

**TECHNICAL SPECIFICATIONS
(Terms of Reference)**

**PROCUREMENT OF ONE YEAR
LICENSE ENDPOINT SECURITY PROTECTION (433 Licenses)
January 1, 2025 – December 31, 2025**

BACKGROUND:

The National Electrification Administration (NEA) annually purchases anti-virus protection to keep the system secure by automatically blocking viruses, pop-ups, spam and other internet system threats. This year contract of NEA for Anti-Virus will expire on December 17, 2024 but extended until December 31, 2024. Thus, the new contract will commence on January 01, 2025.

With the internet becoming an increasingly bigger part of the business industry, the risk of a security breach or threat of a virus, rises. Endpoint security helps businesses keep the devices that connect to a network secure. Endpoint security antivirus scans devices for known malware signatures and suspicious behavior. It uses a combination of signature-based detection, behavioral analysis, and machine learning algorithms to identify and block threats in real time. Typically, endpoint security includes antivirus/anti-malware protection. Moreover, endpoint security extends beyond antivirus, including next-generation protection features like advanced persistent threat detection, investigation, and response, device management, data leak prevention, and others.

OBJECTIVE:

To procure 433 licenses of endpoint security/protection to be monitored via Cloud for the workstations and servers of NEA to safeguard against cyber security threats, ensure data integrity, and maintain uninterrupted business operations.

I. PROJECT DESCRIPTION

- Name of the Project : **Procurement of One Year License Endpoint Protection Upgrade (433 Licenses)**
- Location : **# 57 NEA Building, NIA Road, Government Center, Diliman, Quezon City**
- Approved Budget of the Contract : **Nine Hundred Eighty-Eight Thousand Seven Contract Hundred Fifty Pesos (P988,750.00) chargeable against Maintenance and Other Operating Expenses (MOOE) of CY2024**

II. DELIVERY SCHEDULE : The contract period is **one (1) year**, which shall commence on January 01, 2025.

III. TECHNICAL SPECIFICATIONS

A. FEATURE

Endpoint Protection

- Multi-Layered Anti-Malware
- Behavior detection
- Exploit Prevention
- Remediation Engine
- File threat protection
- Mail threat protection
- Web threat protection
- Firewall
- Host Intrusion Prevention
- Network threat protection
- BadUSB Attack prevention
- AMSI protection
- Security Network
- Security Network
- Adaptive Anomaly Control

Security Management

- Vulnerability assessment
- Patch management
- Encryption management
- Application control
- Web Control
- Device control
- Remote wipe

Cloud Monitoring

- Cloud Discovery - enables the discovery and restriction of inappropriate or unauthorized cloud resources usage, as well as the time wasted on social networks and messengers.

Cloud Security

- Cloud Blocking- block user access to inappropriate or unauthorized cloud resources, social networks or messengers.

Basic EDR Capabilities

- Root Cause Analysis - each new detect is opened and populated with automatically generated information after malicious/suspicious activity has

been detected on the endpoint.

Essential EDR Capabilities

- Threat intelligence Information
 - Reactive approach
 - Proactive approach
 - IoC Scan: scheduled scan
 - IoC export Response guidance
 - 'Single-click' response
- In the alert card several response actions are available as separate buttons:
- *Execution prevention*
 - *Host isolation*
 - *Quarantine file*
- Console response
 - Add to allow list
 - Get file
 - Delete file
 - Start process
 - Terminate process
 - Automatic cross-endpoint response - Threat indicators (IoC) for a specific alert or file found in the threat propagation graph can be automatically generated and an IoC scan can be launched based on this IoC.
 - Recover file from quarantine
 - Remove network isolation

Cybersecurity Trainings for IT

- Equal to number of administrators

Management:

- EXPERT VIEW: Cloud or On-premise management console.

License Type: Per User

- Number of desktop or server per license :1
- Number of mobile devices per license: 2
- Number of MS O365 mailboxes per license: 1.5

IV. QUALIFICATION OF SUPPLIERS

1. Should be an authorized local vendor in the Philippines of the offered products for at least 5 years.
2. Should have at least two (2) certified engineers for end-point solution
3. Supplier must be a Gold Partner with the and must submit a Manufacturer's Certificate of products and services offered.
4. Able to provide 3-Tier support (1st local, 2nd Distributor and 3rd Principal)

V. RESPONSIBILITIES OF THE WINNING SUPPLIER

1. The supplier shall supply NEA with an endpoint security software solution licenses for 433 NEA workstations on an annual subscription similar to the existing antivirus software of the National Electrification Administration.
2. The supplier shall conduct product training/assistance to at least three (3) NEA personnel in deployment, configuration, maintenance and troubleshooting of the software at NEA Building.
3. The supplier shall conduct the installation, configuration and testing of the software during deployment until all have successfully installed, configured and tested.
4. The supplier shall provide software upgrades, signature pattern and patches updates for a period of one (1) year.
5. The supplier shall provide a standard 8 hours a day, 5 working days a week technical support assistance (phone, email and web-remote assistance) with a 24/7 Helpdesk Center (through email and phone support) for a period of one (1) year for free.
6. Knowledge Transfer performed by a Certified Professional Engineer for the product delivered.
7. The winning supplier agrees to hold the Proprietary Information in strict confidence. Winning supplier, furthermore agrees not to reproduce, transcribe, or disclose the proprietary information to third parties without prior written approval of the National Electrification Administration.
8. To ensure the confidentiality of all information that will come to the knowledge of the winning supplier and its employees assigned therein, they shall uphold strict confidentiality of any information that has concern to the NEA, including but not limited to IT infrastructure design/ configuration, workflow process, building layout and design.

VI. RESPONSIBILITIES OF NEA

1. A NEA network administrator representative must be present to assist in the deployment.
2. Provide free access to all work areas to be affected by the project implementation service such as new licenses keys.

VII. SUBMITTALS

1. Certification from manufacturer that the local vendor is an authorized dealer/supplier of the offered products.
2. Name of two (2) engineers for the installation and configuration purposes.

3. Name of contact person to immediately attend on the issues and complaints of NEA

VIII. TERMS OF PAYMENT


Payment to the Supplier shall be on a One-Time basis upon submission of billing statement, Sales Invoice, Inspection and Acceptance Report issued by NEA, and other documentary requirements, if necessary.

IX. OTHER CONDITIONS/ PROVISIONS

It is understood that all other conditions/ provisions under R.A. no. 9184 and its Revised Implementing Rules and Regulations not herein specified shall be deemed incorporated into this Technical Specification with the same meaning as provided under the law.

INFORMATION TECHNOLOGY AND SYSTEMS DEVELOPMENT DIVISION

Prepared by:



CESAR F. JACINTO JR.
MIS Development Chief A

Reviewed by:



ANNABELLE P. CRUZ
Division Manager A



SHEILA ECHIVERRI-VILLANUEVA
Division Manager A

Noted by:



RODERICK N. PADUA
Department Manager, ITCS