DEPARTMENT OF FOREIGN AFFAIRS
KAGAWARAN NG UGNAYANG PANLABAS

BAGONG PILIPINAS

BIDS AND AWARDS COMMITTEE
2330 Roxas Boulevard, Pasay City
Tel. Nos.: 834-4823; Fax No.: 831-9584
Email: bac.secretariat@dfa.gov.ph

SUPPLEMENTAL / BID BULLETIN No. 1

Project	:	ICT Infrastructure for the Enhancement of the Network and Cybersecurity of the Practical Operation and Implementation of the Apostille Convention Systems
Reference	:	PB-GS-13-2024
ABC	:	PhP 27,000,000.00
Date	:	18 October 2024

This **Supplemental/Bid Bulletin** is issued to provide prospective bidders of the amended Technical Specifications for the above mentioned project (copy attached), particularly:

Page No.	Item	Previous Information	New Information
3	Network Firewall	*Must include a license for 3 years*	None
3	Wireless Access Point	*Must include a license for 3 years.*	None
4	Network Switch	*Must include a warranty of at least 5 years*	None
4	Network Switch	*Must include a warranty of at least 3 years PoE+ ports*	None
4	Network Switch, 48 port POE	*Mbps*	Mpps
4	Network Switch, 24 port POE	*Mbps*	Mpps
5	Network Switch	*Must include a warranty of at least 5 years;*	None
18	Desktop Computers	*4.8 GHz*	4.6 GHz
19	Laptop	*5.2 GHz, 30MB smart cache*	5.0 Ghz, 12MB L3 cache
25	Network Attached Storage	*at least four (4) x 64 GB.*	at least four (4) x 16 GB (64 GB)

For the information and guidance of all concerned.

ADELIO ANGELITO S. CRUZ
Chairperson
OCA Bids and Awards Committee

Terms of Reference

Procurement of ICT Infrastructure for the Enhancement of the Network and Cybersecurity of the Practical Operation and Implementation of the Apostille Convention Systems

Approved Budget of Contract: PhP 27,000,000.00

I	**Background** The Department of Foreign Affairs (DFA) aims to enhance the ICT infrastructure being used for the Apostille systems and issuances through the procurement of the network and cybersecurity equipment/tools for the practical operation and implementation of the Apostille Convention. Cybersecurity is a critical, border-level issue and the instances of cybersecurity breaches are rising and are getting increasingly sophisticated. Enhancement of ICT infrastructures is vital in protecting the internet-connected systems such as hardware, software and sensitive data from cyber threats. Having up-to-date tools and equipment ensure that security patches will be provided by the manufacturers. This project aims to increase the capability of the DFA in securing the public's documents and efficiency in servicing a larger volume of the general public applying for the authentication of their public documents and to protect the public's data as the recent significant cyber incidents include multiple government institutions locally and globally. Toward this end, the DFA shall procure ICT equipment and peripherals for the enhancement of network and cybersecurity for the practical operation and implementation of the Apostille Convention that would cater to the requirement of the task and the system for the efficiency and continuity of efficient service being provided to the general public. This initiative is in line with Executive Order No. 170 of 2022 and during the 2023 Statement of the Nation Address of President Ferdinand Marcos, the latter stated that "Government must embrace digitalization to provide better service to the people, through its vital frontline services and its-back end functions". Finally, digitalization was one of the six-cutting strategies under the Philippine Development Plan 2023-2028 that will serve as catalysts for economic, social, institutional and environmental transformation. In particular, Digital transformation of government will result in more efficient and faster service delivery, more transparency, and fewer opportunities for corruption at various levels. It can also help the government build robust

	data systems that will create better programs, such as targeted social protection and more efficient employment-opportunity linking systems.		
II	**Objective** The DFA-Office of Consular Affairs (OCA) shall procure ICT infrastructure for the enhancement of the network and cybersecurity of the practical operation and implementation of the Apostille Convention System to cater efficiently and continuously the needs for the application, processing and issuance of Apostille certificates through a secure and compliant foundation for hosting government workloads. The project's implementation would ensure that the systems and networks being used in the authentication processing of the Philippine public documents for use abroad, especially of Filipinos working overseas and emigrating are secured from cyber-attacks. Having up-to-date tools and equipment ensure that security patches will be provided by the manufacturers.		
III	**Scope of Work**		**Statement of Compliance**
	The contractor shall supply, deliver to DFA-ASEANA and to various Consular Offices with Authentication Services in Luzon, Visayas and Mindanao, and configure the ICT equipment and tools necessary to enhance the network and cybersecurity infrastructure of the DFA for the practical operation and implementation of the Apostille Convention.		
IV	**Technical Specification**		
	Item	**Specifications**	
	Network Firewall	Fifteen (**15**) units of Next-Gen Firewall ● Must have 2 x 1 Gigabit Ethernet SFP ports for WAN uplink; ● Must have 1 x 1 Gigabit Ethernet port for WAN uplink ; ● Must have 8 x 1 Gigabit Ethernet RJ45 LAN ports; ● Must have 1 x 1 Gigabit Ethernet port with PoE+ capabilities dedicated for the WAN uplinks; ● Must support at least 1 Gbps stateful firewall throughput; ● Must support at least 1 Gbps Maximum site-to-site VPN Throughput; ● Must support up to 200 concurrent site-to-site VPN tunnels;	

