digital Single-Lens Reflex (DSLR) Camera (2 units)	PhP75,998.00
	2	Camera Lens (2 units)	PhP66,000.00
	3	Camera Battery (2 units)	PhP3,000.00
	4	Stabilizer (1 unit)	PhP36,500.00
	5	Camera Tripod (1 unit)	PhP2,500.00
	6	Microphone (2 units)	PhP8,236.00
4	1	Interactive Touch Screen Display (4 units)	PhP1,040,000.00
	2	Conference Wireless Speakerphone - External Quantity: Fifteen (15) units	PhP50,000.00
	3	Video Conference Camera (5 units)	PhP50,000.00
5	1	Floor Standing HD Digital Signage with touch function (6 units)	PhP1,020,000.00
6	1	Queue Management System (1 unit)	PhP300,000.00
7	1	License Software	PhP3,900,000.00

G/F Trade and Industry Bldg., 361 Sen. Gil Puyat Avenue, Makati City, 1200 Philippines
☎ 791-3363/3367 🖷 895-3515
www.dti.gov.ph BACSecretariat@dti.gov.ph

Section VI: Schedule of Requirements

Item Number	Description	Quantity	Delivered, Weeks/Months
1	**License Software**	1 lot	2 Years and 5 Months (Prorated: April 18, 2024)

Section VII: Technical Specifications

LOT 1

1. Executive Laptop (76 units)

Warranty:
1/1/1 standard one year onsite, next business day, one-year parts and labor

2. Laptop Computer – HIGH END (25 units)

Warranty:
3/3/3 Standard three year onsite, next business day, three-year parts and labor

3. Desktop Computer – HIGH END (14 units)

Processor: Core i9-10900
Chipset: latest Generation
L3 Cache Minimum: 20M
Memory Installed: Atlease 32GB, 2933MHz DDR4
At least Two (2) Memory slot
Storage Minimum: SSD 512GB + HDD 1TB SATA
Optical Drive:
SATA DVD R/W, Dual layer (same brand as the computer unit)
Display/Monitor (Minimum)
27” LED Full HD
Resolution (1920 x 1080
Graphics/Video: Intel dedicated, 4GB or higher
Connectivity: Wireless Network Wifi 6 2x2 AX

Warranty:
3/3/3 Standard three year onsite, next business day, three-year parts and labor

4. Desktop Computer – MIDRANGE (20 units)

Warranty:
3/3/3 Standard three year onsite, next business day, three-year parts and labor

LOT 3

Camera Lens (2 units)

*Zoom lens 18-105mm minimum

Camera Battery (2 units)

Any battery compatible with the camera

Microphone (2 units)

*1.00g minimum
*1200mm minimum
*Sensitivity: -33.5dB re 1 minimum
*Volt/Pascal (21.00mV @ 94 dB SPL) +/- 2 dB @ 1kHz
*with artificial fur and pop filter

LOT 7

1. License Software (1000 license)

(Must be compatible with existing license of DTI - BitDefender)

4.0 PROJECT DESCRIPTION/RATIONALE:

Security is one of the most critical components in the IT infrastructure of every company or enterprise organization. Securing corporate network requires continuous, layered protection against viruses, spyware, spam, phishing, and inappropriate Internet web content. To provide protection against these threats, the Department in 2020 renewed the Bitdefender Endpoint Security Solution which covers the DTI offices at the Main Office (Head Office), DTI International Trade Group (DTI-ITG), DTI Fair Trade Enforcement Bureau (FTEB), Regional Offices (DTI-RO), Provincial Offices (DTI-PO), Office of the Secretary (OSEC), and other satellite offices of DTI.

However, to ensure continuous protection for the newly purchased computers against threats and not to compromise security, there is an urgent need to purchase additional licenses for the enterprise endpoint security solution that could keep up with the thousands of faster, more insidious content security attacks released every day, such as data-stealing malware, ransom wares, botnet infections, and other blended threats.

As part of the implementation requirement, the Department will employ the use of End Point Protection Platforms (EPP) to provide an enterprise security that will protect PCs, mobile devices and server environments from malware, spyware, rootkits, Trojans and worms. The platform will include technologies such as: Signature based,

malware/spyware detection and removal, Anti-malware protection, vulnerability protection, personal firewall, ransomware protection, exploit-based attack prevention, real-time protection/monitoring, application whitelisting, device control, malicious website blocking, Data Loss Prevention/Intrusion Prevention System (DLP/IPS), data protection (e.g. file encryption), file reputation systems, security management and reporting.

Likewise, coverage of the deployment of this project will expand to other DTI Satellite Offices including the Regional and Provincial Offices. It is expected that through the delivery of this new Enterprise endpoint security solution, it will help eliminate infection, identity theft, data loss, network downtime, lost productivity, and compliance violations—reducing business risk and cost across all Office in the Department.

5.0 OBJECTIVE:

To provide an Enterprise endpoint security solution *(endpoint for desktop, server, mobile devices)* for DTI to continuously protect the Department's ICT infrastructure and its users against computer virus threats, vulnerabilities, and attacks.

