REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

BIDS AND AWARDS COMMITTEE FOR DICTBAC

Supplemental Bid Bulletin No. 1

SUPPLY AND DELIVERY OF E-LEARNING EQUIPMENT AND SOFTWARE

Bid Reference No. DICTBAC-2019-006

ORIGINAL PROVISION	**AMENDED PROVISION**
Section VII. Technical Specifications	
18.1 The Winning Bidder must provide two (2) days LMS Training, comprehensive training on installation, configuration administration and troubleshooting for DICT Employees. The DICT employees in return will train the selected school representatives.	18.1 The winning bidder must provide two (2) Days ***E-Learning software training***, for DICT employees. The DICT employees in return will train the selected school representatives.

All terms, conditions and instructions to bidders specified in the Bidding Documents inconsistent with this Bid Bulletin are hereby superseded and modified accordingly.

Please use the following forms attached in this Supplemental Bid Bulletin:

- Revised Technical Specifications as of 8 May 2019

For information and guidance of all concerned.

Issued this 8th day of May 2019.

(Original Signed)
IVIN RONALD D.M. ALZONA
Chairperson, DICTBAC

Supply and Delivery of E-Learning Equipment and Software
DICTBAC-2019-006

REVISED TECHNICAL SPECIFICATIONS
AS OF 8 May 2019

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).

MINIMUM SPECIFICATIONS	STATEMENT OF COMPLIANCE
1. E-Classroom for Grades 4 to Grades 6	
PC Workstation for Teachers The Contractor must supply PC Workstation that has the following specifications	
1.2 Processor: Intel Core i5-8400 (6 Core/6T up to 4.0Ghz/65W) or AMD Ryzen 5 Pro 2400G (4 Core/8T up to 3.9 Ghz/65W)	
1.3 Memory: 16Gb DDR4 2666Mhz	
1.4 Storage: 1Tb 7200rpm SATA	
1.5 Display port: 1xDisplay Port and 1xVGA port or 1x HDMI port or 1xDisplay port	
1.6 LAN Ports: 1x1Gb/s RJ45	
1.7 Networking: Integrated Ethernet LAN 10Mb/100Mb/1000Mb, Wireless AC 2x2 802.11ac with Bluetooth 4.0	

1.8 Audio: 1 x 3.5mm audio-mic combo jack, 1 x 3.5mm line- out, Internal audio speaker	
1.9 Power: External atleast 200 watts up to 85% efficient Power Supply (80Plus Bronze)	
1.10 Operating System: Windows 10 Pro (64Bit)	
1.11 Warranty: 3 years	
1.12 Certifications: EcoLabel, Energy Star 6.1, EPEAT, EU RoHS	
2. Thin Client PCs	
The Contractor must supply Thin Client PCs that has the following specifications:	
2.1 Processor: Quad Core 1.5ghz, up to 2.5ghz burst	
2.2 Graphics: Built in Intel UHD 600/605 Graphics Controller support up to 2 monitors (2@ 3840x2160@60Hz)	
2.3 Memory: 8GB DDR4 2400MHz, 2 SODIMM Slot	
2.4 Storage: 128GB SSD	
2.5 Chassis: Slim Type	
2.6 USB Slots: 3xUSB 2.0 (2 front, I Internal), 6xUSB 3.0 (1 front, 4 rear, 1 internal),	
2.7 Display port: 2xDisplay Port 1.2a	
2.8 LAN Ports: 1x1Gb/s RJ45	
2.9 Other Ports : 1xSerial Port, 1xSmartcard/CAC reader (optional front integrated)	

2.10 Security: Built-in chassis security lock slot, Trusted Platform Module (TPM) 2.0	
2.11 Networking: Integrated Ethernet LAN 10Mb/100Mb/1000Mb, Wireless AC 2x2 802.11ac with Bluetooth 4.0 external antenna	
2.12 Audio: 1 x 3.5mm audio-mic combo jack ; 1 x 3.5mm audio out, Internal business audio speaker	
2.13 Power: External 65watts AC Adapter, Worldwide auto-sensing 100-240VAC, 50-60Hz; Power consumption:4.6 watts (idle w/RJ45)	
2.14 Orientation: Vertical	
2.15 Dimension: Height 184mm x Width 35.6mm x Depth 184mm	
2.16 Net Weight: 1.2kg (2.65lbs)	
2.17 Temperature Range: Ambient Operating: 32° to 104°F (0° to 40°C), Storage: -40° to 149° (-40° to 65°C)	
2.18 Humidity: 20% to 80% condensing, 20% to 95% non-condensing	
2.19 Warranty: 3 years	
2.20 Certifications: EcoLabel, Energy Star 6.1, EPEAT, WEEE, EU RoHS	
3. LED Monitor	
The Contractor must supply LED Monitor that has the following specifications:	
3.1 Viewable image size - 54.61 cm (21.5 inches)	

3.2 Active display area (Horizontal) - 476.06 mm (18.74 inches)	
3.3 Active display area (Vertical) - 267.79 mm (10.54 inches)	
3.4 Monitor Connectivity : VGA and Display port	
3.5 Maximum Resolution - Full HD 1920 x 1080 at 60 Hz	
3.6 Aspect ratio – 16:9	
3.7 Backlight – LED	
3.8 Viewing Angle - 160° / 170°	
3.9 Panel Technology - TN (active matrix –TFT LCD), anti-glare	
3.10 BFR/PVC-free monitor (excluding external cables) with arsenic-free glass and mercury-free LED panel.	
3.11 Environmental compliance - ENERGY STAR®, EPEAT® Gold3 , TCO Certified Displays, CECP, China Energy Label, RoHS	
4.Networking Equipment	
The Contractor must supply one (1) LAN Switch that has the following specifications:	
4.1 Hardware: 24x 1GbE + 4x 10GbE SFP+ fixed ports, Stacking, IO to PSU airflow	
4.2 Power: AC with Power cord	
4.3 Warranty: 3 years	
5. Management Software for Workstation and ThinClients	