		● Must include Layer 3 and Layer 7 stateful firewall; ● Must support WAN link balancing and automatic WAN failover; ● Must include SD-WAN capabilities; ● Must support content filtering and advanced malware protection; ● Must support IDS/IPS protection ; ● Must support Active Directory integration; ● Must support custom traffic shaping ; ● Must provide network-wide visibility and control via Cloud-based Dashboard; ● Must include historical client usage statistics and Netflow support; ● Must include remote packet capture tools and Syslog integration; ● Must support operating temperature range of 0°C to 40°C; ● Must provide 8x5NBD technical support.	
	Wireless Access Point	Sixteen (**16**) units of Access Point ● Supports Wi-Fi 6E standard for enhanced performance; ● Tri-band operation with 2.4 GHz, 5 GHz, and 6 GHz radios; ● Includes multi-user , multi input, multi output (MU-MIMO) support for increased capacity and efficiency; ● Provides a tri-radio aggregate frame rate of at least 3.7 Gbps; ● Equipped with 2.5 Gbps mGig Ethernet port for high-speed connectivity; ● Support for 2.4 GHz Bluetooth Low Energy (BLE) radio with Beacon and BLE scanning for Concurrent operation of all five radios; ● Supported PoE: 802.3at or above; ● Includes Layer 7 traffic shaping; ● Provides full-time Wi-Fi ;location tracking for improved security ● Incorporates real-time WIDS/WIPS with alerting and automatic rogue AP containment;	

		● Allows for network-wide visibility and control via Cloud-based Dashboard; ● Supports cloud-based automatic RF optimization and seamless firmware updates; ● Includes support for 802.1X and Active Directory integration; ● Complies with RoHS standards for environmental safety; ● Operates within a temperature range of 0°C to 50°C; ● Must provide 8x5NBD technical support;	
	Network Switch	**48-Port POE** Two (**2**) units of Access Switch ● Must have at least 48 x 10/100/1000 Must include 4 x 10 Gigabit Ethernet SFP uplink ports; ● Must support PoE+ (IEEE 802.3at) with a power budget of at least 740W; ● Must have a forwarding rate of at least 75 Mpps; ● Must support at least 16,000 media access control (MAC) addresses; ● Must have a switching capacity of at least 100 Gbps; ● Must support up to 990 static routes; ● Must support IPv4, IPv6, CIDR, RIP v2, and PBR routing; ● Must support advanced security features such as 802.1X, DHCP snooping, and dynamic ARP inspection; ● Must include Access Control Lists (ACLs) for both IPv4 and IPv6 ; ● Must support encrypted communications (SSH, SSL) for management access; ● Must include a CLI, and SNMP support for management; ● Must support remote monitoring and troubleshooting; ● Must support stacking with up to 8 switches in a stack; ● Must include at least one (1) fan for cooling;	

		● Must operate within the temperature range of -5°C to 50°C; ● Must provide 8x5NBD technical support; **24-Port POE** Fourteen (**14**) units of Access Switch ● Must have at least 24 x 10/100/1000 PoE+ ports; ● Must include 4 x 10 Gigabit Ethernet SFP uplink ports; ● Must support PoE+ (IEEE 802.3at) with a power budget of at least 370W; ● Must have a forwarding rate of at least 40 Mpps; ● Must support at least 16,000 MAC addresses; ● Must have a switching capacity of at least 55 Gbps; ● Must support up to 990 static routes; ● Must support IPv4, IPv6, CIDR, RIP v2, and PBR routing; ● Must support advanced security features such as 802.1X, DHCP snooping, and dynamic ARP inspection; ● Must include access control lists (ACLs) for both IPv4 and IPv6 ; ● Must support encrypted communications (SSH, SSL) for management access ● Must include a CLI, and SNMP support for management; ● Must support remote monitoring and troubleshooting; ● Must support stacking with up to 8 switches in a stack; ● Must include at least one (1) fan for cooling; ● Must operate within the temperature range of -5°C to 50°C; ● Must provide 8x5NBD technical support;	

	Endpoint Detection and Response (Security)	Two hundred (**200**) endpoints security **A. General** ● The solution uses a blend of advanced threat protection techniques to eliminate security gaps across any user activity and any endpoint that constantly learns, adapts, and automatically shares threat intelligence across your environment. ● The solution has the capability to automatically detect and respond to the ever-growing variety of threats, including fileless attacks and ransomware. ● The solution should be cloud-managed and must support a hybrid deployment approach that is able to merge on-premise. ● The solution combines machine learning with other advanced detection techniques for the broadest protection against multiple threat sources may it be known or unknown. ● The solution has the ability to clean infected files, perform rollback and even recover lost files if necessary. ● The solution is able to provide off-premises compliance and protection which enables employees to work outside the corporate network and still be covered by the company security solution. ● The security vendor is open to customizing their security offering to tailor fit the needs of the customer. Also, it must allow co-existence with 3rd party security solutions that could also exist within the company environment. ● The solution provides a flexible choice of security agent deployment. It must be able to support mass deployment through the network and remote offices. It must also support	

		uninstallation of 3rd party security agents. B. **Anti-Virus** ● Exploit Prevention (host firewall, exploit protection). ● Command and Control (C&C) protection. ● The MAC security solution is able to provide more than the regular antimalware protection. It should also include capabilities such as device control, machine learning. C. **Vulnerability Protection** ● The solution is able to stop new or emerging threats that could potentially compromise your security regardless of the platform. ● The solution is able to perform virtual patching for vulnerable operating systems. ● The vulnerability protection solution is integrated on a single security agent. D. **Application Control** ● The solution provides a capable allow or deny functionality that is able to manage known and unknown applications, file types, and executables. ● The solution is able to provide a reliable file reputation source to allow cross checking of known good files. This source must be constantly kept up- to-date with the latest known good file listing. Provide methods on how your application control solution accepts whitelisting and blacklisting entries.	
	Systems Vulnerability Assessment and Penetration Testing	**System Architecture** ● The proposed solution must be offered as a Software Product and shall be able to run on a general x86 platform.	

