REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF TRANSPORTATION
MARITIME INDUSTRY AUTHORITY

TECHNICAL SPECIFICATIONS

Project Description	SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF OFFSITE BACKUP
Approved Budget for the Contract	The supplier shall bid for all items described in this Technical Specifications, which shall not exceed the Approved Budget Contract (ABC) in the amount of Nine Million Five Hundred Pesos **₱9,500,000.00**, inclusive of all applicable government charges.
Specifications/ Deliverables *(Ex. Size, color, materials used and other specs requirements)*	

Unit	Quantity
1. Hyperconverged Server	1
2. Switch	1
3. Network Attached Storage	1
4. Firewall	1

I. HYPERCONVERGED SERVER

1. Hardware Specifications (Per Node - Min. 2 Nodes)

- Max 2U rack-mountable per cluster node.
- 2x x86-64 CPUs, min. 12 cores each, ≥ 2.4GHz base frequency (Intel Xeon Silver 4510 or better).
- 128 GB DDR5 ECC RAM (populated via min. 4x 32GB modules).
- Min. 2x 960GB Enterprise SSDs.
- Min. 4x 8TB Enterprise HDDs.
- Min. 4x 1GbE ports and 2x 10GbE SFP+ Multimode ports.
- Redundant, hot-swappable Power Supply Units (PSUs).

2. Software & Architecture Requirements

A. Core Platform Technology

- The solution must be a software-defined IT infrastructure that virtualizes all elements of conventional hardware systems. It must include, at a minimum, native compute virtualization (hypervisor) and storage virtualization (software-defined SAN).
- The platform must be natively capable and ready to support network virtualization, virtual network security (including Virtual Firewalls and Bandwidth Managers), and virtual Load Balancing.
- The cluster must start with a minimum of two (2) nodes and support direct horizontal scaling (adding nodes) without requiring a reinitialization, redeployment, or overhaul of the existing environment.
- The management platform must be integrated and distributed across the cluster, ensuring no reliance on a single virtual or physical machine to avoid a single point of failure (SPOF).
- The system must not require the installation of separate or external management software clients after deployment. Basic web-based GUI access, granular management, and operation must be natively accessible via a standard web browser.
- Must support correlated security services that integrate with an intelligent threat detection and response platform. The system must automatically trigger containment actions (such as

isolating/quarantining a VM via a distributed firewall or taking automated VM snapshots) upon detecting malicious activity.

B. Compute Virtualization (Hypervisor)

- Must support agentless or agent-based format conversion of major virtual disk types, including VMDK, VHD, VHDX, QCOW2, and QEMU.
- Native cluster HA must be supported. If a physical host fails, all affected VMs must automatically recover and restart on the remaining operational host(s) to guarantee business continuity.
- Must include native, agentless, incremental VM-level backup capabilities. For Windows-based VMs, file-level recovery must be natively supported without requiring third-party software or solutions.
- Must support scheduled snapshots and the creation of snapshot consistency groups.
- The platform must continuously evaluate VM performance and support the online adding (hot-add) of vCPU and vRAM resources without requiring virtual machine reboots or business downtime.
- The system must monitor host health parameters. Unhealthy hosts must automatically be moved to an isolated host list, preventing the scheduler from using them as HA failover or VM placement destinations. Once the host returns to a healthy state, it must automatically reintegrate into the active pool.

C. Storage Virtualization (Software-Defined SAN)

- Must support storage striping functions configurable at the individual virtual disk level.
- Storage rebuilds and data synchronization must automatically throttle IO speed to protect active business performance, ensuring reconstruction tasks do not consume excessive IO operations.
- Must include disk bad-sector prediction, scanning, and automated repair features to maximize data preservation.
- Must support storage capacity prediction algorithms based on historical consumption rates and resource utilization trends.
- Must support predictive remaining lifespan metrics for all individual physical disks.

D. Network Virtualization (SDN)

- Must natively support the deployment of virtual switches, virtual routers, and virtual firewalls within the hypervisor layer.
- Must feature a built-in distributed firewall capable of enforcing granular security access control policies on East-West traffic directly between virtual machines.
- Virtual routers must support high availability, automatically recovering routing services on a surviving host in the event of a host failure.
- The management interface must support a graphical drag-and-drop panel, allowing administrators to map, configure, and connect virtual network topologies visually.

3. Features and Functionalities of the Virtualization Platform:

Performance:

- Increase capacity by adding CPU, memory, or devices to VMs when needed without disruption or downtime.

- Load balancing across hosts.

Availability:

- Able to live-migrate virtual machine workloads from one host to another.
- Able to do array-agnostic replication of virtual machine data over LAN or WAN.
- Able to live-migrate virtual machine disks from one storage to another.
- Able to monitor Hardware and VM failures.

Recoverability:

- Back-up image-level virtual machines for ease of recoverability.
- Must support snapshots.
- Provide the function of the virtual machine recycle bin, manage the deleted virtual machine in a unified way, prevent the data loss caused by the false deletion of the virtual machine, support recycle bin file saving cycle configuration, and the overdue file will be automatically deleted.

