REPUBLIC OF THE PHILIPPINES
PHILIPPINE STATISTICS AUTHORITY

Reference No: 2019-BAC01-123

04 December 2019

SUBJECT: Bid Bulletin No. 1

Dear Prospective Bidder:

This serves as the official transmittal of Bid Bulletin No. 1 for the Procurement of Supply, Delivery, Installation, Implementation, and Training of Various ICT Components for the Philippine Registry Office (PRO) and Information Technology and Dissemination Service (ITDS). This bulletin is being issued to amend the Bidding Documents and clarify queries from prospective bidders.

Please be informed that the contents of the Bidding Documents that have not been modified shall remain in full force and effect.

The bulletin shall be posted on both the PhilGEPS and PSA website.

Truly yours,

MINERVA ELOISA P. ESQUIVIAS
Vice-Chairperson, PSA Bids and Awards Committee

PSA Complex, East Avenue, Diliman, Quezon City, Philippines 1101
Telephone: (632) 938-5267
www.psa.gov.ph

PROCUREMENT OF SUPPLY, DELIVERY, INSTALLATION, IMPLEMENTATION AND TRAINING OF VARIOUS ICT COMPONENTS FOR THE PHILIPPINE REGISTRY OFFICE (PRO) AND INFORMATION TECHNOLOGY AND DISSEMINATION SERVICE (ITDS)

BID BULLETIN NO. 1

<table>
<tr><th>Bid Bulletin Ref. No.</th><th>Specific Page/Section in the Bidding Docs.</th><th>Query/Issue</th><th>Clarification/s</th></tr>
<tr><td>BB1-01</td><td>Invitation to Bid</td><td></td><td>The breakdown of the ABC for the procurement is as follows:
<table>
<tr><th>Description</th><th>Quantity</th><th>Total</th></tr>
<tr><td>Lot 1

Supply, Delivery, Installation, Implementation, and Training of ICT Components</td><td>1 lot</td><td>Php 100,000,000.00</td></tr>
<tr><td>Lot 2

ICT Components Computer and Laptop</td><td>1 lot</td><td>Php 7,207,878.08</td></tr>
<tr><td>Lot 3

Expansion of the existing storage of UCS Server for Data Center</td><td>1 lot</td><td>Php 3,200,000.00</td></tr>
</table></td></tr>
<tr><td>BB1-02</td><td>Bid Data Sheet (5.4)

On Similar contract for the</td><td>Will a contract on “Supply and Delivery” alone suffice and be qualified for</td><td>For the purposes of SLCC qualification, “Supply and Delivery of Various ICT” is accepted.</td></tr>
</table>

	"Supply, Delivery and Installation" for the procurement --SLCC	the SLCC? Or does the procuring entity apply strict comparison (meaning, it will only acknowledge contract with "Supply, Delivery and Installation")	
BB1-03	Schedule of Requirements Equipment should be delivered 45 days upon receipt of NTP	Extension of deliverable; from 45 days to 60 days	The 45 days shall be retained. This applies only to the delivery.
BB1-04	Section VII – Technical Specifications Hyperconverged Infrastructure	By "all components", does this pertain to all components of the same brand?	Yes. All components must be from a single brand/manufacturer for ease of support and integrated management.
BB1-05	Technical Specification On Branding	Majority of the specifications for each of the equipment points to a single brand, can the suppliers offer an equivalent alternative?	Yes. Refer to attached revised technical specification.
BB1-06	Section VII – Technical Specification Next Generation Firewall	Is it possible to propose alternative or removing certain features for the Next Generation Firewall?	Revisions will be reflected as to the specification; however, certain technology requirement will be retained as these pertain to cyber security concerns.

BB1-07	Section VII – Technical Specification Network Attached Storage (NAS)	Clarification on how many hard drives are installed on each NAS?	All 16 bay slots of the NAS will be installed with a 4TB hard drive.
BB1-08	Section VII – Technical Specification Endpoint Security	Additional Specifications /Requirement	The length of the license for the Endpoint Security will be for five (5) years.
BB1-09	Section VII – Technical Specification Endpoint Security	Where is the unified management server installed?	Unified management server will be installed at the PSA central office.
BB1-10	Section VII – Technical Specification Workstation Monitor	Clarification on what is meant by “latest generation”	Must have an Intel Core i7 Processor. Refer to revised Section VII – Technical Specifications.
BB1-11	Section VII – Technical Specification Biometric Locks	Clarification on biometric locks, will the device be used as an attendance biometric or a security biometric	The device will be used as a security biometric, Refer to revised Section VII – Technical Specifications.
BB1-12	Section VII – Technical Specification RJ 45	Is the RJ 45 for CAT 6 or can we offer CAT 5E? Also, the standard length for this is 305m / box as opposed to the 300m	The RJ45 will be used with CAT 5/5e cables. The 305m per box is set as the minimum. Please refer to revised technical specifications.

		indicated in the specification	
BB1-13	Section VII – Technical Specification 150 Desktop computers	Clarification on multi-media readers and type of ports listed in the Technical Specifications, current configurations does not offer it anymore.	Please refer to the revised Section VII - Technical Specifications.
BB1-14	Section VII – Technical Specification 29 Laptop computers	Consideration for using 3 cell battery rather than 6 cells.	Please refer to the revised Section VII - Technical Specifications.

Section VII. Technical Specifications

Technical Specifications

Item	Specification	Statement of Compliance
		Bidders must state here either “Comply” or “Not Comply” against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of “Comply” or “Not Comply” must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer’s un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of **ITB** Clause 3.1(a)(ii) and/or **GCC** Clause 2.1(a)(ii).