		● The proposed solution must be able to operate 100% on-premise or Software as a Service. ● The proposed solution must provide an unified system architecture and management user interface to do both real attack testing(penetration testing) and simulated attack testing(adversary cyber emulation). ● The proposed solution must support a fully automated process that can mimic a real hacker's behavior to scan/discover the targets' attack surface exposures, system vulnerabilities, and then auto-exploit the system vulnerabilities to validate the real risk of the targets. ● The proposed solution must support a scalable architecture to do large scale network/system scan & asset profiling, vulnerability discovery & knowledge base mining, vulnerability auto-exploitation, post exploitation and risk prioritization/reporting. ● The proposed solution must support at least 4-tier of stealth level control for penetration testing tasks, including: Stealthy mode, Intermediate mode, Normal mode and Noisy mode. **Installation** ● The proposed solution must be able to run on general x86 platform and shall support 64-bit operating systems. ● The proposed solution shall be able to be deployed on bare metal servers or in virtual environments. ● The proposed solution shall be able to be deployed in popular Cloud platforms. ● The proposed solution shall include 200 ip addresses and 5 web servers licenses.	

		● The Bidder should provide a server if needed without additional cost to the DFA. **Performance** ● The proposed solution shall be able to utilize the symmetric multiprocessing capability of the x86 server platform to scale up the performance of a standalone server. ● The proposed solution must be able to run multiple software bot instances on one server and each bot instance can run its own testing tasks to improve overall system performance. ● The proposed solution shall support at least 100 concurrent bot instances on one server if the server hardware configuration allows. The number of bot instances supported shall be based on the server's computation resources. **Penetration Testing Coverage** ● The proposed solution must support plugin architecture for vulnerability discovery and exploit, and the plugin knowledge base shall be 100% on-premise and can be upgraded offline in environment where Internet access is not available. ● The proposed solution must support broader IT environment, supported target platform must include Server Hosts, Web Servers, Web Content Management Systems, Application Servers, Database Management Systems, Network Equipment, IoT Equipment, etc. ● The proposed solution must have a vulnerability/exploit plugin knowledge base with more than 36,000 plugins: a. Each plugin shall include CVSS score, CVSS vector, CVE number information if available	

		b. Each plugin shall have a vulnerability severity level & an exploitation risk control level associated with it. c. Plugin severity level shall have High, Medium, Low and Informational ● The proposed solution shall support user developed vulnerability/exploit plugins. ● The proposed solution must support user intervention mode and have attack logs for high impact penetration testing attacks. ● The proposed solution shall support free asset and attack surface discovery capability without consuming any license. Users can use it to discover IT infrastructure and identify critical assets and server open-port attack surfaces & website URL attack surfaces. ● The proposed solution must support pre-defined templates for following penetration testing use cases, e.g. Website Penetration, Intranet Penetration, Host Penetration, Ransomware Penetration, Weak password brute force and etc, simplify pentest operation for system administrators. ● The proposed solution must support both internal attack pentest scenario(e.g. host/application servers on Intranet) and external attack pentest scenario (e.g. Cloud hosted websites, CDN and etc). ● The proposed solution must support Ransomware penetration testing use case, can simulate popular ransomware intrusion techniques to exploit and validate target systems' risks for potential ransomware attacks. ● The proposed solution shall support Host Scan type and Web Scan type and allow system administrator to	

		configure networking parameters(e.g. port range, scan method) and crawler parameters(e.g.crawler mode, depth of URL, 404 page policy, Suffix filter, URL filter, URL white list) for scan jobs. ● The proposed solution shall support website's authenticated penetration testing. For non-standard website, the proposed solution shall provide a website login sequence recorder utility which can be used for non-standard website automatic login during a testing task. ● The proposed solution shall support Web Scan for both static web pages and dynamic web pages for vulnerability discovery and risk validation. ● The proposed solution shall support an intelligent mode for Web Scan. The system shall select dynamic web page crawlering or static web page crawlering automatically based on the web framework used by the target website. ● The proposed solution shall support webpage password bypass technology and shall be able to discover attack surfaces of password protected websites. ● The proposed solution shall be able to allow system administrator to configure proxy mode for smart crawling. ● The proposed solution shall support vulnerability/exploit plugin search capability on its web user interface. ● The proposed solution shall support integration with 3rd party VA scanner and have dedicated task template to validate the scanning results of a VA scanner, e.g. Tenable Nessus Pro, Rapid7 Nexpose. ● The proposed solution must support brute-force attack on services including but not limited to DB2, FTP,	

		Microsoft SQL Server, MySQL, PostgreSQL, RDP, Redis, Microsoft SMB, SNMP, SSH, Telnet, Web User Login, VNC, InfluxDb, Vmware ESXi, Weblogic, Drupal, Joomla, Apache CouchDB, Apache Tomcat, Apache ActiveMQ, Apache Axis2, RabbitMQ, SonarQube and etc. **Vulnerability Exploitation** ● The proposed solution must support automatic vulnerability exploitation and shall be able to show the real-time exploit progress on its web user interface. ● The proposed solution shall allow the system administrator to configure exploitation based on OS type, vulnerability severity levels, exploitation risk control levels and user defined keywords. ● The proposed solution must allow the system administrator to disable the auto-exploit functionality to provide more flexibility on risk control. ● The proposed solution shall support running individual exploit plugin based on system administrator's configuration on the web user interface. ● The proposed solution must be able to show the target environment's attack topology with at least 5 layers of information during the exploitation, including but not limited to target machine's IP, service, attack surface, vulnerability and business risk. ● The proposed solution must be able to show the whole kill chain information of an exploited vulnerability. ● The proposed solution must support reverse shell setup to validate exploitation of RCE vulnerability. ● The proposed solution must support deploying of persistent listeners on a designated node to allow exploited	