Manageability:

- Discover and provide inventory of the whole virtualized environment through a single window.
- Convert, create, and deploy VMs.
- Provide screenshots of product functions.
- Support using a one-click mouse button to export cluster, host, and virtual machine configuration and status information in Excel and PDF format.
- Provide a product function screenshot
- Clone virtual machines and create templates.
- Support using a one-click mouse button to analyze the use of historical resources of the virtual machine and host and provide data support for planning and decision-making.
- Provide health monitoring, performance analytics, and capacity management through a single operations dashboard.

Security:

- Create virtual switches that have VLANs for network segregation.
- Leverage an agent-less anti-virus solution to offload AV processing from the virtual machines.
- Support user password complexity policy customization and password change cycle customization.

4. Backup Solution

a. Must have license to back up the total disk capacity of the HCI
b. Must be able to support major virtualization software
c. Must be able to scale out up to 32 nodes
d. Must support disk optimization

5. Vendor Eligibility & Industry Certifications

- The software platform vendor/principal must hold a CMMI Level 5 certification.
- The software vendor/principal must be recognized and listed in the Gartner Magic Quadrant for Hyperconverged Infrastructure.

II. SWITCH

- 26× 10G SFP+ slots and 6× 25G SFP28 slots
- Full L3 routing including RIP, OSPF, ECMP, & VRRP
- Switch capacity : 820 Gbps
- Packet forwarding rate : 610.1 Mpps

III. NETWORK ATTACHED STORAGE

1. Core Hardware & Compute

- Form Factor: 2U Rackmount
- Processor: AMD Ryzen™ 7 7000 series 8-core/16-thread processor, burst up to 5.3 GHz / 64-bit x86
- Hardware Encryption: AES-NI
- System Memory: 32 GB UDIMM DDR5
- Maximum Memory: 192 GB (4 x 48 GB)

2. Drive Bay & Storage Architecture

- Drive Bays: Hot-swappable 200TB - 3.5-inch SATA 6Gb/s, 3Gb/s
- Drive Compatibility: 3.5-inch SATA hard disk drives/2.5-inch SATA solid state drives
- M.2 Slot: 2D x M.2 2280 PCIe Gen5 - 8TB
- Storage: 200TB HDD (7 X 30TB HDD / 10 x 20TB)

3. Advanced Networking & Expansion

- 2 x 2.5 Gigabit Ethernet Port (2.5G/1G/100M)
- 2 x 10GBASE-T (10G/5G/2.5G/1G/100M)

4. Power & Reliability Specs

- Power Supply Unit 550W(x2), 100-240V
- System fan: 3 x 60mm, 12VDC

5. Warranty and Support

- Three (3) Years Warranty & Next-Business-Day Support

IV. FIREWALL

- Must have 10Gbps Firewall Throughput
- Must have 1.2Gbps NGFW throughput
- Must have 600Mbps IPSec throughput
- Must have at least 128GB SSD storage
- Must have 800,000 Maximum Concurrent Sessions
- The proposed solution must support: (1) IPS (2) Botnet Protection (3) Anti-Virus (4) Anti-DoS (5) Anti-Brute force
- The proposed solution supports over 13000+ IPS signature entries built-in entries on-premise
- The proposed solution should be able to detect the virus inside compressed files, up to 16 layers of compression.
- The proposed solution must support a dedicated Ransomware protection module:
- (1) Present ransomware threats in the dedicated dashboard, including vulnerable devices, risk open ports, weak passwords, and ransomware infections.
- (2) Provide recommendations for solving related security issues.
- (3) Generate ransomware protection policy automatically.

<table>
<tr>
<td></td>
<td>
extinguishing agent has been discharged
• Provision for Fire Exit
■ Raised Floor Specifications
• 61cm x 61cm (24" x 24") panels
• 750cm vertical clearance under-floor
• 1,200kg/sqm floor loading
■ Support
• 24 x 7 Helpdesk, phone and email support
• Remote Hands
• 24 x 7 site access to customer
■ Security
• 24 x 7 Physical Access Security
• Use of both swipe card and biometric authentication for access control
• Video surveillance cameras located in strategic areas of the building and its perimeter. Six (6) months video retention