5.1 The Contractor must supply a platform(s) and/or software(s) that have the following features:	
5.2 See everything students see on their computers	
5.3 Share Teacher's screen to any PC connected to it	
5.4 Lock the screen of any PC connected to it	
5.5 Reboot or Shutdown any PC connected to it	
5.6 Should have built in support for LDAP/AD	
5.7 Should have the ability to log out users	
5.8 Should have the ability to allow the teacher's PC to send messages to all or to a specific PC/Thin Clients	
5.9 Should have a demonstration mode. During this mode, the teacher's screen content will be displayed in full screen. Logged-in users/students cannot use their computers for other tasks because all input devices are locked.	
5.10 Should have a screenshot feature that allows teachers to save the screen content to image files	
6.E-Learning Application Electronic Resources for Math and Science	
6.1 The Contractor must have platform(s) and/or reader(s) that contain the following resources and/or have the following features	
6.2 Content 6.2.1 contains eLessons for El Filibusterismo, Noli Me Tangere, Ibong Adarna, and Florante at Laura with each lesson providing the following user experience: ▪ animated content	

▪ navigation tools ▪ annotation on words that may not be familiar to users 6.2.2contents that are secured by copyright ownership and exclusive contract	
6.3 Accessibility 6.3.1Can be accessed offline thru an application that does the following: ▪ supports iOS and Android devices ▪ ensures the security of contents and user identity by allowing the users to only access the contents upon successfully connecting to the server URL https://mcourser.ph ▪ lets users change the look and feel of the application by choosing between Windows 2000 or latest or Windows XP themes ▪ supports contents having HTML format ▪ supports contents having various multimedia elements such as audio files, videos, and animations that can be viewed for offline use 6.3.2 Can be accessed online thru a dedicated online platform1 that does the following: ▪ supports desktop computers having Windows 7 or latest operating system ▪ supports OS X desktop computers ▪ supports contents with external links and have various multimedia elements such as audio files, videos, and animations 6.3.3 The platform is subject to system upgrades, which aims to improve the user interface and user experience.	
7. Anti-Virus Application for PC Workstation	
7.1 Ant-Virus/Anti-Spyware 7.1.1 Platforms supported: • Windows/Vista/8/10/2008/RBS2011/2012, • MacOS, Linux 7.1.2 Rootkit detection and cleanup	

7.2 Host Intrusion Prevention System (HIPS) • Behavior of code is analyzed before it runs and is prevented from running if it is considered to be Suspicious or malicious. Inter-check Technology. Runtime detection intercepts threats that cannot be detected before execution.	
7.3 Enterprise Console • A single, automated console for Windows, Mac, Linux and virtualized platforms centrally deploys and manage antivirus and client firewall protection; intrusion prevention; web protection; patch assessment; encryption; data, device and application control; and assessment and control.	
7.4 Runtime Protection • Monitor and block suspicious behavior like registry or critical Windows system files modification • Protection against buffer-overflow	
7.5 Client Firewall • Platforms supported: Windows 7/8/10 • ntegrated to Antivirus • Supported stealth mode operation • Prevents application hijacking and checksum-based • Exclusion • Location-aware firewall so different firewall policies can be applied when Antivirus is within or outside the company network • A centrally managed client firewall designed for the enterprise environment blocks worms, stops hackers and prevents intrusions.	
7.6 Application Control • Selectively authorize or block legitimate applications that impact network bandwidth, system availability, and user productivity • Vendor-managed list to offload the administrator from monitoring new applications or versions • List should include browser plug-ins, desktop search tools, email client, encryption tools, file sharing applications, games, instant messaging, internet browsers, mapping apps, media player, online storage, proxy apps, remote management tools, security tools, toolbars, virtualization, and voice over IP software	
7.7 Device Control • Control the use of removable storage, optical media drives, floppy drives, and wireless, modems,Bluetooth, and Infrared devices	

• Should be port-agnostic and should support whatever port is used to connect the device like USB, FireWire, SATA, and PCMIA interfaces • Ability to run in alert-only mode providing administrators a view of the device usage across the network • Ability to set storage devices in "Read-Only mode" to prevent data from being written • Prevents wireless bridging – ex. Disables wireless when Ethernet is connected • Supports device instance and model exceptions • A single Antivirus agent for Windows that detects viruses, spyware and adware, rootkits and suspicious files and behavior. It monitors the transfer of sensitive data off the network and blocks malicious and inappropriate websites. The agent also controls use of removable storage devices and unauthorized applications across multiple platforms • Ability to control required access for MTP/PTP devices.	
7.8 Live Web Protection • Live in-the-cloud lookups check database of millions of compromised sites	
7.9 System Protection • System Protection is a component of the Antivirus protection software providing coordination between detection engines and performing lookups as required to ensure the most up to date protection	
7.10Download Reputation • Download Reputation is a feature of the Windows Antivirus product that checks files downloaded from some internet browsers against a database of files	
7.11 Live Malware Lookup • Instantly checks the reputation of suspicious checksums and file meta data; use an extensive in-the-cloud database of known good and bad reputation data and to improve proactive detection, reducing reliance on updating	
7.12 Malicious Traffic detection • Malicious Traffic Detection is a component that will monitor HTTP traffic for signs of connectivity to known bad URLs such as Command and Control servers.	
7.13 Web Control • Provides protection, control for endpoint machines that are located, or roam, outside your corporate network. Web filtering on 14 essential site categories on user machines.	

7.14 Enhanced Runtime behavior detection • Should detect writing to the registry, calling a Windows API; looks at pre-execution analysis results source of files, packers used, other suspicious rule triggers • Should be Integrated into existing Antivirus agent • with no Antivirus configuration required • Prevents users or malicious applications from making changes to configuration of the anti-virus. Protects files, registry keys, services, and processes.	
7.15 Central Management • Management Console Platform support: Microsoft Server 2008/2012/2016 • Single management console for Windows, Mac, Linux computers • Ability to perform cleanup centrally from the console • Ability to authorize files centrally from console	
7.16 Audit Logging Support • Delivering (among other features) support for audit logging. It enables IT managers to run detailed reporting on management console activity for regulatory compliance, security audits and forensic analysis.	
7.17 Policy-based • Role-based administration privileges with the ability to assign management to estates and sub-estates • Centralized policy enforcement relating to Updating, Antivirus and HIPS, Client Firewall, Application control, Device control, Data control, Patch assessment, Web control, Anti-ransom ware, Anti-exploit prevention	
7.18 Active Directory support • Automatic computer discovery and synchronization with AD structure • Automatic installation of newly discovered computers	
7.19 Location Roaming • Intelligent updating for roaming laptops where updates are performed from a best update location and updating does not rely solely on the primary and secondary update locations specified in the Antivirus updating policy. 7.20 Failsafe updating • Multiple sources of update with automatic Failover • Bandwidth throttling support for low-speed network links	