		hosts to connect back and validate data exfiltration. ● The proposed solution must be able to provide proof of a successful exploitation, including but not limited to database snapshots, web console outputs, filesystem directories, credentials. ● The proposed solution must be able to provide one-click validation to re-validate the vulnerability and the fix. ● The proposed solution must be able to provide one-click attack trace cleanup functionality. **Post-Exploitation Lateral Movement** ● The proposed solution must support lateral movement of post-exploitation and can use a compromised asset as a pivot to discover and exploit additional assets on adjacent networks. **Business Risk Prioritization** ● The proposed solution must be able to calculate the target system's risk based on the impact of exploited vulnerability and kill chain information. ● The proposed solution must be able to calculate the target system's overall health score based on the number of found attack surfaces, the numbers and severities of vulnerabilities and risks, as well as the conversion rate of attack surfaces to vulnerabilities & vulnerabilities to risks. **Adversary Cyber Emulation** ● The proposed solution shall provide a software agent that can be installed on assessment targets and simulate real-world cyber-attacks without any real harm or impact for the customer IT environment. ● The proposed solution shall support both commonly used operating	

		system platforms to install simulated attack agents. ● The proposed solution shall support a separated assessment testing script that can be executed independently on the assessment test agent. ● The proposed solution shall provide a block rate measurement for all assessment testing scripts executed. ● The proposed solution must support MITRE ATT&CK framework when using simulated attack to assess the target systems' security controls. **Vulnerability Management** ● The proposed solution must have a dedicated task template to identify and document the target machines' attack surface exposure. ● The proposed solution must support risk-based vulnerability prioritization, provide a simple risk table of high priority risk that the user needs to mitigate ASAP. ● The proposed solution must provide detailed information for every vulnerability discovered, including but not limited to vulnerability's type, severity, CVSS(Common Vulnerability Scoring System) score, CVSS vector, description, solution, reference link as well as the vulnerable target machine, attack surface and attack path for this vulnerability. The solution also need to provide a vulnerability validation tool which help user to re-validate the vulnerability after software patching. ● The proposed solution must provide detailed information for every risk it validates, including but not limited to risk type, compromised target machine and its OS version, compromised attack surface, attack path, user privilege and shell type the hacker may get. ● The proposed solution must provide a test report that include risk kill chain	

		information that the user can use for mitigation. ● The proposed solution must provide historical and trending reports for target machines' health score, total # of risk, total # of vulnerabilities, total # of attack surface and risk list of very previous test. ● The proposed solution must provide comparison reports to evaluate the security posture changes of target machines overtime, e.g. health score changes, difference of business risk, vulnerability and attack surface exposure of two security validation tests. **Assets Management** ● The proposed solution shall have a centralized database to manage IT assets for security validation. The managed assets shall include hosts with OS version info, server open ports & active application info, websites & application info, domain names & IP addresses as well as the assessment testing agent status. **Licensing** ● The proposed solution must support the subscription licensing model, and user can run an unlimited number of penetration testing during the license period. ● The proposed solution must support license migration when the underlying server platform is changed. ● The proposed solution must support licenses based on the quantity of target systems. **API** ● The proposed solution shall offer RESTful API for 3rd party system integration. ● The proposed solution shall support Token-based authentication for API. **Administration** ● The proposed solution must offer local administrative console for	

		secure system setup, e.g. password reset, system process restart, server shutdown/reboot and etc. ● The proposed solution must include web-based management user interface over encrypted traffic. It must not be accessed in clear-text. ● The proposed solution shall support two-factor authentication(2FA) for web user login. ● The proposed solution shall support SSL cert. management, users can upload its own SSL cert. or generate its own self-signed SSL cert. for WebUI. ● The proposed solution shall support online updates for system and vulnerability/exploit knowledge base when Internet access is available. ● The proposed solution must be able to update the system and vulnerability/exploit knowledge base in an environment where no Internet access is available. ● The proposed solution must support role-based access control for system operators to perform different tasks, e.g. create new pentest tasks, backup system/database, review system logs, etc. ● The proposed solution shall support manual and automatic backup for penetration testing task configurations and system databases/logs. ● The proposed solution shall support system database migration between different servers. ● The proposed solution shall allow the system administrator to configure notification for penetration testing tasks, e.g. email and syslog. ● The proposed solution shall be able to send CEF compliant syslog to integrate with SIEMs or other centralized management platforms.	

		● The proposed solution must be able to integrate with popular DevSecOps platform, Jira Cloud, Jira Data Center, ServiceNow and GitLab, for security issue and bug tracking. ● The proposed solution shall support GDPR and worldwide data privacy compliance. **Report and Data Export** ● The proposed solution must provide a built-in report for penetration testing results. ● The proposed solution must provide standard reports and support customized report functionality for different users, e.g. executive, IT operator, SOC operator, etc. ● The proposed solution must provide standard reports that prioritize business risks over vulnerabilities. ● The proposed solution must provide standard report for vulnerabilities, risks with kill chain details and overall system health score information. ● The proposed solution shall provide a standard report for asset profiling results, including system fingerprints. ● The proposed solution shall provide an Attack Surface Report template to report all public exposed attack surfaces of target systems. ● The proposed solution shall provide OWASP Top-10:2017 and OWASP Top-10:2021 Compliance Report templates for web penetration testing tasks. ● The proposed solution must support multiple report formats, including but not limited to PDF, HTML, CSV. ● The proposed solution shall provide multi-language support for the reports, e.g. English, Italian, Spanish and Korean. ● The proposed solution must allow a customer to add its company logo on the front page of the pentest reports.	