Item	Specification	Statement of Compliance	Proposed Equivalent Technology
LOT 1: Supply, Delivery, Installation and Configuration of Server Components and IT Infrastructure			
Hyper Converged Solution for 5 nodes			
Architecture	A Hyperconverged Infrastructure (HCI) that includes at least one (1) 42U Rack Cabinet, five (5) Hyperconverged Appliance Nodes, two (2) Top-Of-Rack Switches, and one (1) Management Switch.		
	This will provide PhilSys Registry Office the resources for a software-centric architecture that tightly integrates compute, storage and virtualization resources in a single system. This will aid the organization by leveraging virtualization technologies and addressing the challenges with the complexity and cost of data protection and storage. It is a technology that would allow PhilSys Registry Office to focus their time, money and employee resources more on the operational aspects of their business and less on maintaining infrastructure.		
Infrastructure	All components must be from a single manufacturer for ease of support and integrated management		
	Supports industry standard hypervisors like VMware ESXi, Microsoft Hyper-V, and AHV		
	Supports differing CPU & memory configurations of nodes within the same cluster		
	Supports adding storage only nodes in the cluster		
	Supports an unlimited number of nodes in a cluster		
	Supports VM-centric snapshots and clones		
	Must be able to provide different levels of resiliency in the same cluster (RF2 or RF3 can be applied at a container level)		

	Must have native File, Block and Object services built into the platform		
	The solution should provide enterprise data services such as deduplication and compression with erasure coding completely in software without dependence on any proprietary hardware		
	Must have inline compression, inline deduplication, post-process compression, and post-process deduplication		
	Must have feature to do backup to public clouds		
	Must have feature to do multi site DR		
	Must have feature to do data-at-rest encryption		
	Must maintain data locality and services reads from the local host server		
	The solution should provide a single unified management console for the management of the entire environment including virtualized environment as well as software defined storage environment, underlying Hardware and associated components		
One (1) - Unit 42U Rack			
	Must have a 42U capacity		
	Must have square rack mount flange hole type		
	Must have 6 sidewall compartments		
	Must have PDU mounting points		
	Must have front stabilizers, side stabilizers, casters, leveling feet, side covers, and perforated front door		
	Must include four (4) Switched and Monitored 32A 3 Phase PDU		
Two (2) - Top-of Rack Switches			
	Must have a 1U form factor		
	Must have 48X SFP28/SFP+ active ports and QSFP28/SQFP+ ports		
	Must cut-through switching method		

	Must have unicast, multicast, and broadcast data traffic types		
	Must have the following software features: Layer 2 switching, Layer 3 switching, virtual local area networks (VLANs), VLAN tagging, spanning tree protocol (STP), link aggregation (trunk) groups (LAGs),, Layer 2 failover, quality of service (QoS), IPv4/IPv6 management, IPv4/IPv6 routing, equal cost multiple paths (ECMP), IPv4/IPv6 virtual router redundancy protocol (VRRP), IPv4 policy-based routing (PBR), Converged Enhanced Ethernet (CEE) or Data Center Bridging, Network Policy Agent, VXLAN gateway, Python scripting, REST API programming, Telemetry agent.		
	Must have six N+1 redundant hot-swap fans. Rear (non-port side) to front (port side) or front to rear airflow for cooling.		
	Must have two load-sharing, redundant hot-swap 770W platinum power supplies.		
	Must have 1x 10/100/1000Mb Ethernet port (RJ-45); 1x RS-232 port (RJ-45); 1x USB 2.0 port		
	Management interface must have industry standard command line interface (isCLI); SNMP v1, V2, and V3; REST API.		
	Management Integration with Hyperconverged Dashboard must have the ability for the infrastructure or server administrator to modify the network as needed to support typical tasks, such as the creation, starting, and shutdown of new machines, as well as manipulation of guest virtual machines on VLANs. These tasks are performed through the hyperconverged management dashboard.		
	Secure features must include Secure Shell (SSH); Secure Copy (SCP); Secure FTP (sFTP); user level security; Role-based Access Control (RBAC); LDAP/LDAPS, RADIUS, and TACACS+ authentication; access control lists (ACLs); secure mode; Trusted Platform Module (TPM) 1.2.		
	Must have 5 years warranty, 24x7 with 4 hour response time.		

One (1) - Management Switch			
	Form factor must be 1U		
	Active ports must have 48x 1 Gb Ethernet fixed ports (RJ-45)		
	Must have unicast, multicast, and broadcast data traffic types		
	Must have the following software features: Layer 2 switching, Layer 3 switching, virtual local area networks (VLANs), VLAN tagging, spanning tree protocol (STP), link aggregation (trunk) groups (LAGs),, Layer 2 failover, quality of service (QoS), IPv4/IPv6 management, IPv4/IPv6 routing, equal cost multiple paths (ECMP), IPv4/IPv6 virtual router redundancy protocol (VRRP), Network Policy Agent, Python scripting, REST API programming.		
	Must have N+1 redundant hot-swap fans. Rear (non-port side) to front (port side) or front to rear airflow for cooling.		
	Must have two load-sharing, redundant hot-swap power supplies.		
	Must have hot-swappable parts for SFP/SFP+ transceivers, SFP+ DAC cables and AOCs, power supplies, fans.		
	Management ports must have ethernet, rs-232, and USB port.		
	Management Integration with Hyperconverged Dashboard must have the ability for the infrastructure or server administrator to modify the network as needed to support typical tasks, such as the creation, starting, and shutdown of new machines, as well as manipulation of guest virtual machines on VLANs. These tasks are performed through the hyperconverged management dashboard.		
	Secure features must include Secure Shell (SSH); Secure Copy (SCP); Secure FTP (sFTP); user level security; Role-based Access Control (RBAC); LDAP/LDAPS, RADIUS, and TACACS+ authentication; access control lists (ACLs); secure mode; Trusted Platform Module (TPM) 1.2.		

