Bid Bulletin No. 1

"Supply, Delivery, Design, Testing and Maintenance of a Cloud-based Enterprise Endpoint Security Solution"
20-021

November 10, 2020

This Bid Bulletin No. 1 is hereby issued to modify or amend the Bidding Documents.

Section VII. Technical Specifications

1. **OBJECTIVE:**
To provide a Cloud-based 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.

1.1. ENDPOINT ANTI-VIRUS SOLUTION

DTI Office/Location	License
DTI-Main (includes Head Office, DTI-ITG, FTEB, DTI Offices in BOI, TARA Bldg, HAIPIN Bldg.)	900
DTI-Regional Offices	1600
Total	**2,500**

2. **SCOPE OF WORK AND DELIVERABLES:**

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

Summary of Cloud-Based Enterprise Endpoint Security Solution Requirements for DTI-MAIN (Makati area)	License
DTI Head-Office	500
DTI-ITG (EMB)	100
HAIPIN Bldg	100
DTI Offices at UPRC Bldg. (FTEB)	100
TARA	50
DTI Offices at BOI Bldg.	50
Total	**900**

BIDS AND AWARDS COMMITTEE

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

Summary of Cloud-Based Enterprise Endpoint Security Solution Requirements for Regional Offices	License
DTI-CAR (Cordillera Administrative Region)	100
DTI-Region 1 (Ilocos Region)	100
DTI-Region 2 (Cagayan Valley Region)	100
DTI-Region 3 (Central Luzon)	100
DTI-Region 4a (CALABARZON)	100
DTI-Region 4b (MIMAROPA)	100
DTI-Region 5 (Bicol Region)	100
DTI-Region 6 (Western Visayas)	100
DTI-Region 7 (Central Visayas)	100
DTI-Region 8 (Eastern Visayas)	100
DTI-Region 9 (Zamboanga Peninsula)	100
DTI-Region 10 (Northern Mindanao)	100
DTI-Region 11 (Southern Mindanao)	100
DTI-Region 12 (Central Mindanao)	100
DTI-Region (CARAGA)	100
DTI-NCR (National Capital Region)	100
Total	**1,600**

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

3.1. **Features and Functionalities**

Features and Functionalities
• **Cloud Management** - Manage policies in a single, centralized console via Cloud.
• **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.

Features and Functionalities
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 and more
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 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**

Features and Functionalities
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
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.

3.2. The winning bidder shall carry out the, configuration, testing, training, installation of Enterprise endpoint security solution Software to all servers, network computers, laptops, mobile devices and installation of Anti-Virus end-point client to DTI-HO and Regional Offices must be **completed within 1 month upon to awarding of contract** and shall also perform the following identified activities:

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

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

3.2.3. 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.

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

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

3.2.6. Remove previous installations of anti-virus software.

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

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

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

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

3.2.11. 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.

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

3.3.1. 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.

3.3.2. 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.

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

3.3.4. Submit comprehensive monthly report on the following:

3.3.4.1. System health check results (based on usage, % utilization, and system capacity), configuration and policy fine tuning changes, log file analysis.

3.3.4.2. Anti-Virus System endpoint update status, phishing activity, data protection status, protection status, malware status, license usage, AV update status, and AV upgrade status.

3.4. 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.

3.5. 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).*

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

3.6.1.1. Project Implementation Plan

3.6.1.2. Enterprise endpoint security solution Security Plan and Policy Manual

3.6.1.3. Configuration Management Manual

3.6.1.4. Systems Administrator's Manual

3.6.1.5. End-user Manual

3.6.1.6. End-user client anti-virus installation procedures (for cloud, network and standalone clients)

3.6.1.7. 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)

3.6.1.8. SLA (Service Level Agreement) and NDA (Non-Disclosure Agreement)

4. The Supplier shall deliver, install, and configure the proposed equipment including all components at the DTI extension offices and branches within **thirty (30) calendar days** upon receipt of Notice to Proceed (NTP).
5. The years of contract license subscription for the 2,500 anti-virus solutions is **three (3) years.**
6. API keys will be used in SEIM integration.

For the guidance and information of all concerned.

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