7.21 Signature Updates • Small update size with an average of 50kb per signature update • Ability to check for updates as often as every 10 minutes • Separate schedule for signature and software updates	
7.22 Reporting Interface • Reporting Interface and Reporting Log Writer provide the components that allow third-party applications to access Enterprise Console threat and event data.	
7.23 Patch Assessment • Scans and identifies computers missing critical patches for vulnerabilities commonly targeted by threats.	
7.24 Home Use • Your employees are allowed to use the Licensed Product at home on a single workstation provided that you are responsible for support and the distribution of Upgrades and Updates of such licenses.	
8. **E-Classroom for Literacy, Reading and Research**	
8.1 Content • shows an assemblage of at least 5,000 curriculum-aligned ebooks in the primary collection • (i.e., approximately 10% of the total collection comes in two languages, Spanish and English) • provides users with a wide range of high-quality reading resources, which are wired to the user's lexile score, grade level, and interests • contains authentic texts, which consist of illustrated and picture books, graphic novels, literary nonfiction, and informational texts among others • supports reading scaffolding thru narrated audio and text highlighting, either word or sentence • allows students to check on unfamiliar words using the platform's dictionary feature • checks user's understanding of the ebook read by answering a quiz with approximately 3 to 5 items at the end of selected books	
8.2 Accessibility 8.2.1 can be accessed offline thru an application that does the following: • supports iOS and Android devices • ensures the security of contents and user identity by allowing the users to only access the contents thru the application	

• allows the downloading of up to 20 titles2 at a time for offline reading 8.2.2 can be accessed online thru a dedicated online platform1 that does the following: • supports desktop computers having Windows 7 or latest operating system • supports OS X desktop computers • allows single delivery of contents • availability of the following reports3 (using the teacher account): • Core Report – provides general idea on students' activity and progress • Quizzes – provides an idea on which students answered the end-of-the-book short quiz and how they scored • Reading Habits – provides an idea on what time of the day students usually take time to read and how much they are reading in and out of school • Timeline - shows patterns and trends over time on a variety of the platform's metrics. Learn more than just what students have done – uncover where they're going • Most Popular Books – shows the type of books students are reading most of the time, which can help teachers design more effective projects and recommend books the students are sure to love. • Most Popular Categories – shows the student's most selected book categories (e.g., adventure, monsters and mysteries, etc.) • Reading Details – allows teachers to delve a little deeper into the students' reading data • Extended User Activity – shows the student's current platform activity prior to the start of the school year, which aims to see an overview of student progress throughout the year • On-target Lexile Reading – shows relation between the student's Lexile scores and the type of books he/she is reading.	
9. PC Workstation for Librarian	
9.1 The Contractor must supply 50 PCs that has the following specifications	
9.2 Processor: Intel Core i5-8400 (6 Core/6T up to 4.0Ghz/65W) or AMD Ryzen 5 Pro 2400G (4 Core/8T up to 3.9 Ghz/65W)	
9.3 Memory: 16Gb DDR4 2666Mhz	
9.4 Storage: 1Tb 7200rpm SATA	
9.5 Display port: 1xDisplay Port and 1xVGA port or 1x HDMI port or 1xDisplay port	
9.6 LAN Ports: 1x1Gb/s RJ45	

9.7 Networking: Integrated Ethernet LAN 10Mb/100Mb/1000Mb, Wireless AC 2x2 802.11ac with Bluetooth 4.0	
9.8 Audio: 1 x 3.5mm audio-mic combo jack, 1 x 3.5mm line-out, Internal audio speaker	
9.9 Power: External atleast 200 watts up to 85% efficient Power Supply (80Plus Bronze)	
9.10 Operating System: Windows 10 Pro (64Bit)	
9.11 Warranty: 3 years	
9.12 Certifications: EcoLabel, Energy Star 6.1, EPEAT, EU RoHS	
10 **Management Software for Library PCs**	
10.1 The Contractor must supply a platform(s) and/or software(s) that have the following features:	
10.2 See everything students see on their computers	
10.3 Share Teacher's screen to any PC connected to it	
10.4 Lock the screen of any PC connected to it	
10.5 Reboot or Shutdown any PC connected to it	
10.6 Should have built in support for LDAP/AD	
10.7 Should have the ability to log out users	

10.8 Should have the ability to allow the teacher's PC to send messages to all or to a specific PC/Thin Clients	
10.9 Should have a demonstration mode. During this mode, the teacher's screen content will be displayed in full screen. Logged-in users/students cannot use their computers for other tasks because all input devices are locked.	
10.10 Should have a screenshot feature that allows teachers to save the screen content to image files	
11 **PC Workstation for Students**	
11.1 The Contractor must supply 1 PC that has the following specifications:	
11.2 Processor: Intel Core i5-8400 (6 Core/1Mb/6T up to 4.0Ghz/65W) or AMD Ryzen 5 Pro 2400G (4 Core/8T up to 3.9 Ghz/65W)	
11.3 Memory: 16Gb DDR4 2666Mhz	
11.4 Storage: 1Tb 7200rpm SATA	
11.5 Display port: 1xDisplay Port and 1xVGA port or 1x HDMI port or 1xDisplay port	
11.6 Display port: 1xDisplay Port and 1xVGA port or 1x HDMI port or 1xDisplay port	
11.7 Networking: Integrated Ethernet LAN 10Mb/100Mb/1000Mb, Wireless AC 2x2 802.11ac with Bluetooth 4.0	
11.8 Audio: 1x 3.5mm audio-mic combo jack, 1 x 3.5mm line-out, Internal audio speaker	
11.9 Power: External atleast 200 watts up to 85% efficient Power Supply (80Plus Bronze)	
11.10 Operating System: Windows 10 Pro (64Bit)	
11.11 Warranty: 3 years	
11.12 Certifications: EcoLabel, Energy Star 6.1, EPEAT, EU RoHS	