	Must have 5 years warranty, 24x7 with 4 hour response time.		
Five (5) - Hyper Converged Appliances			
	Must be a 1U rack mount form factor		
	Must have 2x Intel Xeon Gold 6238 22 core 2.1Ghz processor		
	Must have 24x 64GB TruDDR4 RDIMM memory		
	Memory must offer protection in the event of a non-correctable memory failure, Adaptive Double Device Data Correction, Error correction code (ECC),memory mirroring, and memory rank sparing, patrol scrubbing, and demand scrubbing.		
	Must have 10x 3.84TB SAS 12Gb Hot Swap SSD		
	Must have 2xplatinum Hot-Swap power supply		
	Must have seven hot-swap system funs with N+1 redundancy for cooling		
	Must have 2x 10Gb Base-T ports and 4x 10/25GbE SFP28		
	Systems management must have a system of LEDs on various external and internal components of the server that leads you to the failed component. When an error occurs, LEDs are lit on the front I/O assembly, the rear panel, the system board, and the failed component to simplify servicing, speeds up problem resolution, and helps improve system availability.		
	Systems management must continuously monitors system parameters, triggers alerts, and performs recovery actions in case of failure to minimize downtime with Built-in Server Management Module		
	Systems management must be able to provide proactive alerts for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, NVMe SSDs, M.2 storage, flash storage adapters), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures		
	Must comply with the following standards:		

	• United States: FCC Part 15, Class A; UL 60950-1 • Canada: ICES-003/NMB-03, Class A; CAN/CSA-C22.2 60950-1 • Mexico: NOM-19 • Argentina: IEC 60950-1 • European Union: CE Mark (EN55022 Class A, IEC/EN 60950-1, EN55024, EN61000-3-2, EN 61000-3-3) • Germany: TUV-GS (IEC/EN 60950-1, EK1-ITB2000) • Russia, Kazakhstan, Belarus: EAC (TR CU 004/2011, TR CU 020/2011) • China: CCC GB4943.1, GB9254 Class A, GB17625.1 • India: BIS • Japan: VCCI, Class A • Taiwan: BSMI CNS13438, Class A; CNS 14336-1 • Korea: KN22, Class A; KN24 • Australia/New Zealand: AS/NZS CISPR 22 Class A • Reduction of Hazardous Substances (ROHS) • Energy Star 2.1 • ASHRAE Class A2, A3 and A4 specifications		
	Must have 5 years warranty, 24x7 with 4 hour response time.		
	HCIS ENTERPRISE ADMINISTRATION The HCIS Enterprise Administration course is aimed to train administrators (system, network, and storage) to successfully deploy HCIS in the datacenter. It covers the basic		

	troubleshooting tools and advance tasks performed by HCIS administrators, including certification for HCIS Certified Professional. A minimum of four (4) days classroom-type training with hands-on laboratory, good for four (4) packs inclusive of accommodation and transportation. The training course shall be conducted by a certified or authorized HCIS training partners, including but not limited to the following training modules: ● Module 1: Introduction Introducing the Hypervisor. ● Module 2: Managing the HCIS Cluster Configuring an HCIS cluster, including setting up a name server and adding network connections, and set up file system whitelists. ● Module 3: Securing the HCIS Cluster Securing an HCIS cluster through user authentication, SSL certificate installation and cluster access control. ● Module 4: Networking Managing networks using Open vSwitch (OVS). The module also describes how to configure bridges, bonds, and VLANs. ● Module 5: VM Management Creating and managing Virtual Machines (VM), create a guest VM and importing a new image that can be applied to the VM. ● Module 6: Health Monitoring and Alerts Monitoring cluster health and performance in addition to configuring health checks for various components. Provides guidelines in monitoring cluster performance, and customization of system alerts and events. ● Module 7: Overview of the various HCIS storage components, including		

	Storage Tiers, Pools, Containers, Volume Groups, vDisks, and Datastores/SMB Shares. ● Module 8: Workload Migration Migrating workloads in hypervisor.. ● Module 9: Services Shows Block Services provide high-availability, high-performance block storage through simple client configuration. ● Module 10: Business Continuity Provides comprehensive data protection at all levels of the virtual datacenter: VM, file, and volume group. ● Module 11: Data Protection Using the HCIS main Web Console to create a remote site and a Protection Domain. ● Module 12: HCIS Central Multiple capabilities of HCIS Central, including monitoring and managing multiple activities across a set of the cluster. ● Module 13: Maintaining the HCIS Cluster HCIS Cluster Check (HCIS-CC), a framework of scripts that helps diagnose cluster health. ● Module 14: Life Cycle Operations Provides an overview of the essential lifecycle operations, including starting/ stopping an HCIS cluster, starting/shutting down a cluster node and searching/ updating inventory, and how to expand a cluster, manage licenses and upgrade software and firmware.		
Two (2) - Next Generation Firewall			

	The proposed NGFW should be based on a dedicated ASIC-based standalone appliance which should include: 1. Content Processor that accelerates content scanning activities such as AV 2. Network Processors (inbuilt and/or modules) used for acceleration of many key security functions including stateful packet header inspection, VPN encryption/decryption, protocol anomaly offloading, and quality of service enforcement. It should also provide acceleration for processing all packet sizes which include time sensitive applications such as VoIP, real-time protocols, and multimedia applications. 3. The proposed Appliance vendor must have "Recommended" Rating in NSS Labs 2019 NGFW Group Test 4. The proposed NGFW vendor must have ICSA validated security and performance 5. The proposed NGFW must be able to control wireless access points and switches of the same brand. The wireless access point devices communicate with the Firewall unit over wired networks. Add wireless interfaces (SSIDs) to the WiFi network and configure security features such as Rogue AP detection and WIDS. 6. The proposed NGFW must be able to support SD-WAN with no 3rd party hardware or additional licenses		
	The proposed NGFW Operating System must: 1. Resided on flash disk for reliability over hard disk 2. Allow dual booting 3. Upgradeable via Web UI or TFTP		