		● The proposed solution must be able to support an administrator to encrypt the penetration testing report before downloading it to protect the sensitive user data in the report.	
	Honeypot Security Mechanism	One (1) unit. ● The management server of the solution should run on a cloud based platform. ● The solution should provide a lightweight and reliable communication mechanism to the Console. ● The solution should create mechanisms to ensure reliability and security, such as preventing data exfiltration. ● The solution should be all communication between the sensor and console is encrypted and authenticated ● The Solution events should include but not be limited to: A. Source IP address B. Source port C. Destination IP address D. Destination port E. Reverse lookup of the host F. Description of the event G. Additional information (protocol-specific) ● The solution events should be correlated with the incidents and alerts on the console. ● Must have a Full Technical Support over 12 month subscription	
	Remote Access Software Subscription	One (**1**) lot **A. Auditability** ● Remote Access/Support; ● Outgoing and Incoming Connection Reporting; ● Enforced Session Recording; ● Customized Policies; ● Customized Installer. **B. Security**	

		● Encryption ■ 2048 RSA private/public key exchange ■ AES (256 bit) ● Access Protection ● Trusted Device Management ● Enforced Password Reset ● Unattended Access ● Wake-on-LAN ● Two Factor Authentication **C. Scalability** ● Mass Deployment ● Silent roll-out **D. Productivity** ● Account Provisioning ● One-click Remote Script Execution ● Custom Device Information ● Collaboration (virtual meeting up to 10 participants) **E. Manageability** ● Licensed users (10) ● Concurrent Connectivity (3 channels) ● Management Console ● Manage up to 500 devices ● User Management ● International Language ● Support for mobile device ● Commonly used operating systems **F. Device Grouping** ● Manage Group A. Add B. Edit C. Share D. Delete	
	Overhead Scanning Equipment	Thirteen (**13**) units ● Must have overhead and simplex scanner type ● Must have Scanning Color Mode: Color, Grayscale, Monochrome,	

		Automatic (Color / Grayscale / Monochrome detection) ● Must have at least one (1) Image Sensor: Lens reduction optics / Color CCD ● Must have an Optical Resolution of: A. 285 to 218 dpi (Horizontal scanning) B. 283 to 152 dpi (Vertical scanning) ● Document Size: A. Maximum must be 432 x 300 mm (17.0 x 11.8 in.) B. Minimum must be 25.4 x 25.4 mm (1 x 1 in.) ● Must have at least USB2.0 / USB1.1 (Connector Type: Type-B) ● Must have AC Power Requirements of 100 up to 240 V, 50/60 Hz ● Power Consumption A. Operating Mode: 20 W or less B. Sleep Mode: 2.6 W or less C. Auto Standby (Off) Mode: 0.4 W or less ● Operating Environment A. Temperature: 5 to 35 °C (41 to 95 °F) B. Relative Humidity: 20 to 80% (Non-condensing) ● Must have ScanSnap specific driver ● Image Processing Functions A. Deskew by text on document B. Automatic size detection C. Automatic rotation D. Automatic color detection E. Book image correction F. Multiple document detection	
	Desktop Computers	Thirty (**30**) units ● Must have at least 23.8” Full HD Borderless IPS Display (Non-Touch) ● Must have the at least 13th generation Processor (at least up to 4.6 GHz, 20MB smart cache) ● Must have at least 2 x 8GB DDR4 3200MHz (Upgradeable up to 32 GB of DDR4 3200 MHz)	

		• Must support up to 512GB PCIe SSD • Must have latest compatible graphics card • Must be integrated with WiFi 6E & Bluetooth • Must support wireless keyboard & mouse • Must have a built-in stereo speakers • Must have dimensions of at least 540.4 (W) x 37.3 (D) x 405.24 (H) mm • Must support Front/Side I/O connectors A. Card reader: N B. At least 1 USB 2.0 Type-A port(s) • Must support Rear I/O connectors A. At least 2 (in/out) HDMI port(s) B. At least 1 LAN port(s) C. At least 1 Audio jack(s) D. At least 1 - Thunderbolt 4 USB Type-C port(s): E. At least 3 USB 3.2 Gen2 Type A port(s) F. At least 1 USB 3.2 Gen2 Type C port(s)	
	Laptop	Fifteen (**15**) units • Must support the latest user-friendly, widely-used operating system. • Must have 13th Generation processor (at least up to 5.0 Ghz, 12MB L3 cache) with integrated SoC. • Must have memory up to 16 GB DDR4-3200 MHz RAM • Internal Storage up to 512 GB PCIe Gen4 NVMe M.2 SSD • Must be with a display of at least 14" diagonal, FHD (1920 x 1080) • Must be touchscreen • Brightness up to 250 nits • Must be Flicker-free • Must have cloud service of up to 25 GB Dropbox storage for 12 months • Battery type: 3-cell, 43 Wh Li-ion polymer • Must have a battery life of up to 9 hours or longer	

		● Must supports battery fast charge: approximately 50% in 30 minutes or better ● Must have at least Wi-Fi 6 and Bluetooth® 5.3 wireless card (supporting gigabit data rate) ● Must support full-size with backlit keyboard ● Must have a Wide Vision 720p HD camera ● Must have Dual speakers and Audio Boost ● Must have an Imagepad with multi-touch gesture support ● At least 1 microSD media card reader expansion slot ● Ports A. At least 1 USB Type-C with 10Gbps signaling rate B. At least 2 USB Type-A with 5Gbps signaling rate C. At least 1 HDMI 2.1 D. 1 AC smart pin E. 1 headphone/microphone combo ● Must have power supply type of 65 W Smart AC power adapter ● Must support Trusted Platform Module (Firmware TPM)	
	Tablet	Twenty seven (**27**) units ● Must have at least 11-inch display ● Must have at least 128GB capacity ● Must have LED-backlit Multi-Touch display with IPS technology ● Must have 2360x1640-pixel resolution at 264 ppi ● Must support stylus pen ● Must have at least 8-core CPU with 4 performance cores and 4 efficiency cores ● Must have at least 9-core GPU ● Must have at least 16-core Neural Engine ● Must have at least 8GB RAM ● Must have hardware-accelerated H.264 and HEVC	