12. LED Monitor	
12.1 The Contractor must supply LED Monitor that has the following specifications:	
12.2 Viewable image size - 54.61 cm (21.5 inches)	
12.3 Active display area (Horizontal) - 476.06 mm (18.74 inches)	
12.4 Active display area (Vertical) - 267.79 mm (10.54 inches)	
12.5 Monitor Connectivity: VGA and Display port	
12.6 Maximum Resolution - Full HD 1920 x 1080 at 60 Hz	
12.7 Aspect ratio – 16:9	
12.8 Backlight – LED	
12.9 Viewing Angle - 160° / 170°	
12.10 Panel Technology - TN (active matrix –TFT LCD), anti-glare	
12.11 BFR/PVC-free monitor (excluding external cables) with arsenic-free glass and mercury-free LED panel.	
12.12 Environmental compliance - ENERGY STAR®, EPEAT® Gold3 , TCO Certified Displays, CECP, China Energy Label, RoHS	
13 Wireless Access Point for School Library	
13.1 The Contractor must supply Wireless Access Point that support the following specifications:	

13.2 Ethernet Support - 10/100/1000	
13.3 802.11ac Wave 2	
13.4 3x3 Wave 2 802.11ac technology with MU-MIMO capability and 3 spatial streams	
13.5 Software configurable radio for dual 5 GHz operation	
13.6 Built-in Bluetooth Low Energy for iBeacon/ other beacon technologies	
13.7 IoT readiness with USB port	
13.8 Full performance with IEEE 802.3af power	
13.9 Trusted Platform Module (TPM) – Hardware-based key storage and encryption	
13.10 RF-IQ antenna and radio technology	
13.11 Guest access - Supported	
14. Anti-Virus Application for PC Workstation	
14.1 Ant-Virus/Anti-Spyware 14.1.1 Platforms supported: • Windows/Vista/8/10/2008/RBS2011/2012, • MacOS, Linux 14.1.2 Rootkit detection and cleanup	
14.2 Host Intrusion Prevention System (HIPS) • Behavior of code is analyzed before it runs and is prevented from running if it is considered to be Suspicious or malicious. Inter-check Technology. Runtime detection intercepts threats that cannot be detected before execution.	
14.3 Enterprise Console • A single, automated console for Windows, Mac, Linux and virtualized platforms centrally deploys and manage antivirus and client firewall protection; intrusion prevention; web protection; patch assessment;	

encryption; data, device and application control; and assessment and control.	
14.4 Runtime Protection • Monitor and block suspicious behavior like registry or critical Windows system files modification • Protection against buffer-overflow	
14.5 Client Firewall • Platforms supported: Windows 7/8/10 • Integrated to Antivirus • Supported stealth mode operation • Prevents application hijacking and checksum-based • Exclusion • Location-aware firewall so different firewall policies can be applied when Antivirus is within or outside the company network • A centrally managed client firewall designed for the enterprise environment blocks worms, stops hackers and prevents intrusions.	
14.6 Application Control • Selectively authorize or block legitimate applications that impact network bandwidth, system availability, and user productivity • Vendor-managed list to offload the administrator from monitoring new applications or versions • List should include browser plug-ins, desktop search tools, email client, encryption tools, file sharing applications, games, instant messaging, internet browsers, mapping apps, media player, online storage, proxy apps, remote management tools, security tools, toolbars, virtualization, and voice over IP software	
14.7Device Control • Control the use of removable storage, optical media drives, floppy drives, and wireless, modems,Bluetooth, and Infrared devices • Should be port-agnostic and should support whatever port is used to connect the device like USB, FireWire, SATA, and PCMIA interfaces • Ability to run in alert-only mode providing administrators a view of the device usage across the network • Ability to set storage devices in "Read-Only mode" to prevent data from being written • Prevents wireless bridging – ex. Disables wireless when Ethernet is connected • Supports device instance and model exceptions • A single Antivirus agent for Windows that detects viruses, spyware and adware, rootkits and suspicious files and behavior. It monitors the transfer of sensitive data off the network and blocks malicious and inappropriate websites. The agent also controls use of removable storage devices and unauthorized applications across multiple platforms	

• Ability to control required access for MTP/PTP devices.	
14.8 Live Web Protection • Live in-the-cloud lookups check database of millions of compromised sites	
14.9 System Protection • System Protection is a component of the Antivirus protection software providing coordination between detection engines and performing lookups as required to ensure the most up to date protection	
14.10 Download Reputation • Download Reputation is a feature of the Windows Antivirus product that checks files downloaded from some internet browsers against a database of files	
14.11Live Malware Lookup • Instantly checks the reputation of suspicious checksums and file meta data; use an extensive in-the-cloud database of known good and bad reputation data and to improve proactive detection, reducing reliance on updating	
14.12 Malicious Traffic detection • Malicious Traffic Detection is a component that will monitor HTTP traffic for signs of connectivity to known bad URLs such as Command and Control servers.	
14.13 Web Control • Provides protection, control for endpoint machines that are located, or roam, outside your corporate network. Web filtering on 14 essential site categories on user machines.	
14.14Enhanced Runtime behavior detection • Should detect writing to the registry, calling a Windows API; looks at pre-execution analysis results source of files, packers used, other suspicious rule triggers • Should be Integrated into existing Antivirus agent • with no Antivirus configuration required • Prevents users or malicious applications from making changes to configuration of the anti-virus. Protects files, registry keys, services, and processes.	
14.15 Central Management • Management Console Platform support: Microsoft Server 2008/2012/2016	

• Single management console for Windows, Mac, Linux computers • Ability to perform cleanup centrally from the console • Ability to authorize files centrally from console	
14.16 Audit Logging Support • Delivering (among other features) support for audit logging. It enables IT managers to run detailed reporting on management console activity for regulatory compliance, security audits and forensic analysis.	
14.17Policy-based • Role-based administration privileges with the ability to assign management to estates and sub-estates • Centralized policy enforcement relating to Updating, Antivirus and HIPS, Client Firewall, Application control, Device control, Data control, Patch assessment, Web control, Anti-ransom ware, Anti-exploit prevention	
14.18 Active Directory support • Automatic computer discovery and synchronization with AD structure • Automatic installation of newly discovered computers	
14.19 Location Roaming • Intelligent updating for roaming laptops where updates are performed from a best update location and updating does not rely solely on the primary and secondary update locations specified in the Antivirus updating policy.	
14.20 Failsafe updating • Multiple sources of update with automatic Failover • Bandwidth throttling support for low-speed network links	
14.21Signature Updates • Small update size with an average of 50kb per signature update • Ability to check for updates as often as every 10 minutes • Separate schedule for signature and software updates	
14.22 Reporting Interface • Reporting Interface and Reporting Log Writer provide the components that allow third-party applications to access Enterprise Console threat and event data.	
14.23 Patch Assessment • Scans and identifies computers missing critical patches for vulnerabilities commonly targeted by threats.	