	The configurations on the device shall: 1. Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk 2. Provide CLI command configuration file that is readable by Windows Notepad 3. Have option for encrypted backup file 4. Have revisions listed on GUI for ease of use. The display shall allow revert to selected revision and configuration diff between 2 selected revisions. Administrators shall be able to add comments for each revision. The proposed NGFW shall minimally provide management access through: 1. GUI using HTTP or HTTPs access which administration service port can be configured, for example via tcp port 8080 2. CLI console using console port, SSHv2, telnet or on GUI's dashboard 3. The proposed NGFW shall offer option to automatically redirect HTTP management access to HTTPS 4. The proposed NGFW shall enforce mandatory default administrator password setup upon first time log in or after a factory reset.		
	The proposed NGFW shall have option to implement local administrator password policy enforcement		

	The proposed NGFW must be able to support the following feature components: 1. Intrusion Prevention System 2. Antivirus 3. Web Filtering 4. Application Control 5. User Group 6. Log & report Configurations		
	The proposed NGFW shall have the ability to interconnect discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire attack surface. The solution should offers the following capabilities: 1. A physical topology view that shows all connected devices, including access layer device and a logical topology view that show information about the interfaces that each device is connected to.		
	The proposed NGFW shall provide robust visibility GUI panels and dashboards that: 1. Utilizes data from options of local disk, external logging system 2. Pulls data from supported external systems via REST APIs 3. Draws real-time and historical data for displays of information in both text and visual format 4. Presents information visually using graphs, bubble charts and world map 5. Allows filtering (using specific time range, by user ID or local IP address, by application, etc) and drill-down of data 6. Allows customizable Top N views on the dashboard 7. Provides one-click action to quarantine		

	host based on selected data 8. The proposed NGFW shall provide administrators ability to assign arbitrary score given based on the perceived risk of certain events such as visits to malicious websites and malware detection. Threat scores will be logged and computed for each host as they match risky events. Thus, administrator shall be able to rank and identify most risky hosts in the network.		
	The proposed NGFW shall provide monitoring capabilities through GUI including: 1. Static, dynamic and policy routing status 2. DHCP service status 3. SD-WAN links status and usage 4. IPsec and SSL VPN sessions status 5. Host security and quarantine status		
	Network Capabilities 1. The proposed NGFW shall support the IEEE standard 802.3ad for physical link aggregation 2. Administrators shall be able to configure both IPv4 and IPv6 DHCP service on an interface of the proposed NGFW. The interface shall automatically broadcast DHCP requests and then provide IP address, any DNS server addresses, and the default gateway address to clients 3. Administrators shall be able to configure an interface as a DHCP relay 4. Administrators shall be able to adjust the maximum transmission unit (MTU) of the packets that the proposed NGFW transmits to improve network performance		

	5. A loopback interface is a logical interface that's always up (no physical link dependency) and the attached subnet is always present in the routing table. Administrators shall be able to configure multiple loopback interfaces on the proposed NGFW 6. The proposed NGFW shall support static routing 7. Support for both IPv4 and IPv6 routes 8. Ability to define static routes with administrative distance and priority. Priority, which will artificially weight the route during route selection. The higher the priority number, the less likely the route is to be selected over other routes. 9. Ability to define destinations in static routes using IP subnet, firewall address (including FQDN type) objects, and Internet service objects. Internet service objects are IP lists mapped to popular Internet services and are residing on a dynamically updated database. 10. The proposed NGFW shall support reverse path lookup (anti-spoofing). This feature can be disabled to enable asymmetric routing. 11. The proposed NGFW shall support Open Shortest Path First (OSPF), OSPFv2 and OSPFv3 routing protocols 12. The proposed NGFW shall support BGP routing protocol		
	The proposed NGFW shall support performance SLA (also known as health checks) settings which are used to monitor WAN interfaces link quality and to detect link failures. They can be used to remove routes, and to reroute traffic when an SD-WAN member cannot detect the server. The settings should include: 1. Predefined performance SLA profiles		

	such as Office 365, AWS and Gmail 2. Health check probes using IPv4/IPv6 Ping and HTTP 3. Selection of multiple destinations(or servers) to probe 4. Interfaces relating to the performance SLA profile		
	The proposed NGFW shall allow SLA targets to be created. These are a set of constraints that are used in SD-WAN rules to control the paths that traffic takes. These constraints should include: 1. Latency threshold 2. Jitter threshold 3. Packet loss threshold 4. The proposed NGFW shall provide settings to the characteristics of probes, including check interval, link failure and restoration considerations. 5. The proposed NGFW shall provide option to disable the implicated static route when an interface is inactive.		
	The proposed NGFW shall provide the following path control strategies: 1. Manual: Interfaces are manually assigned a priority 2. Best Quality: Interface are assigned a priority based on the quality of the interface. Quality criteria may be latency, jitter, packet loss, available bandwidth (for upstream, downstream, or both) or custom with a cocktail of weighted criteria 3. Lowest Cost (SLA): Interface is selected based on the lowest cost defined on SD-WAN interfaces that meets selected SLA settings 4. Maximize Bandwidth (SLA): Traffic is distributed among all available links		

	that satisfies selected SLA profile based on a round-robin load balancing algorithm		
	The proposed NGFW shall provide implicit an SD-WAN rule for sessions that do not meet the conditions of defined rules. This implicit rule shall offer the following load balancing algorithms with the ability to assign weight on each member interfaces: 1. Source IP: The system divides traffic equally between the interfaces. However, sessions that start at the same source IP address use the same path 2. Sessions: The system distributes the workload based on the number of sessions that are connected through the interfaces. 3. Spillover: If the amount of traffic bandwidth on an interface exceeds the ingress or egress thresholds that organization set for that interface, the system sends additional traffic through one of the other member interfaces. 4. Source-Destination IP: Sessions that start at the same source IP address and go to the same destination IP address use the same path. 5. Volume: The system uses the weight that is assigned to each interface to calculate a percentage of the total bandwidth that's allowed to go through each interface. 6. The proposed NGFW shall support forward error correction (FEC) on VPN overlay networks.		
	Support and Training Requirements 1. Principal TAC Support must be available 24/7/365		
	NGFW Platform Specifications 1. Threat Protection Throughput must be at least 1.2 Gbps 2. Concurrent Sessions (TCP) must be at		