5.0.1 ENDPOINT ANTI-VIRUS SOLUTION

DTI Office/Location	License
DTI-Main (includes Head Office, DTI-ITG, FTEB, DTI Offices in BOI, TARA Bldg, HAIPIN Bldg)	360
DTI-Regional Offices	640
Total	**1,000**

6.0 SCOPE OF WORK AND DELIVERABLES:

Supply, delivery, design, testing and maintenance of an Enterprise endpoint security solution for the following DTI sites:

Summary of Cloud Enterprise Endpoint Security Requirements for DTI-MAIN (Makati area)	License
DTI Head-Office	160
DTI-ITG (EMB)	40
HAIPIN Bldg	40
DTI Offices at UPRC Bldg. (FTEB)	40
TARA	40

DTI Offices at BOI Bldg.	40
TOTAL	**360**

Summary of Cloud Enterprise Endpoint Security Requirements for Regional Offices	**License**
DTI-CAR (Cordillera Administrative Region)	40
DTI-Region 1 (Ilocos Region)	40
DTI-Region 2 (Cagayan Valley Region)	40
DTI-Region 3 (Central Luzon)	40
DTI-Region 4a (CALABARZON)	40
DTI-Region 4b (MIMAROPA)	40
DTI-Region 5 (Bicol Region)	40
DTI-Region 6 (Western Visayas)	40
DTI-Region 7 (Central Visayas)	40
DTI-Region 8 (Eastern Visayas)	40
DTI-Region 9 (Zamboanga Peninsula)	40
DTI-Region 10 (Northern Mindanao)	40
DTI-Region 11 (Southern Mindanao)	40
DTI-Region 12 (Central Mindanao)	40
DTI-Region (CARAGA)	40
DTI-NCR (National Capital Region)	40
TOTAL	**640**

6.1 The winning bidder shall provide the following Enterprise endpoint security solution Technical Requirements and Functionalities:

6.1.1 **ANTI-VIRUS SOLUTION**

Features and Functionalities	**Cloud Enterprise Endpoint Anti-virus**
• **Cloud Management -** Manage policies in a single, centralized console via Cloud.	✓

Features and Functionalities	Cloud Enterprise Endpoint Anti-virus
• **Type of Endpoint Protected** - Protection for Laptop and Desktop / Physical and Virtual Workstation and Servers	✓
PREVENTION MODULES	
• **Local and Cloud Machine Learning** - Predictive detection of unknown malware; Dynamic file analysis trained on billions of samples; Local machine learning trained on 80,000 malware features. Threat intelligence from over 500 million endpoints globally.	✓
• **Advanced Anti-**Exploit - Focuses on attack tools and techniques to detect both known and zero-day exploits that target popular software applications.	✓
• **Automatic Disinfection and Removal** - Automatically blocks confirmed threats through a set of predefined rules, including process termination, moving to quarantine or access blocking	✓
• **Fileless Attacks Defense** - Protects against attacks that attempt to write changes directly in memory.	✓
• **Network Attack Defense** - Protects against attacks that attempt to write changes directly in memory.	✓
• **HyperDetect™ (Tunable Machine Learning)** - Tunable machine learning layer, detects sophisticated threats. Blocks hacking tools, fileless attacks, zero-day malware.	✓
• **Sandbox Analyzer** - Sends suspicious files for detonation, analyzes and provides a verdict in real time. Detects zero-day & targeted attacks; Real time attack prevention with auto-submit; Analyzes once enterprise-wide block.	✓
• **DETECTION AND RESPONSE MODULES**	✓
• **Process Inspector** - Behavior-based real time detection; Monitors all processes running in the operating system and if the process is deemed malicious, will terminate it.	✓
• **Incident Visualization** - Easy to understand visual guides highlight critical attack paths, easing burdens on IT staff	✓
• **Root Cause Analysis** - Highlights the attack vector, the attack entry point, and how the attack originated. Helps	✓

Features and Functionalities	Cloud Enterprise Endpoint Anti-virus
pinpoint the origin node of attack, highlighted in the Incident page. The confidence score provides context for security events	
• **Anomaly Defense** - Baselines system resources to spotlight unusual behavior based on MITRE threat techniques and Bitdefender's own research.	✓
• **MITRE Event Tagging** - MITRE attack techniques and indicators of compromise provide up to the minute insight into named threats and other malware that may be involved	✓
HARDENING AND RISK ANALYTICS MODULES	
• **Endpoint Risk Analytics** - Assesses, prioritizes and hardens endpoint security misconfigurations and settings with an easy-to-understand prioritized list.	✓
• **Web Threat Protection** - Scans incoming web traffic, including SSL, HTTP and HTTPSs traffic, to prevent the download of malware to the endpoint. Automatically blocks phishing and fraudulent web pages. Displays search ratings signaling trusted and untrusted pages.	✓
• **Device Control** - Threats are often introduced into the company via removable devices. Choose which devices to allow to run and decide what will be blocked or scanned automatically.	✓
• **Application Control (Blacklisting)** - Enables full visibility and control of running applications by blacklisting unwanted software. Helps limit the risk of malicious code running undetected.	✓
• **Firewall - Fully-featured two-way firewall that controls applications' access to the network and to the Internet. Furthermore, the firewall can protect the system against port scans, restrict ICS and warn when new nodes join a Wi-Fi connection**	✓
COMPATIBLE PRODUCTS	
• **Security for Storage** - Machine learning-driven antimalware scanning for ICAP-compatible network-attached storage (NAS) and file-sharing systems	✓