14.24 Home Use • Your employees are allowed to use the Licensed Product at home on a single workstation provided that you are responsible for support and the distribution of Upgrades and Updates of such licenses.	
15. **Web Isolation Software for PC**	
15.1 **Web Isolation Platform General Requirements**	
15.2 The proposed Web Isolation Platform shall include the following sub-systems:	
15.3Technology - Web Isolation Platform Cloud-base service	
15.4 Services - Professional Services for Project Management, Deployment, UAT and Systems Documentation	
15.5 The proposed Web Isolation Platform shall be a high performance, scalable and flexible cloud-base only, purpose-built solution that allows growth dynamically without any limitation. Scalability shall be achieved without the need to make architecture changes or without the need to invest in third party device to scale up. System that requires the use of hybrid setup consisting of on-premise appliance, software, agent, cloud analysis service, VDI technology and creation of airgap network that separate the user network from the Internet will NOT be considered.	
15.6 The proposed Web Isolation Platform shall be pure cloud base solution with the ability to support at least 5000 users as a subscription service.	
15.7 The proposed Web Isolation Platform shall protect enterprises from cyber-attacks by isolating and executing all web content in the proposed Isolation Platform, away from the endpoint, eliminating malware before it can reach user devices.	
15.8 The proposed Web Isolation Platform shall be using signatureless threat Isolation technique as its core technology without relying in any form of signatureless detection engine (e.g. sandbox) or without using any signature base engine (e.g. IPS, secure web gateway etc.) to eliminate the risk of web-borne malware reaching user devices via compromised or malicious web sites, email or documents.	
Deployment Requirements	

15.9 The proposed Web Isolation Platform shall support Explicit Proxy and Proxy Chaining modes.	
15.10 The proposed Web Isolation Platform shall be a proxy-compatible device and can be easily deployed within an existing proxy environment with proxy-chaining capability.	
15.11 The proposed Web Isolation Platform shall support the hosting of the PAC file on behalf of the customer.	
15.12 The proposed Web Isolation Platform hosted PAC file shall customization of the PAC file to allow host, domains and IP address/subnet to be bypass from the cloud base Web Isolation Platform.	
15.13 The proposed Web Isolation Platform shall support hosting of multiple customized PAC file on the same portal where different PAC file can be deployed to different group of users.	
Web Isolation Requirements	
15.14 The proposed Web Isolation Platform shall not be a detection or classification technology. It shall meet the following isolation requirement. • End-user web session and all active content (e.g. Java, Flash, etc.), whether good or bad, shall be fully executed and contained in an Isolation Platform. • Only safe, malware-free rendering information is delivered to the user's endpoint. • No active content, including any potential malware shall leave the isolation platform. • In the proposed isolation model, malware has no path to reach an endpoint, and legitimate content needn't be blocked in the interests of security. • Administrators can open up more of the Internet to the end-user while simultaneously eliminating the risk of attacks. • The proposed Web Isolation Platform shall execute all web content, including Java, Flash and other common sources of malware occurs in the proposed Isolation Platform in real time without requiring any form of analysis and there shall not be a victim zero for new unknown zero-day threat. Only malware-free rendering information is sent to the native browser on the user's endpoint, without any client software or plug-ins, so users enjoy a seamless and transparent experience with no perceivable latency.	

• The proposed Web Isolation Platform shall use isolation-centric approach that splits web browsing and document retrieval between the user's device and an isolated, Disposable Virtual Container (DVC) away from the endpoint. All risky code shall only be executed in the isolated DVC and never reaches the endpoint. Only safe render data is sent to the user's browser. • The proposed Web Isolation Platform shall support Virtual Shredding that quickly discards completed Dynamic Virtual Container to eliminate infection persistence.	
15.15 The proposed Web Isolation Platform shall be based on the following additional specifications: • No client software or plug-ins required to be deployed to utilize the service • Transparent user experience • No false positives or false negatives • Works with any end-user device, OS and browser • Integrates easily with existing web security gateways • Equipped with integrated Anti-virus and Sandboxing solution in addition to the isolation technology where isolation remains the core requirement.	
15.16 The proposed Web Isolation Platform shall support transparent remoting technology using a technique known as Document Object Model (DOM) mirroring to provide transparent adaptive clientless rendering user experience by mirroring only the benign portions of the isolated browser's DOM tree on the endpoint browser.	
15.17 The proposed Web Isolation Platform shall support Adaptive Transcoding that enables the selection of remoting strategy at DOM element granularity, whereby non-active safe elements are left as is and active unsafe elements are either dropped altogether or are replaced with a safe, transcoded variant that is best suited for the element's media type.	
15.18 The proposed Web Isolation Platform shall support rendering and workflow offloading to prevent website scrolling from being impacted. E.g. How the proposed System deal with quick scrolling up/down or fine grain movements on objects in a page.	
15.19 The proposed Web Isolation Platform shall support semantically-aware rendering that enables the client browser to apply natively-available fonts and UI widgets to the final rendered result for a truly native look and feel regardless of endpoint browser or platform.	