	least 2 million 3. New Sessions/Sec (TCP) must be at least 135,000 4. IPsec VPN Throughput (512 byte) must be at least 9 Gbps 5. Gateway-to-Gateway IPsec VPN Tunnels must be at least 2,000 6. Client-to-Gateway IPsec VPN Tunnels must be at least 10,000 7. SSL Inspection Throughput must be at least 820 Mbps 8. Form factor should be 1RU 9. Required Network Interface per NGFW are: 18 x GE RJ45 (including 2 x WAN ports, 1 x MGMT port, 1 X HA port, 14 x switch ports), 4 x GE SFP slots 10. 480GB Onboard Storage 11. Required security license and support: 5 years		
Twenty (20) - Managed Switch (Gigabit 24 Port)			
	Form factor must be 1U Rack Mount		
	Media Type: Must be 1 Gb Ethernet fixed ports (1000BASE-T): RJ-45 UTP Category 5 or 5e 1 Gb Ethernet SFP 1 GbE short-wavelength (SX) SFP transceivers 1 GbE long-wavelength (LX) SFP transceivers 10 Gb Ethernet SFP+: 10 GbE short-range (SR) SFP+ transceivers 10 GbE long-range (LR) SFP+ transceivers 10 GbE extended-range (ER) SFP+ transceivers 10 GbE RJ-45 SFP+		

	transceivers 10 GbE SFP+ active optical cables 10 GbE SFP+ DAC cables		
	Port Speeds: 1 GbE fixed ports must be 10 / 100 / 1000 Mbps auto-sensing		
	1 GbE SFP transceivers must be at least 1 Gbps		
	10 GbE SFP+ transceivers, DAC cables, and AOCs must be at least 10 Gbps		
	1/10 GbE SFP+ transceivers must be at least 1 Gbps or 10 Gbps		
	Must have store-and-forward for switching method		
	Must be Unicast, multicast, broadcast for data traffic types		
	Must be Two fixed, internal, variable-speed system fans with side-to-side (left-to-right) airflow for cooling		
	Must have One fixed 30 W AC (100 - 240 V) power supply (IEC 320-C14 connector). for the power supply		
	Must have SFP/SFP+ transceivers, SFP+ DAC cables, and SFP+ AOCs for hot swapping parts		
	Must have 1x 10/100 Mb Ethernet port (RJ-45), 1x RS-232 port (RJ-45) for management ports		
	Must have Web-based GUI; Command line interface (CLI); SNMP v1, V2, and v3 for management interfaces		
	Must have Secure Shell (SSH); Secure Copy (SCP); Secure FTP (sFTP); user level security; Role-based Access Control (RBAC); RADIUS and TACACS+ authentication; access control lists (ACLs), port security; port-based network access control (IEEE 802.1x) for security features		
	Must have (3) Three-year warranty		
Four (4) - NAS (Network Attached Storage)			
	Must have a 3U form factor.		

	Must have Intel Xeon processor		
	Must have hardware encryption engine		
	Must have at least 8GB memory and expandable to 64GB		
	Must have 16 drive bays with 4TB enterprise HDD included/installed per each bay		
	Must include sliding rail kit.		
	Five (5) years warranty with media retention		
Forty (40) - Monitoring Workstation			
	Must have an Intel Core i7 Processor		
	Must have 16GB of memory		
	Must have 2 x 23” LED with DisplayPort Interface		
	Must have 256 M.2 SSD and 2TB HDD		
	Must have a dedicated graphics card with HDMI and 2x DisplayPort interface		
	Must have a preloaded operating system Windows 10 Pro 64 bit (installed and activated)		
	Must have USB Keyboard and Mouse		
	Must have 1000 KVA UPS		
	Must have TPM 2.0 and Energy Star Compliance		
	Must have a Warranty of Three (3) years on on-site support; Three (3) years on parts; and Three (3) years warranty on labor) with media retention		
Ten (10) - Display Screen 55" w/ LAN Port			
	Must have a screen size of 55”		
	Must have a resolution at least 3840 X 2160		
	Must have a Lan Port		
	Must have at least 4 HDMI Slots		
	One (1) year warranty		
Two (2) - Display Screen 65" w/ LAN Port			

	Must have a screen size of 65”		
	Must have a resolution at least 3840 x 2160		
	Must have a Lan Port		
	Must have at least 4 HDMI Slots		
	One (1) year warranty		
Forty (40) - IP Camera			
	Must have a resolution of 1080p FULL HD 30 FPS		
	Must have at least effective focal length of 3.6mm, f/1.8		
	Must be Outdoor Weather Resistant		
	Must have 802.3af PoE 24V Passive PoE of power supply		
	Must have Built-in Microphone		
	Must be Wall, Ceiling or Pole mount mountable		
	One (1) year warranty		
	Installation not included		
Five (5) - Biometric Door Locks			
	Unlock Method: Fingerprint, Password, Key, APP, Card		
	Must have electric lock, door sensor, exit button, alarm for Access control Interface		
	Must have door mounting kit		
	Must have power supply		
Twenty (20) - Two-Way Radio			
	Must have frequency range or [TX] 136 - 174MHz, 400 - 520MHz [RX] 136 - 174MHz, 400 - 520MHz, 68-108MHz (FM Broadcast)		
	Must have at least 128 channels		
	Must have at least 25KHz (wide band)12.5KHz (narrow band) for channel		