		● Must have Video decode engine ● Must have Video encode engine ● Must have at least 12MP Wide camera, ƒ/1.8 aperture ● Must have Wi-Fi 6E (802.11ax) with 2x2 MIMO ● Must have Simultaneous dual band ● Must have at least Bluetooth 5.3	
	Inkjet Printers	Nine (**9**) units ● Must have hi-speed USB 2.0 port, Wireless 802.11 b/g/n ● Must support wireless capability with built-in Wi-Fi 802.11b/g/n ● Acoustic power emissions (active, printing): 6.5 B(A) ● Must have operating humidity range of 20 up to 70% RH (non-condensing) ● Must have an operating temperature range of 15°C to 27°C ● Must have a storage temperature range -20°C to 40°C ● Must support mercury free ● Must have memory of at least 64 MB ● Must have a maximum memory of up to 64 MB ● Must support mobile printing services: A. AirPrint B. Google Cloud Print™ C. Mobile Apps; Mopria™ Certified D. Wi-Fi® Direct printing ● Must support Network protocols: A. Via built-in networking solution B. TCP/IP, IPv4, IPv6; print C. TCP-IP port 9100 Direct Mode, LPD (raw queue support only), Web Services Printing; discovery: SLP, Bonjour, Web Services Discovery; D. IP Config: IPv4 (BootP, DHCP, AutoIP, Manual), IPv6 (Stateless Link-Local and via Router, Stateful via DHCPv6); E. management: SNMPv1/v2/v3, HTTP	

		● At least up to 150 sheets input capacity ● At least up to 10 Standard input capacity (envelopes) ● At least up to 100 sheets output capacity ● Must support energy savings feature technology: A. Auto-On/Auto-Off Technology; Power save; B. Power supply type: Internal (built-in) Power Supply; C. Power supply: 110-volt input voltage: 110 to 127 VAC, 50/60Hz and 220-volt input voltage: 220 to 240 VAC, 50/60Hz; D. Power consumption: 320 watts (Active Printing), 33 watts (Ready), 1.1 watts (Sleep), 0.2 watts (Manual off), 0.2 watts (Auto off/Manual on). ● Must have Print technology of Laser. ● Must support duplex printing: Manual (driver support provided). ● Must have Print resolution of up to 1,200 x 1,200 dpi. ● Must have at least maximum print area (metric) of 216 x 356 mm ● Must have monthly duty cycle of up to 10,000 pages. ● Must support printer smart software features: Manual duplex, N-up printing, collation, watermarks, accepts a variety of paper sizes and types. ● Must support minimum system requirements for operating systems from 2008 to latest, 1 GHz 32-bit or 64-bit processor or higher, 1 GB RAM, 16 GB HDD. ● Must have Compatible Network Operating Systems for 2008 operating system, 2008 Server R2, 8 (32/64 bit),10 (32/64 bit), 2012 Server, 2016 Server.	

		• Must support 2008 operating system to the latest.	
	Colored Printer	Two (**2**) units • Must have a features of Print, Scan, Copy, Fax with ADF. • Must have a Wi-Fi, Wi-Fi Direct connection. • Must have a minimum Ink Droplet Volume of at least 3.3 pl. • Must support Bi-directional printing. • Must have Nozzle Configuration of 400 x 1 nozzles (Black), 128 x 1 nozzles per color (Cyan, Magenta, Yellow). • Must have a maximum resolution of 4800 x 1200 dpi. • Must have Automatic 2-sided Printing (up to A4 / Letter). • Must have First Page Out Time from Ready Mode (Black / Colour): A. Simplex: Up to 10 sec / 16 sec B. Duplex: Up to 17 sec / 25 sec	
	Queueing System Printer	Fourteen (**14**) units • Must support multiple connectivity with USB, Ethernet, Bluetooth and Wifi options. • Must have a high print speed of up to 250 mm/sec. • Must be efficient and user-friendly: Equipped with additional LED indications for easy operation. • Must support Printer Driver for commonly used operating systems. • Must have Paper End and Cover Open sensors. • Must have LED Indicators: A. for Power, Interfaces (LAN, Wi-Fi, Bluetooth) B. for Error and/or Paper Out • Must have a built-in Feature: Advanced Paper Reduction, 180 degree rotation, backfeed guide.	
	Barcode Scanner	One hundred sixty (**160**) units • Must have a Bi-directional scanner.	

		• Must have Light Source (Laser) of at least 650nm laser diode. • Must have a Scan Rate up to 100 scans per second. • Must support multiple interfaces: RS232, USB, KBW (keyboard wedge) in one scanner. • Must have a plug and play design. • Must have a high quality 1D laser scanner — choice of triggered or Auto-Scan (continuous mode) scanning. • Voltage & Current: 5 +/-10%VDC @ 100 mA (Stand by: <35 mA). • Must support Host power or external power supply. • Must have Beeper Volume: User-selectable: three levels. • Must have Beeper Tone: User-selectable: three tones. • Must have Laser Safety of IEC Class 1.	
	RAM	Fifty (**50**) units (Random Access Memory) • Must have at least 16GB DDR 4 • Must have at least 17 cycles CL(IDD) • Must have at least 45.75ns(min.) Row Cycle Time (tRCmin) • Must have Refresh to Active/Refresh • Must have Command Time (tRFCmin) of at least 350ns(min.) • Must have Row Active Time (tRASmin) of at least 32ns(min.) • Must have UL Rating of 94 V - 0 • Must have Operating Temperature of 0°C to +85°C • Must have Storage Temperature of -55°C to +100°C • Must have Power Supply of VDD = 1.2V Typical • Must have VDDQ of at least 1.2V Typical • Must have VPP of at least 2.5V Typical • Must have VDDSPD of at least 2.2V to 3.6V • Must have On-Die termination (ODT)	