Additional Component
<table>
<tr><th>Service</th><th>Qty</th></tr>
<tr><td>Copper Cross Connect</td><td>1</td></tr>
<tr><td>Leased Internet Line (per Mbps)</td><td>50</td></tr>
</table>
</td>
</tr>
<tr>
<td>Project Scope</td>
<td>
• Supply all hardware, software, licenses, and components required for a fully functional virtualized Disaster Recovery (DR) environment.
• Install, configure, test, and commission the virtualized infrastructure, including High Availability (HA) and DR capabilities.
• Migrate existing physical and virtual servers, applications, data, and Active Directory services with minimal downtime while preserving security and system integrity.
• Supply, deliver, install, and commission the HCI Server for the DR Site, complete with all required accessories, operating system, database software, and other necessary applications.
• Deliver all equipment free of charge and conduct on-site inspection, testing, and acceptance with MARINA representatives.
• Provide only genuine, fully licensed software and turn over all licenses, activation keys, and related documentation to MARINA upon project completion.
• Ensure all servers are delivered with the latest stable firmware, operating system updates, security patches, and service packs.
• Submit a comprehensive DR Plan and complete technical documentation, including architecture, configurations, network diagrams, asset inventory, software licenses, and Administrator/User Manuals.
• Provide technical assistance during installation, configuration, migration, deployment, and knowledge transfer to MARINA personnel.
• Provide preventive and corrective maintenance, including manufacturer support, for three (3) years from final acceptance, with a maximum response time of four (4) hours and next business day on-site support when required.
• Assign at least two (2) qualified technical personnel to provide on-site implementation, monitoring, and post-deployment support.
</td>
</tr>
</table>

<table>
<tr>
<td>Service Legal Agreement</td>
<td>
The winning bidder shall conform to the service level requirements, which shall include the following:

1. Service Support Escalation

The winning bidder shall provide MARINA with a Service Support Escalation List. Provide the contact details of the helpdesk and update MARINA regularly for any changes. This includes names, positions, email addresses, and telephone numbers.

2. Response Time

Service requests shall be acted immediately by the winning bidder according to the following response and expected resolution time.
<table>
<tr><th></th><th>Email Support</th><th>Phone Support Request</th><th>Onsite Support Request</th></tr>
<tr><td>Coverage</td><td>8 x 5</td><td>8 x 5</td><td>8 x 5</td></tr>
<tr><td>Response Time</td><td>Within 8 hours reply is expected</td><td>Within 15 minutes, a callback response is expected</td><td>With 2 to 3 hours onsite, an engineer is expected to arrive</td></tr>
<tr><td>Resolution Time</td><td>Within 48 hours</td><td colspan="2">Resolution of problems within the given period depending on the nature thereof:

Hardware replacement of malfunctioning parts depending on the availability of the spare parts

Software and Licenses – Within 8 hours</td></tr>
</table>
</td>
</tr>
<tr>
<td>Technical Support</td>
<td>
• The winning bidder shall establish a centralized Helpdesk or Service Desk with hotline and email support as the single point of contact for incidents, technical support, and service requests.
• The winning bidder shall provide technical support throughout the implementation, warranty, and maintenance periods, including system administration, troubleshooting, preventive and corrective maintenance, software updates, and technical consultation, at no additional cost to MARINA.
• The winning bidder shall provide qualified technical personnel for on-site diagnosis, repair, replacement, installation, testing, and corrective actions within the prescribed response and resolution times.
• All defective hardware shall be repaired or replaced with new or manufacturer-authorized equivalent parts, including all labor, materials, and installation costs, at no additional cost to MARINA.
• If equipment cannot be restored within the required resolution period, the winning bidder shall provide a temporary replacement unit of equivalent functionality until the original unit is repaired or replaced.
• Technical support shall be available via telephone, email, remote assistance, and on-site service during regular business hours (8:00 A.M.–5:00 P.M., excluding holidays), unless otherwise approved by MARINA.
• The winning bidder shall perform on-site diagnostics and testing and shoulder all costs related to technical personnel, transportation, tools,
</td>
</tr>
</table>

	equipment, and other expenses necessary to provide support and maintenance services.
Delivery Terms *(to be determined by the End-User)*	Thirty (30) Calendar Days upon Receipt of Notice to Proceed/Purchase Order.
Bidders Requirements	• The bidder must be a legally registered business entity authorized to provide ICT infrastructure solutions and must have operated continuously in the Philippines for at least ten (10) years. • The bidder must have completed, within the last five (5) years, at least one (1) similar contract involving enterprise backup, storage, disaster recovery, data protection, or related ICT infrastructure. • The bidder must have a PMI-certified Project Manager and submit the corresponding Certificate of Employment, Company ID, and SSS contribution. • The bidder must provide manufacturer authorization or partnership documentation and have at least two (2) manufacturer-certified technical engineers for implementation and support. • The bidder must maintain a local office or authorized service center in the Philippines capable of providing onsite and remote technical support, maintenance, warranty, and SLA-compliant services. • The bidder shall supply a complete, brand-new, genuine, and fully supported offsite backup solution, including all required hardware, software, licenses, accessories, and components. • The bidder shall provide installation, configuration, integration, testing, commissioning, documentation, knowledge transfer, and manufacturer support, including firmware, software updates, security patches, and warranty services.
Note: Prospective suppliers must comply with all of the above requirements to become eligible with the said procurement project.	

Prepared by:

DALMACIO L. GONZALES JR.
ITO III, ICTMD

Approved by:

SAMUEL L. BATALLA
Executive Director
STCW Office