	spacing		
	Must have ≤0.25µV (wide band) ≤0.35µV (narrow band) for sensitivity		
	Must be 2.5, 5, 6.25, 10, 12.5, 20, 25, 30 and 50KHz for frequency steps		
	Must be SMA-Female / Antenna Impedance: 50Ω for antenna connector		
	Must have power adapter,earpiece,belt clip,hand strap,battery charger and manual		
	Must have warranty		
Five (5) – Laptop			
	Must have 1.4Ghz quad-core 8th-generation Intel Core I5 Processor, Turbo Boost up to 3.9Ghz		
	Must have integrated graphics		
	Must have 8GB Memory of RAM		
	Must have 256GB SSD storage		
	Must have a Wireless Keyboard and Mouse		
	Must include a MAC operating system		
	Must have Energy Star Compliance		
Five (5) - Laptop 64 Bit High Capacity			
	Must have Intel I7 of processor		
	Must have 16GB of Memory		
	Must have 256 M.2 SSD and 1TB HDD for storage		
	Must have a Dedicated graphics card		
	Must have a Wireless Keyboard and Mouse		
	Must have Windows 10 Pro 64 bit (installed and activated) of preloaded operating system		
	Must have TPM 2.0 and Energy Star Compliance		
	Must have warranty (Three (3) years on on-site support; Three (3) years on parts; and Three (3) years on warranty on labor) with		

	media retention		
	Must have Wireless Keyboard and Mouse		
Fifty (50) - Router/Gateway			
	Must have (3) 10/100/1000 for RJ45 Ports		
	Must have (1) RJ45 Serial Console Port		
	Must be quiet and fan-less operation		
	Must have Layer 3 Forwarding Performance		
	Must be 1,000,000pps for the packet size of 64bytes		
	Must be at least 3Gbps for line rate		
Twenty (20) - UTP Cable CAT 6			
	Category 6 UTP cable minimum of 305 meters per box		
Ten Thousand (10,000) - RJ 45 (Cat 5e)			
	RJ 45 Network connector		
One Thousand (1,000) - Rubber Boot			
	Rubber boot for RJ 45 connector		
Five Thousand Three Hundred (5,300) - Endpoint Security			
	ANTI-MALWARE 1. The solution must have multiple anti-malware engines – with the combination of the traditional Signature-based, heuristic, Cloud-Assisted scanning and Machine Learning technology – for superior scanning and detection capability. 2. The solution should be able to provide security for heterogeneous IT environment. It shall support a range of platforms – including Mac, Linux and Windows – Including the new Windows 10 and Windows Server 2016 operating system.		

	3. Lightweight mode for Threat Protection ("Cloud mode"). Light antivirus databases (require less RAM and drive space). 4. The solution should provide protection against new and unknown malwares. It should have an urgent detection system that may help protect the system against new threats, even before the release of a new malware signature. 5. The solution should be able to monitor the behaviour of applications automatically. It should have Behavioural Detection, Exploit, Anti-Rootkit and Remediation Engine that monitor the system – real time and will detect any suspicious behaviour deeper within your system and application that rolls back actions done by malware. 6. The Solution should have Protection against encryption for shared folders unique anti-cryptor mechanism capable of blocking encryption of files on the shared resources from the malicious process running on another machine on the same network. 7. The solution should have a deeper level of protection that could work on the lowest level of a computers' operating system. 8. The Solution should have technologies that are improving its performance by estimating file threat level on the basis of its last modification date. File last modification date is compared against its first scan date, creation date, and antivirus databases release date. 9. The solution should have Host-based Intrusion Prevention System (HIPS) and personal firewall that would protect against hacker attacks. It should be able to control inbound and outbound traffic – by setting up parameters for an individual port, IP address or application. 10. The solution should have a Network		

	Threat Blocker mechanism that detects and monitors suspicious activity on your network. It should be pre-configurable on how the system should respond when suspicious behaviouris detected. 11. The solutions should be able to auto-quarantine or auto-delete identified malwares without end-user interaction. 12. The solution should be able to scan body text and attachments of incoming e-mail messages that are delivered through POP3 / IMAP mail clients. 13. The solution should be able to block malicious/phishing URLs. 14. The solution should be able to scan password protected compressed files for malicious programs. 15. The solution should be able to re-launch itself automatically - when file server restarts - on events that the server experiences fault or suffering an unplanned shut down. 16. The Solution should have AMSI Protection Provider. Antimalware Scan Interface (AMSI) allows a third-party application with AMSI support to send objects (for example, PowerShell scripts) to endpoint security solution for additional scan and to receive scan results for these objects. 17. The Solution should be able to monitor and block abnormal behavior of applications. 18. The solution should have the option of single agent for EDR and EPP (Endpoint Protection) that can be activated via licensing option.		
	APPLICATION CONTROL 1. The solution should be able to control application startup by blocking, granting or auditing each application upon launch.		

	2. The solution should be able to monitor and classify each application as trusted, untrusted or restricted. 3. The solution should be able to control whether an application is given access to specific system resources, such as the file system or the registry. 4. The solution should be able to do Blacklisting and Whitelisting technology. 5. The solution should have a dynamic whitelisting service that assesses the security of commonly used applications. Whitelist database should be updated regularly and automatically to ensure up-to-date protection. 6. Policy should be able to use user account-based profile on the active directory.		
	DEVICE CONTROL 1. The solution should be able to allow administrator to set policy and control to any connected device, on any connection bus (not only USB), at any time. 2. The solutions should be able to support device management and shall allow administrator to monitor, block or make the device Read-Only along with the option of providing exceptions. 3. The solution should be able to block or allow devices based on specific serial number. 4. The solution should be able to generate logs of events associated with deleting and saving files on USB device. 5. The solution should be able to generate logs of list of trusted Wi-Fi networks, based on network name, encryption type, and authentication type. 6. The solution should be able to monitor		