15.20 The proposed Web Isolation Platform shall preserve native end user web browsing experience and avoids disruption to work flow operations such as continue support of copy-paste, find-replace, and printing functionality even though content is loaded in the isolation platform.	
15.21 The proposed Web Isolation Platform shall allow end user to print content from the isolation platform render to the end user browser without causing pixilation or difference in the displayed web content.	
15.22 The proposed Web Isolation Platform shall not cause pixilation to the web content and shall not introduce increase in bandwidth to render the isolated content back in video format to the end user.	
15.23 The proposed Web Isolation Platform shall support integrated SSL Decryption functionality, providing isolation for both clear-text (HTTP) and SSL-encrypted (HTTPS) Web content without requiring to deploy an external third-party SSL decryption tools. This function shall be available as a borderless solution where SSL-encrypted can be isolated regardless of where and user is connected to the Internet.	
Document Isolation Requirement	
15.24 The proposed Web Isolation Platform shall protect end user from cyber-attacks by isolating and rendering the common document types in real time; including PDF, Word, Excel and PowerPoint Documents; in the cloud-base Web Isolation Platform, away from endpoints, eliminating malware before it can reach end user devices.	
15.25 The proposed Web Isolation Platform shall only present safe, malware-free rendering information where end users enjoy a safe, transparent viewing experience using their native browser, without the need to download or install endpoint software or plugins.	
15.26 The proposed Web Isolation Platform shall provide configurable policy to allow end users to download a clean copy of the document in "safe" PDF versions, with all active content removed without requiring to use any form of signature or heuristic engine to remove the malware embedded in the weaponized document.	
15.27 The proposed Web Isolation Platform shall provide configurable policy to allow end users to download the original documents for designated users.	

15.28 The proposed Web Isolation Platform shall preserve native end user web browsing experience and avoids disruption to work flow operations such as continue support of copy-paste, find-replace, and printing functionality even though document is loaded in the isolation platform.	
15.29 The proposed Web Isolation Platform shall allow end user to print content from the isolation platform render to the end user browser without causing pixilation or difference in the displayed web content	
End-user Authentication Requirements	
15.30 The proposed Web Isolation Platform shall support the ability to authenticate the end user before granting access. User authentication shall support the following method to authenticate the user: • Creation of local user on the web isolation platform • Using SAML 2.0 to provide a standards-based single sign-on capability leveraging existing authentication services	
15.31 The proposed Web Isolation Platform shall support Single sign-on functionality by integrating with existing on-premise Microsoft Active Directory system using Active Directory Federation Services (ADFS) 2.0 or via a cloud-based solution, such as OneLogin, Okta, Ping or other Identity-as-a-Service (IDaaS) provider using SAML 2.0.	
15.32 The proposed Web Isolation Platform using SAML 2.0 for single sign-on shall authenticate users without any requirement for user creation, user credential management, or direct access into the corporate network. Passwords shall never leave the Identity Provider and shall use a cryptographically signed token to pass to the Web Isolation Platform for user authorization.	
SSL Traffic Inspection Requirement	
15.33The proposed Web Isolation Platform shall support integrated SSL Decryption functionality, providing isolation for both clear-text (HTTP) and SSL-encrypted (HTTPS) Web content without requiring to deploy an external third-party SSL decryption tools.	
15.34 The proposed Web Isolation Platform SSL (HTTPS) traffic inspection function shall be available as a borderless solution where SSL-encrypted traffic can be isolated regardless of where and user is connected to the Internet	

15.35 The proposed Web Isolation Platform shall allow flexible configurable SSL policy not to perform SSL inspection by the following options: • URL Category • Source IP or IP Subnet • Destination IP or IP Subnet	
Borderless Prevention & Failover Requirement	
15.36 The proposed Web Isolation Platform shall provide borderless protection cloud base service to the end user, enforcing the same level of web isolation threat prevention regardless of where the user is accessing from (e.g. LAN, Home and Free Wi-Fi etc.).	
15.37 The proposed Web Isolation Platform borderless protection cloud base service shall have data centers throughout the world and is mandatory to have major data center, inclusive of all data center mentioned, in Singapore, Australia, Japan, Ireland, Germany, both East and West Coast of USA as part of offering.	
15.38 The proposed Web Isolation Platform shall be geo-location aware, allowing end user to initiate connections from different locations / geographical regions and automatically direct the end user traffic to their nearest available web isolation platform data center (for example, traveling workers or global office locations). This mandatory requirement is to ensure minimum routing latency in the service and to avoid web traffic being backhaul to a single data center. For example, end user web traffic in Singapore is routed through Singapore data center while Germany user is routed through Germany data center.	
15.39 The proposed Web Isolation Platform shall automatically steer the traffic to the closest data center by using latency-based routing technology.	
15.40 The proposed Web Isolation Platform shall have redundant components at each of the data centers to ensure service availability before failover to a different data center.	
15.41 The proposed Web Isolation Platform shall in the event of a failure at any of the data center locations, the above latency-based routing technology shall re-route the traffic to a different location to ensure service availability.	
Administrative and Reporting Requirements	

15.42The proposed Web Isolation Platform shall have configurable interfaces in the form of Graphical User Interface accessible by administrator through standard web browser and using only secure communication protocol (i.e. HTTPS).	
15.43 The proposed Web Isolation Platform shall support collection of web traffic and threats identified by the isolation platform and graphical displays the following types of information: • The Threat Analysis pane - Provides information about the domains and events that were flagged as threats by the isolation platform. • The Traffic Analysis pane - Provides information about web traffic and any actions taken by the proxy service.	
15.44 The proposed Web Isolation Platform shall retain web traffic logs for at least 30 days and allow the web traffic logs to be searchable from the administrator portal in Graphical User Interface.	
15.45 The proposed Web Isolation Platform shall provide interactive update of the web traffic and threats identified by the isolation platform where the logs shall be made available in near real time where the searchable information can be filtered based on the last 15minutes, last 1 hour, last 12 hours, last 24 hours, last 2 days, last week, or last month period.	
15.46 The proposed Web Isolation Platform shall provide detailed information about all web traffic logs and any actions taken by web isolation service, displaying the information in Graphical User Interface and allows searching and filtering of the logs by any of the following categories: • Time period – Options of last 15 minutes, 1 hour, 12 hours, 24 hours, 2 days, past week, or past month. • User ID – Filter by user name. • Domain – Filter by domain URL. • Category – Filter by domain category type (e.g., business, games, news, etc.). • Threat type – Filter by threat type encountered e.g. Flash, malware, plugin risk, risky file, spam, uncategorized site, or vulnerable service. • Threat level – Filter by threat level e.g. all, green, yellow, or red. • Request type – Filter by request type e.g. all, page request, file upload, file request, Flash, or isolated document. • Actions taken – Filter by action taken e.g. all, allow, isolate, block, or bypass. • Protocols – Filter by protocol e.g. all, HTTP, or HTTPS.	