		• Must have at least 16 internal banks; 4 groups of 4 banks each • Must have Bi-Directional Differential Data Strobe • Must have at least 8 bit pre-fetch • Must have Burst Length (BL) switch on-the-fly BL8 or BC4(Burst Chop) • Must have Height of at least 1.34" (34mm), w/heatsink	
	SSD	Fifty (**50**) units Solid State Drive • Must have up to 500GB SSD capacity • Must have a SATA 6 Gb/s Interface, compatible with SATA 3 Gb/s & SATA 1.5 Gb/s interface • Must have Sequential Read of up to 560 MB/s • Must have Sequential Write of up to 530 MB/s • Must have Storage Memory of V-NAND 3 bit MLC • Must have Cache Memory of up to 512 MB Low Power DDR4 SDRAM • Must support TRIM • Must support S.M.A.R.T • Must support Encryption: AES 256-bit Encryption (Class 0),TCG/Opal, IEEE1667 (Encrypted drive) • Must support Auto Garbage Collection Algorithm	
	Web Camera	Twenty-six (**26**) units • Must have a Resolution of Full HD 1080P, 1920*1080 Pixels • Must have Lens Type of Full HD Glass Lens • Must have a Viewing Angle of at least 70 Degrees • Must have a Focus Type of Fixed Focus • Must have a Focus Range of at least 60cm and beyond • Must have a Built-in Mic of Digital HD Omni-Directional Mic. • Must have an Output Format of MJPEG	

		● Must have Frame Rate of up to 30fps ● Must support USB 2.0 ● **System Requirements:** A. Must support commonly used operating system B. Must works in USB Video Device Class (UVC) Mode ● Must support social and video calling software of the above system.	
	Network Attached Storage	Two (**2**) units **Hardware Requirement** **Processor:** ● Must support commonly used processor. ● Must have at least one (1) CPU. ● Must support eight (8) Core. ● Must support 64-bit. ● Must support 2.1 GHz (base) / 2.7 GHz (turbo) CPU frequency. ● Must support Hardware Encryption Engine. **Memory:** ● Must support System Memory of at least 8 GB DDR4 ECC UDIMM. ● Must support Memory Module Pre-installed of at least one (1) x 8 GB. ● Must support four (4) Total Memory Slots. ● Must support Maximum Memory Capacity of at least four (4) x 16 GB (64 GB). **Storage:** ● Must support at least twelve (12) Drive Bays. ● Must have a Maximum Drive Bays with Expansion Unit of at least thirty-six (36) (RX1217 x 2).	

		● Must support Compatible Drive Types 3.5" SATA HDD, 2.5" SATA SSD. ● Must have Hot Swappable Drive. **External Ports:** ● Must support at least four (4) RJ-45 1GbE LAN Port. ● Must support at least two (2) RJ-45 10GbE LAN Port. ● Must support at least two (2) USB 3.2 Gen 1 Port. ● Must support at least two (2) Expansion Port. ● Must support Infiniband Expansion Port Type. **PCIe:** ● Must support at least 2 x Gen3 x8 slots (x8 link) PCIe Expansion. **Appearance:** ● Must support 2U Form Factor (RU). ● Must support dimension Size (Height x Width x Depth) of at least 88 mm x 482 mm x 724 mm. ● Must support Weight of at least 14.5 kg. ● Must support 4-post 19" rack Rack Installation. **System Features:** ● Must have at least 80 mm x 80 mm x 4 pcs. System Fan. ● Must support Fan Speed Mode: A. Full-Speed Mode B. Cool Mode C. Quiet Mode ● Must support Easy Replacement System Fan. ● Must support Power Recovery. ● Must support at least 50.2 dB(A) Noise Level. ● Must support Scheduled Power On / O.ff. ● Must support Wake on LAN / WAN	

		● Must support 500 watts, 550 watts Power Supply. ● Must support Redundant Power Supply. ● Must support AC Input Power Voltage of at least 100 V to 240 V AC. ● Must support Power Frequency of at least 50/60 Hz, Single Phase. ● Must support Power Consumption: A. Of at least 142.5 watts (Access). B. Of at least 72.76 watts (HDD Hibernation). ● Must support British Thermal Unit: A. 485.93 BTU/hr (Access). B. 248.11 BTU/hr (HDD Hibernation). **Temperature:** ● Must support Operating Temperature of 0°C up to 35°C (32°F to 95°F). ● Must support Storage Temperature of -20°C up to 60°C (-5°F to 140°F). ● Must support Relative Humidity of 5% up to 95% RH. **Certification:** ● Must support certifications: FCC, CE, BSMI, VCCI, RCM, EAC, CCC, KC, UL. **Software Specifications** **Storage Management:** ● Must support a Maximum Single Volume Size: A. 1 PB (64 GB memory required, for RAID 6 groups only). B. 200 TB (32 GB memory required). C. 108 TB. ● Must support 256 Maximum Internal Volume Number. ● Must support SSD Read/Write Cache (Determining cache size). ● Must support SSD TRIM. ● Must support RAID Group.	

		● Must support RAID Type: A. RAID F1. B. Basic. C. JBOD. D. RAID 0. E. RAID 1. F. RAID 5. G. RAID 6. H. RAID 10. ● Must support RAID Migration: A. Basic to RAID 1. B. Basic to RAID 5. C. RAID 1 to RAID 5. D. RAID 5 to RAID 6. ● Must support Volume Expansion with Larger HDDs: A. RAID F1. B. RAID 1. C. RAID 5. D. RAID 6. E. RAID 10. ● Must support Volume Expansion by Adding a HDD: A. RAID F1. B. JBOD. C. RAID 5. D. RAID 6. ● Must support Global Hot Spare RAID Type: A. RAID F1. B. RAID 1. C. RAID 5. D. RAID 6. E. RAID 10. **File System:** ● Must support Internal Drives: Btrfs, ext4 ● Must support External Drives: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT. **File Services:** ● Must support File Protocol: SMB, AFP, NFS, FTP, WebDAV, Rsync. ● Must support at least 2,000 Maximum Concurrent SMB/AFP/FTP Connections. ● Must support at least 10,000 Maximum Concurrent SMB/AFP/FTP Connections (with RAM expansion).	