	information about write and removal operations performed with files located on removable drives. 7. The solution should have Anti-Bridging capability which blocks unauthorized commuting between networks. 8. Policy should be able to use user account-based profile on the active directory.		
	WEB CONTROL 1. The solution should be able to filter each client's web browser usage. It should be able to permit, prohibit, limit or audit users' access to individual websites or categories of websites – including games websites, gambling sites or social networks. 2. Policy should be able to use user account-based profile on the active directory.		
	DATA PROTECTION 1. The solution should be capable of doing Full-Disk Encryption (FDE) and protects data on hard-drives 2. The Solution should be capable of Bitlocker Management 3. The solution should be able to do - pre-boot authentication – that is requiring users to pass through an authentication process before the operating system will even launch. 4. The solution should be capable of doing single sign-on (SSO). 5. The solution should be capable of doing File-Level Encryption (FLE). 6. The solutions should be capable of encryption removable drive (USB) by means of Entire Drive Encryption and Portable Mode. 7. The solutions should be capable of		

	protecting data during transfer, storage and restoration, regardless of the policy settings at the endpoint to which the data is restored. 8. The solution should be able to prevent exchange of encrypted files over IM or Skype, without restricting legitimate message exchange. 9. The solution should be capable of providing mechanism for password recovery. 10. Ability to recover disk data in case of hardware failures. 11. The solution should be GDPR compliant.		
	MOBILE DEVICE MANAGEMENT AND SECURITY 1. The solution should be able to configure and manage smartphones and tablets from a single console. 2. The solution should be compatible with different mobile platforms – IOS and Android. 3. The solution should be able to do – “Over the Air” Provisioning. It should be able to secure phones remotely by sending either an email or SMS containing a link to the corporate portal where users can download the profile and applications that administrator has approved. 4. The solution should be able to detect rooted and jailbreak mobile devices to ensure compliance policy in the network. 5. The solution should be able to enforce security settings such as camera disabling and force password. 6. The solution should be able to control the applications that are being run in the mobile devices. 7. The solution should be able to encrypt		

	corporate data on mobile devices. 8. The solution should have “Anti-Theft” mechanism for mobile devices. 9. The solution should have multiple layers of anti-malware protection on mobile devices. 10. The solution should have a “CONTAINERIZATION” mechanism that will separate corporate data from personal data on mobile devices.		
	SYSTEM MANAGEMENT TOOLS 1. The solution should have operating system and application provisioning. Provide easy creation, storage, cloning and deployment of system images from a central location. 2. The solution should be able to check operating system and other application vulnerabilities 3. The solution should be able to patch Microsoft systems files and other 3rd party applications seamlessly. 4. Patching should be automatic or scheduled. 5. The solution should have license provision and control. It should have tools that could limit usage only to approved applications and versions - and restrict the number of licenses in use. 6. The solution should have an asset inventory system that would list all hardware devices and software applications in the network. A notification should be sent to administrator once a new device has been found in the network. 7. The solution should support “Wake-On LAN Technology” that would allow the solution to power-on workstations remotely during long hours of deployment or troubleshooting		

	process. 8. The solution should be able to assign workstations that would act as remote agent in a remote branch office for central update agent. 9. The solution should have the capability to do remote and software installation from centralized management server. 10. The solutions should have troubleshooting tools that can be used to remotely and securely connect to a client system to fix issues — from the same administration console. UNIFIED MANAGEMENT CONSOLE 1. The solution should be capable of deploying applications such as end-point and third-party applications on a machine remotely. 2. The solutions shall support Policy Enforcement 3. The solutions shall provide dashboard with multiple information & these information should also be fetched from database based on different queries. 4. The solution should be able to have automated mobile policies for devices that leave the corporate network. 5. The solution should provide pre-defined policies as well as provide provision to change and customize policies based on groupings. 6. The solution should have a single and unified management console to all its security and control features. 7. The solutions should be able to manage mixed platforms in one management console. 8. The solution should be able to support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet of		

	machines or a particular site. 9. The solution should be able to provide a concise and accurate report that can be customized by the administrator. 10. The solution shall support reporting in the following format like XML, HTML and or PDF 11. The solution should have a web-interface that will be used to monitor the protection status and reports remotely.		
	CERTIFICATIONS AND ACCREDITATIONS 1. The solution should be recognized by ICSA Lab, NSS Lab. 2. The solution must be certified by the following 3rd party testing organization: VB100, AV Comparatives –with +ADVANCE rating at least for 3 consecutive years.		
	MAINTENANCE AND SUPPORT LEVEL AGREEMENT 1. The solution should have a local distributor representative in the Philippines. 2. The supplier of the solution should have certified engineers for end-point solution. 3. The solution must be able to provide a 3-tier support. The local reseller as the first-level of support, the distributor as the second-level and the principal as the third-level of support. 4. The supplier of the solution must be able to provide a comprehensive after-sales support and 5. Maintenance agreement with options of 8x5, 8x7 SLA. 6. The supplier of the solution must be able to provide support through Phone, Email, Web-Remote		

	Assistance and On-Site/On-Call support. 7. The supplier of the solution must be able to provide quarterly systems check-up for health monitoring.		
	License for five (5) years		
Twenty (20) - Managed Switch (Gigabit 16-Port)			
	Must have 16 Gigabit RJ45 Ports		
	Must have 2 SFP Ports		
	Must have 1 Serial Console Port		
	Must have at least 18Gbps of Non-Blocking Throughput		
	Must have at least 36Gbps of switching capacity		
	Must be Rack-Mountable or Wall-Mountable with Rackmount (Brackets Included)		
	Must have Supports for PoE+ IEEE 802.3at/af and 24V Passive PoE		
	One (1) year warranty		
Fifteen (15) - Crimping Tool			
	Must be heavy duty and able to crimp RJ45, RJ-11 connector.		
One (1) - Fiber Cable			
	Must be duplex single core fiber cable for SC type connector (300 meter box)		
One Hundred (100) - Fiber Connector			
	Must be SC/UPC-P Optic Fiber Quick Connector Fast Adapter Single Mode.		
Ten (10) - Media Converter			
	Gigabit Fiber Media Converter with SC type connector		
Ten (10) - Network Wire Tracker and Tester			
	Network Wire Tracker and Tester ● Must be able to trace and locate RJ45		