15.47 The proposed Web Isolation Platform shall allow administrator to extract the web logs from the cloud-base service administrator portal through logging API and stored locally.	
15.48 The proposed Web Isolation Platform Logging API shall have authentication and security build-in where it must authenticate all requests with HTTPS, use of Auth Token, and IP Whitelisting to ensure only known IP address is allowed to download the web logs.	
Cloud-Base Data Center Certification and Third-Party Audit	
15.49 The proposed Web Isolation Platform shall have Service Organization Control Reports that demonstrate how the service provider achieves key compliance controls and objectives in the following areas: • A description of the cloud-base data center provider control environment and external audit of the provider defined controls and objectives	
15.50 The proposed Web Isolation Platform Cloud-base data center shall attain Attestation Standard Section 801 (AT 801) issued by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and supersedes the two prior service organization controls guidance standards for auditors commonly known as SSAE 16 and SAS 70.	
15.51 The proposed Web Isolation Platform shall include independent third-party audit of the cloud-base data center Service Organization Control report by one of the internationally renowned big four audit firms (ie Deloitte, E&Y, KPMG or PWC).	
15.52 The proposed Web Isolation Platform Cloud-base data center SOC report shall be reviewed, issued and valid on a half yearly (ie 6 months) basis.	
Product Support Requirements	
15.53 The proposed Web Isolation Platform shall provide 24x7 follow-the-sun support model, with support teams in multiple geographical regions.	
15.54 The proposed Web Isolation Platform shall allow customer to submit support request through the following	

• Phone • Email • Customer Online Support Portal		
16. Bidders Qualifications		
16.1 The winning bidder should have ISO 9001:2015 Quality Management Systems, if for joint venture agreement, both of the JV should be ISO 9001: 2015 certified.		
16.2 To ensure compatibility, all hardware components should be of the same brand.		
16.3 All E-learning Components and application must be approved by DepEd. A valid certification coming from Dep-ED must be presented during Bid Opening.		
17 Payment Schedule		
Advance Payment subject to submission of an irrevocable letter of credit or bank guarantee issued by a universal or commercial bank pursuant to Section 4.5 of Annex D of the Revised IRR of RA 9184	15%	
After final inspection and acceptance of the total delivered equipment and licenses	75%	
Upon completion of training	10%	
	Total 100%	
18 Training		
18.1 The winning bidder must provide two (2) Days E-Learning software training, for DICT employees. The DICT employees in return will train the selected school representatives.		
18.2 All Costs relative to the conduct of training must be at the expense of the winning bidder, including transportation, venue, food and training materials of the participants within Metro Manila.		
19 Delivery Schedule		

Item	**Delivery Date**	
PC Workstations for Teachers	120 calendar days after receipt of Notice to Proceed	
Thin Client for Students		
LED Monitors		
Network Equipment		
Management Software for Workstations and Thin Clients		
E-Learning Application for Math and Science		
E-Learning Application for Filipino		
Antivirus License for Workstation		
Comprehensive Training on the installation, configuration and administration of the desktop management system, and e-learning system.	60 calendar days after Delivery of equipment	

Name of Company	Signature Over Printed Name Of Authorized Representative	Date

DICTBAC
REVISED CHECKLIST OF REQUIREMENTS FOR BIDDERS
AS 8 May 2019

Name of Company : _____
Name of the Project : Supply and Delivery of E-Learning Equipment and Software
Bid Reference Number : DICTBAC-2019-006
ABC : ₱90,000,000.00

Ref. No.	Particulars	
ENVELOPE 1: ELIGIBILITY AND TECHNICAL DOCUMENTS		
ELIGIBILITY DOCUMENTS		
CLASS "A" DOCUMENTS		
12.1	**(a.1.) <u>ELIGIBILITY DOCUMENTS</u>**	
	i. PhilGEPS Certificate of Registration and Membership in accordance with Section 8.5.2 of the IRR, except for foreign bidders participating in the procurement by a Philippine Foreign Service Office or Post, which shall submit their eligibility documents under Section 23.1 of the IRR, provided, that the winning bidder shall register with the PhilGEPS in accordance with section 37.1.4 of the IRR.	
	ii. Statement of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid **(Annex I)**	
	iii. Statement of Completed Single Largest Contract within the last 7 years from the date of submission and receipt of bids equivalent to at least fifty percent (50%) of the ABC. Annex I-A	
	iv. Duly signed Net Financial Contracting Capacity Computation (NFCC)* per **Annex II,** in accordance with ITB Clause 5.5 or a committed Line of Credit from a universal or commercial bank *NFCC = [(Current Assets minus Current Liabilities) (15)] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started coinciding with the contract to be bid. Notes: a) The values of the bidder's current assets and current liabilities shall be based on the data submitted to BIR through its Electronic Filing and Payment System. b) Value of all outstanding or uncompleted contracts refers those listed in Annex-I. c) The detailed computation using the required formula must be shown as provided above. d) The NFCC computation must at least be equal to the total ABC of the project.	
CLASS "B" DOCUMENTS (FOR JOINT VENTURE)		
	i. For Joint Ventures, Bidder to submit either: 1. Copy of the JOINT VENTURE AGREEMENT (JVA) in case the joint venture is already in existence, or 2. Copy of Protocol / Undertaking of Agreement to Enter into Joint Venture signed by all the potential join venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful. **(Annex III)** **<u>The JVA or the Protocol/Undertaking of Agreement to Enter into Joint Venture (Annex III) must include/specify the company/partner and the name of the office designated as authorized representative of the Joint Venture.</u>**	