		● Must support Access Control List (ACL) Integration. ● Must support NFS Kerberos Authentication **Account & Shared Folder:** ● Must support at least 16,000 Maximum Local User Accounts. ● Must support at least 512 Maximum Local Groups. ● Must support at least 512 Maximum Shared Folder. ● Must support at least 32 Maximum Shared Folder Sync Tasks. **Hybrid Share:** ● Must support at least 15 Maximum Hybrid Share Folders. **Hyper Backup:** ● Must support Folder and Package Backup. ● Must support Entire System Backup. **Log Center:** ● Must support at least 3,000 Syslog Events per Second. **Virtualization:** ● Must support VMware ESXi 6.5 and VAAI. ● Must support 2016 and latest server operating systems ● Must be Citrix Ready. ● Must support OpenStack. **General Specifications:** ● Must support SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, Fibre Channel, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV Protocols. ● Must support Chrome, Firefox, Edge, Safari Browsers.	
V	**Security and Compliance**		
	a. The contracting parties must strictly observe the provisions of Republic Act 10173 otherwise known as the “Data Privacy Act of 2012” and all other related laws in ensuring the protection of data and information obtained under the Agreement. Failure to		**C**

	comply with the confidentiality clause shall be subject to penalties. b. Any information or document obtained in connection with the execution or implementation of the Project shall not be disclosed to any person or entity without the written consent of the DFA. The non-disclosure and confidentiality requirement in this provision must continue even after the expiration or termination of the Agreement.	
VI	**Mode of Procurement**	
	The mode of procurement shall be public bidding.	
VII	**Bidder's Qualifications**	
	1. Has been in the business for at least 15 years. 2. Must be a certified partner of the manufacturer for at least ten (10) years for the major products being offered. 3. Must submit a list of engineers or technical personnel who shall perform corrective, preventive maintenance, and calibration of the products. 4. The Contractor's technical engineers shall have the following qualifications and must be locally employed for the installation of all equipment: ● At least five (5) Certified Network Engineer ● At least five (5) networking associates ● At least two (2) Certified Network Specialists ● At least one (1) Certified Network Professional ● At least one (1) PMP (Project Management Professional). 5. The Contractor's technical engineers mentioned above must submit the following proof: ● Certified True Copy of Certificate ● Certified True Copy of Company ID ● Certified True Copy of Certificate of Income Tax Return ● Certified True Copy of Certificate of Employment 6. Must submit original brochures or manuals which contain all technical specifications required by the bidding documents in the English language. 7. Must submit a list of locations and contact numbers of the service centers in the Philippines responsible for the warranty of the products supplied. 8. Must submit a certification from the winning bidder that the bidder shall be responsible for the notification, transportation, delivery, installation,	

	commissioning, and testing to be provided at no cost to the government. 9. Must submit a certification from the winning bidder that the bidder shall guarantee that the delivery of the product and all accessories shall be within the period required by the Bids and Awards Committee (BAC). 10. Must submit the proposed costing of preventive maintenance for sophisticated equipment and consumables or accessories. 11. Must submit a certificate of compliance or equivalent certification from the winning bidder showing the proof of compliance with the TOR.	
VIII	**Maintenance and Technical Support**	
	a. During the project implementation, the contractor shall provide highly technical personnel to deliver service and support to the production, staging, and transition of the infrastructure to the DFA Team and with regard to any related problems that may occur. They will sign a Non-Disclosure Agreement which will be submitted to the Department prior to the commencement of the service. b. 24/7 phone, chat, and email support shall be available, especially during configuration. c. The Contractor shall immediately inform the Department of breaches, attacks, or other forms of cyber threats/activities that may contribute to disclosure of any confidential information. The Contractor shall immediately undertake necessary actions to address such breach, attack, or other form of cyber threat/activity. d. During the project implementation, the contractor shall provide highly technical personnel to bring forth necessary training to DFA personnel who will be handling the infrastructure at no cost to the DFA. e. The Contractor shall provide one year warranty of the tools and equipment and one year maintenance support services or at the duration of the contract. f. The equipment to be provided must be in line and compatible with the department's current projects and equipment to allow interoperability.	

IX	**Duration and Delivery**	
	a. DURATION: The contract shall be valid for a period of one (1) year, commencing from the date of successful delivery, configuration and deployment of the equipment and acceptance by the DFA . b. DELIVERY: The Contractor shall deliver and setup/configure the network and cybersecurity equipment and tools within thirty(30) working days from the receipt of the Notice to Proceed (NTP) at DFA Aseana and Consular Offices stated. c. The DFA shall have the right to inspect and/or test the delivered items to confirm conformity with the requirements. All of the equipment and peripherals must be brand new and not refurbished. d. Inspection and Acceptance Report from the DFA shall form part of the payment process as proof of compliance of the supplier on the requirements herein.	
X	**Payment**	
	Payments shall be made thirty (30) working days upon full implementation of the Solutions and receipt of OCA-Authentication of the invoice Provisional Acknowledgement Receipt, and complete documentary requirements through List of Due and Demandable Accounts Payable (LDDAP). The list of documentary requirements needed for payment will be provided by the Office of Financial Management Services-Financial Resources Management Division (OFMS-FRMD) upon signing of the contract. All payments shall be inclusive of Value Added Tax (VAT) and other lawful charges.	

Conformé:

[Signature/s]
[Name of Bidder's Authorized Representative/s]
[Position]
[Date]

Official	Initial	Date
Executive Director	**On official business**	
Auth Dir	MCA	22 Oct 2024
AO OCA	MIR	22Oct2024
Finance	gss	21 Oct 2024
Proc Head	cdmb	21 Oct 2024
Action Officer	rrg	21 Oct 2024
End-User	rnlm	21 Oct 2024