Features and Functionalities	Cloud Enterprise Endpoint Anti-virus
• **Network Traffic Security Analytics** - Cloud threat intelligence, Machine Learning and behavior analytics applied to network traffic to detect advanced attacks early and enable effective threat hunting	✓
• **Advanced Threat Intelligence** - Collects data from sensors across the globe - correlate hundreds of thousands of Indicators of Compromise and turn data into actionable, real-time insights.	✓

6.2 The winning bidder shall carry out installation and configuration of Enterprise endpoint security solution Software to all servers, network computers, laptops and mobile devices and shall also perform the following identified activities:

6.2.1 Analyze and evaluate existing DTI ICT infrastructure and recommend security measures and policies based on industry best practices.

6.2.2 Design Enterprise endpoint security solution that will support existing DTI ICT infrastructure and resources.

6.2.3 Prepare and submit list of activities, timetable, initial configuration settings and policy templates for endpoint security, central management, access control, Internet gateway security, application and device control.

6.2.4 Set-up and configure Enterprise endpoint security solution Central Management and policies.

6.2.5 Assist DTI ISMS personnel in doing end-users' data files backup.

6.2.6 Remove previous installations of anti-virus software.

6.2.7 Pre-scan and repair end-user data files, Program Files, OS, and documents and settings.

6.2.8 Update server and desktop Operating System service pack and security patches.

6.2.9 Detect and remove virus, Trojans, rootkits, spyware, adware, backdoors, worms and other malicious files and codes prior to the installation of anti-virus software.

6.2.10 Install client/end-user anti-virus software.

6.2.11 Conduct intensive testing on the installed Enterprise endpoint security solution software for configuration and policy compliance, systems-performance impact, on-access and on-demand scanners performance, spam test, false positive testing, and end client penetration testing.

6.3 The winning bidder shall provide the following technical assistance to the Department:

6.3.1 24/7 Helpdesk Technical Support Service (Telephone/Email/IM) for an Enterprise endpoint security solution on operational/functional problems and other virus-related issues that has minimal impact to DTI operations.

6.3.2 Conduct on-site technical support with response time of two (2) hours upon confirmation of call during critical problems such as virus outbreak and Enterprise Anti-virus server downtime that has major impact to DTI operations.

6.3.3 Conduct Monthly on-site maintenance for system health check, configuration and policy fine tuning, configuration backup, and log file analysis.

6.3.4 Submit comprehensive quarterly report on system health check results (based on usage, % utilization, and system capacity), configuration and policy fine tuning changes, log file analysis.

6.3.5 Deploy in-house personnel in DTI Head-Office to provide (A) daily monitoring and maintenance of Anti-Virus System, (B) weekly & monthly report of Anti-Virus System endpoint update status, phishing activity, data protection status, protection status, malware status, license usage, AV update status, and AV upgrade status.

6.4 The winning bidder shall conduct one-time in-depth technical trainings for Ten (10) DTI IT personnel regarding the installation, configuration, administration and maintenance on “Enterprise endpoint security solution” to be handled by designated product expert/s.

6.5 The winning bidder shall conduct annual Information Security Awareness and Virus Protection Seminars for DTI employees for (3) three years. *(DTI will provide venue and meal/snacks for the participants).*

6.6 The winning bidder shall submit in hard and soft copies detailed project documentation of the following:

- Project Implementation Plan
- Enterprise endpoint security solution Security Plan and Policy Manual
- Configuration Management Manual
- Systems Administrator’s Manual
- End-user Manual
- End-user client anti-virus installation procedures (for cloud, network and standalone clients)
- Incident and problem escalation procedure applicable for DTI-head offices and Regional Office (includes List of Technical Support Engineers, Disaster Recovery Plan for Enterprise Anti-Virus System, Security Breach Incidents, AV Outbreak)
- SLA (Service Level Agreement) and NDA (Non-Disclosure Agreement)

Activity	Schedule
Submission and Opening of Technical and Financial Bids	December 13, 2021, 9:00 AM for Submission and 9:30 AM for Opening of Technical and Financial Documents through video conference with the following details: Zoom Meeting: **https://zoom.us/j/97941148385?pwd=OCs1bFNvM3dpZFM2QzZPZlJhaEpnZz09** Meeting ID: 979 4114 8385 Passcode: 499376

For the guidance and information of all concerned.

MARY JEAN T. PACHECO
Assistant Secretary
Chairperson, DTI Bids and Awards Committee