<table>
<tr><td></td><td>For Joint Venture, the following documents must likewise be submitted by each partner:
PhilGEPS Certificate of Registration and Membership in accordance with Section 8.5.2 of the IRR, except for foreign bidders participating in the procurement by a Philippine Foreign Service Office or Post, which shall submit their eligibility documents under Section 23.1 of the IRR, provided, that the winning bidder shall register with the PhilGEPS in accordance with section 37.1.4 of the IRR.</td><td></td></tr>
<tr><td></td><td>For item (ii) to (iv) of the required eligibility documents, submission by any of the Joint Venture partner constitutes compliance.</td><td></td></tr>
<tr><td colspan="3">TECHNICAL DOCUMENTS</td></tr>
<tr><td>12.1 (b)(i)</td><td>Bid security shall be issued in favor of the DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT) valid at least one hundred twenty (120) days after date of bid opening in any of the following forms:
a) BID SECURING DECLARATION per Annex IV; or
b) Cashier’s / Manager’s Check equivalent to at least 2% of ABC issued by an Universal or Commercial Bank.
c) Bank Draft / Guarantee or Irrevocable Letter of Credit issued by a Universal or Commercial Bank equivalent to at least 2% of the ABC: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank
d) Surety Bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security equivalent to at least 5% of the ABC
<table>
<tr><td colspan="2">Description</td><td>Supply and Delivery of E-Learning Equipment and Software</td></tr>
<tr><td colspan="2">Qty</td><td>1 lot</td></tr>
<tr><td colspan="2">Total ABC (PhP)
(VAT Inclusive)</td><td>PhP90,000,000.00</td></tr>
<tr><td rowspan="3">BID SECURITY</td><td>Cashier’s / Manager’s Check equivalent to at least 2% of the ABC</td><td rowspan="2">PhP1,800,000.00</td></tr>
<tr><td>Bank Draft / Guarantee or Irrevocable Letter of Credit equivalent to at least 2 % of the ABC</td></tr>
<tr><td>Surety Bond equivalent to at least 5% of the ABC</td><td>PhP4,500,000.00</td></tr>
<tr><td></td><td>Bid Securing Declaration</td><td>No required percentage</td></tr>
</table></td><td></td></tr>
<tr><td>12.1 (b)(ii)</td><td>Proof of Authority of the Bidder’s authorized representative/s:
a) FOR SOLE PROPRIETORSHIP (IF OWNER OPTS TO APPOINT A REPRESENTATIVE):
Duly notarized Special Power of Attorney
b) FOR CORPORATIONS, COOPERATIVE OR THE MEMBERS OF THE JOINT VENTURE:
Duly notarized Secretary’s Certificate evidencing the authority of the designated representative/s.
c) IN THE CASE OF UNINCORPORATED JOINT VENTURE: Each member shall submit a separate Special Power of Attorney and/or Secretary’s Certificate evidencing the authority of the designated representative/s.</td><td></td></tr>
<tr><td rowspan="6">12.1 (b)(iii)</td><td>Omnibus Sworn Statements using the form prescribed. (Annex V)</td><td></td></tr>
<tr><td>a) Authority of the designated representative</td><td></td></tr>
<tr><td>b) Non-inclusion of blacklist or under suspension status</td><td></td></tr>
<tr><td>c) Authenticity of Submitted Documents</td><td></td></tr>
<tr><td>d) Authority to validate Submitted Documents</td><td></td></tr>
<tr><td>e) Disclosure of Relations</td><td></td></tr>
</table>

	f) Compliance with existing labor laws and standards	
	g) Bidder's Responsibility	
	h) Did not pay any form of consideration	
	i) Company Official Contact Reference	
12.1 (b)(iv)	Company Profile **(Annex VI).** Company printed brochure may be included	
12.1 (b)(v)	Vicinity / Location of Bidder's principal place of business	
12.1 (b)(vi)	Certificate of Performance Evaluation **(Annex VII)** showing a rating at least Satisfactory issued by the Bidder's Single Largest Completed Contract Client stated in the submitted Annex I-A;	
12.1 (b)(vii)	Completed and signed Technical Bid Form **(Annex VIII)**	
12.1 (b)(viii)	Brochure (original or internet download) / Technical Data Sheet or equivalent document	
12.1 (b)(ix)	Valid and Current Certificate of Distributorship / Dealership/ Resellership of the following product being offered, issued by the principal or manufacturer of the product (if Bidder is not the manufacturer). If not issued by manufacturer, must also submit certification / document linking bidder to the manufacturer	
12.1 (b)(x)	Valid and current ISO 9001 Quality Management System Certificate issued to the manufacturer of the product being offered issued by an Independent Certifying body;	
12.1 (b)(xi)	List of authorized Service Centers in the Philippines (with available spare parts, indicating address, telephone & fax number/s, e-mail address & contact person). In the event of closure of business, termination of franchise / service center, the supplier shall notify the DICT accordingly of the new service centers with telephone numbers and address who can provide the needed parts, supplies and service	
12.1 (b)(xii)	Compliance with the Schedule of Requirements as per Section VI	
12.1 (b)(xiii)	Compliance with the **Revised Technical Specifications as of 8 May 2019** as per Section VII	
ENVELOPE 2: FINANCIAL DOCUMENTS		
13.1 (a)	Completed and signed Financial Bid Form. Bidder must use, accomplish and submit Financial Bid Form hereto attached **Annex IX.** **Description** | **Qty** | **ABC ₱ (VAT Inclusive) Total** Supply and Delivery of E-Learning Equipment and Software | 1 Lot | PhP90,000,000.00 The ABC is inclusive of VAT. Any proposal with a financial component exceeding the ABC shall not be accepted. Further, the sum of bid for each item indicated in the **Detailed Financial Breakdown per Annex X** must be equal to the signed and submitted Financial Bid Form per Annex IX.	
13.1 (a)	**Detailed Financial Breakdown per Annex X**	
15.4(a)(i) & 15.4(b)(ii)	Completed **"For Goods Offered from Abroad"** and/or **"For Goods Offered From Within the Philippine"** Forms per **Annex XI-A** and **Annex XI-B, whichever is applicable.**	
13.1 (b)	If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a Certification from the DTI, SEC or CDA to be enclosed pursuant to the Revised IRR of R.A. 9184.	
NOTE:	**In case of inconsistency between the Checklist of Requirements for Bidders and the provisions in the Instruction to Bidders/Bid Data Sheet, the Instruction to Bidders/Bid Data Sheet shall prevail**	