	(STP / 4-core), RJ11, USB, BNC cables. ● Anti-jamming, capable of working on the exchanger and PC startup. ● Measure cable length for RJ45, BNC cable. ● Check open, short, cross, crosstalk for RJ11, RJ45, BNC Cable. ● Locate short and breakage point accurately. ● With LCD screen		
Two Thousand (2,000) - Velcro straps (1/2" x 6")			
	Nylon Velcro cable ties/tidy straps for organizing network cables.		
Five (5) - Electric Drill			
	Must be 600Watts and heavy duty Must have Forward/Reverse rotation function Must have speed selection Must have all ball bearing construction		
Ten (10) - Electric Screwdriver			
	Must have a rechargeable battery Must have a maximum screw diameter of 5mm Must have 3/4/-Nm (soft/hard/max) torque rating		
Ten (10) - Screwdriver Set			
	Must have common sizes of screwdrivers used for ICT (Slot/Flat, Cross/Phillips)		
Twenty (20) - Barcode Scanner 2D			
	Barcode scanner/reader must have a scan pattern area mage of 838 x 640 pixel, motion tolerance of up to 610 cm/s. Scan angle HD focus of 41.4 degrees horizontal and 32.2 degrees vertical. Must have decode capability for 1D, PDF, 2D, postal and OCR symbologies. At least IP 41 environmental sealing.		

	One (1) year warranty		
Six (6) - Security Label Sticker			
	Must be compatible with Zebra S4M label printer Must be 2.0" (L) x 1.0"(W) of size Must have at least 5,000pcs/Roll Must be 1 Across for column Must have at least 3-inch of core		
Twelve (12) - Polyester Label Sticker			
	Must be compatible with Zebra S4M label printer Must be 2.0" (W) x 1.0" (L) of size Must have at least 10,000pcs/Roll Must be 2 across of column Must have 3-inch Core Must include 1 roll of ribbon for every 2 rolls		
Five (5) - Projector (LED) Full HD			
	Must have Full HD native resolution Must include a five (5) meter HDMI cable Must support wireless connection (802.11bgn) Must have HDMI, D-Sub and Composite RCA input One (1) year warranty		
Ten (10) - Heavy Duty Paper Shredder			
	Shredder must cut 4mmx12mm Shredder must have auto document feed feature to accommodate upto 150 pages of A4/Letter. One (1) year warranty		
Ten (10) - Laser Printer (Black and White) Network Duplex			
	Paper input tray must at least accommodate 500 sheets of A4/Letter		

	Must be capable of 40pages (A4) per minute		
	Must be able to print in duplex mode		
	Must be able to connect to LAN		
	One (1) year warranty		
One (1) - A1 Inkjet Printer			
	Must be able to print on a 329mm to 610 mm wide paper roll		
	Must be able to accept cutsheet paper (A4 to A3) via automatic sheet feeder (ASF)		
	Must be able to accept inkjet coater paper, tracing paper and plain paper.		
	Must be able to print 2400 x 1200 dpi maximum resolution		
	Must have a minimum ink droplet size of 4.0pl		
	Must have 4 color ink: CMYK (Cyan, Magenta, Yellow, Black)		
	Must include additional 4x 80ml black ink and 2x 50ml ink each for Cyan, Magenta and Yellow		
	Two (2) year warranty		
Five (5) - Piano Wire Cutters			
	Piano wire cutter / Hard wire side cutter		
Six (6) - Foldable Trolley 500KG Capacity			
	Must be foldable and has a capacity of 500KG		

Item	Specification	Statement of Compliance
LOT 2 : ICT Equipments Computer and Laptop		
Twenty Nine (29) Laptop lightweight Branded		

	Must have an Intel Core i7 / AMD Ryzen 7 Must have 8Gb DDR4 Memory Must have a minimum 512GB SSD Drive Must have a minimum of 15.6” Diagonal HD Screen Must have a built-in 720p HD Webcam Must have Gigabit Ethernet, 802.11 a/b/g/n/ac WiFi and Bluetooth Must have a USB 3.0, USB 2.0, HDMI connectors Must have pre-installed and activated Windows 10 Professional 64bit Must have TPM 2.0 and Energy Star Compliance	
	WARRANTY:	
	Three (3) years warranty on both parts and labor One (1) year on Batteries & Optical Mouse	
One Hundred Fifty (150) DESKTOP BRANDED		
	Must have Intel Core i5 / Ryzen 5 Must have a minimum of 8GB Must have a minimum of 256GB SSD Must have Gigabit ethernet network interface Must have USB 3.0 and 2.0 Ports Must have VGA and HDMI Ports Must have a minimum of 21.5” Full HD on Display Screen Must have USB Mouse and full-sized keyboard	

	Must have Windows 10 Professional 64bit preloaded Operating System Must have TPM 1.2 or higher and Energy Star Compliance Must have a warranty of Three (3) years on parts and labor	

Item	Specification	Statement of Compliance
Lot 3 : Expansion of the existing storage of UCS server for Data Center		
One (1) VSP G200 Upgrade Unified		
	2 Drive chassis -SFF (supports 24 x 2.5” drives) 55.334TB Usable (Base 10) 50.326TB (Base 2) 1.2TB SFF HDD RAID 5 6D+ 1P Array Group Complete Cords/Cables for attachment to the existing SAN Power cable 250VAC 10A IEC320-C14 If parts/disk drives are found defective within the warranty period, it should be changed at no cost. Supply, delivery, installation, knowledge transfer and training 24x7 access to helpdesk Configuration to attach with existing (at no cost) If parts/disk drives are found defective within the warranty period, it should be changed at no cost. 13 Months support from the time the equipment is configured	

_____	_____	_____
Name of Company	Signature over Printed Name of Authorized Representative	Date