General Directorate of Administrative Affairs IEA

National Procurement Directorate

Technical Deputy

Procurement Plans Integration & Analysis Department

Amendment No.1

Project: Procurement of Equipment & Software for Upgrading of Central Dispatching System, Digitalization and Automation of Stations & Substations required by SCADA Department of DABS with Ref.No: NPD/DABS/1402/G-37/ICB/Rebid Procurement Entity: Da Afghanistan Breshna Sherkat – DABS Date: May 13, 2024

SBD or Annexure1 Technical Document Reference	Existing text	Amended to
Annexure1Technical Document (Page.7,8,9,37,42) & SBD (Page.38,56,74,76,77); or if mentioned in other pages.	FAT (Factory Acceptance Test) is applicable.	FAT (Factory Acceptance Test) is not applicable.
SBD Page.38	Note2: DABS will introduce three Representative for training as mentioned in price schedule and technical document in abroad where FAT test will be conducted (each item training: 7 days, totally: 3 items = 21 days). The bidder should consider the cost of the FAT test and travel cost of three representatives on its price.	Note2: DABS will introduce three Representative for training as mentioned in price schedule and technical document in one of neighbor or near countries for total 30 working days. The bidder should consider the travel cost of 3 representatives on its price & should specify the training country on its offer.

Note: other contents of SBD & Technical Document are remain applicable without any changes.

d) The vendor shall provide appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

e) The vendor shall provide a listing of services required for any computer system running control system applications or required to interface the control system applications. The listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation.

f) The vendor shall verify and provide documentation that all services are patched to current status. The vendor shall provide, within a pre-negotiated period, appropriate software, and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

g) The vendor shall remove and/or disable software components (such as services and executables) that are not required for the operation and maintenance of the control system. The vendor shall provide documentation of what is removed and/or disabled. Examples of the software to be removed and/or disabled may include:

- Games
- Device drivers for network devices not delivered.
- Messaging services, Social network file sharing (e.g., MSN, FB, Twitter, IM, etc.)
- Servers or clients for unused Internet services
- Software compilers in all user workstations and servers except for development workstations and servers.
- Software compilers for languages that are not used in the control system.
- Unused networking and communications protocols.
- Unused administrative utilities, diagnostics, network management and system management functions.
- Backups of files, databases and programs used only during system development.
- All unused data and configuration files.
- Sample programs and scripts.
- Unused document processing utilities (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.), unless used and required by the system.
- Unneeded third-party applications such as Flash Player, Java, PDF viewers, and browser add-ons/plug-ins.

h) The vendor shall configure hosts with least privilege file and account access and provide documentation of the configuration. The vendor shall configure the necessary system services to execute at the least user privilege level possible for that service and provide documentation of the configuration. The vendor shall document that the changing or disabling of access to such files and functions has been completed.

i) The vendor shall have a formal patch management and update process for all vendor-supplied software, including operating system and any required third-party applications, and for any vendor-supplied hardware (firmware updates).

06/Nov/2023

j) The vendor shall provide details of their patch management and update process. Responsibility for installation and update of patches shall be identified.

k) The vendor shall provide firewalls and firewall rule sets between network zones or provide firewall rule sets if the firewalls are not provided by the vendor. The vendor shall provide firewall rule sets and/or other equivalent documentation. The basis of the rule set shall be "deny all," with exceptions explicitly identified by the vendor. Note that this information is deemed business sensitive and shall be protected as such.

l) The vendor shall provide detailed information on all communications (including protocols) required through a firewall, whether inbound or outbound, and identify each network device initiating a communication in accordance with the corresponding rule sets.

m) The vendor shall recommend which accounts need to be active as well as those which can. The end user shall approve in writing the vendor's recommendation. The vendor shall disable, remove, or modify all the accounts pursuant to the approved recommendation.

n) After contract award, the vendor shall disable or remove all default and guest accounts. Once changed, new accounts will not be published except that new account information and passwords will be provided by the vendor via protected media.

o) After the site acceptance testing (SAT), the vendor shall disable, or modify all vendor-owned accounts or negotiate account ownership with the DPDC.

p) The vendor shall not permit user credentials to be transmitted in clear text. The vendor shall provide the strongest encryption method to commensurate with the technology platform and response time constraints. The vendor shall not allow applications to retain login information between sessions, provide any auto-fill functionality during login or allow anonymous logins. The vendor shall provide user account-based logout and timeout settings.

q) The vendor shall provide a configurable account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of logins attempts and inactive session logout.

r) The vendor shall not store passwords electronically or in vendor-supplied hardcopy documentation in clear text unless the media is physically protected. The vendor shall control configuration
interface access to the account management system. The vendor shall provide a mechanism for rollback of security authentication policies during emergency system recovery or other abnormal operations where system availability would be negatively impacted by normal security procedures.

s) The vendor shall provide a system whereby account activity is logged and is auditable both from a management (policy) and operational (account use activity) perspective. The vendor shall time stamp and control access to audit trails and log files. The vendor shall ensure audit logging does not adversely impact system performance requirements.

t) The vendor shall provide for user accounts with configurable access and permissions associated with the defined user role. The vendor shall adhere to least privilege permission schemes for all user accounts and application-to-application communications.

u) The vendor shall verify that a user cannot escalate privileges, under any circumstances, without logging into a higher-privileged role first. The vendor shall provide a mechanism for changing user(s) role (e.g., group) associations. After contract award, the vendor shall provide documentation defining access and security permissions, user accounts, applications, and communication paths with associated roles.

v) Use of browser-based user interfaces for the critical control GUI is not desirable. The primary user interface for the control system should not utilize vulnerable technologies such as native operating system JRE/Java, X-Windows, ActiveX Controls, etc. Vendors shall describe the use of any web-based interfaces for critical control functions. If they are used, vendors should respond to the requirements listed below.

w) The vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time and throughput (including during the SAT) when connected to existing equipment).

x) The vendor shall remove or disable all software components and services that are not required for the operation and maintenance of the devices that run an HTTP server. The vendor shall provide documentation on what is removed and/or disabled.

y) The vendor shall provide, within a pre-negotiated period, appropriate software, and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

2.1.5. System Sizing

The system software shall be capable of accommodating in its database 1 million Tag Points (at least 250000 external) which includes status and control points, analog input points, text points, communication lines, RTUs, IEDs, reports, graphic symbols.

Vendor shall provide documentation of 99.98% system availability.

2.1.6. Hardware Platform

The hardware platform encompasses all the physical hardware devices utilized by the SCADA system including host servers, operator workstations (local and remote), storage devices, communication interfaces, printers, GUI devices (LCD Flat Panels) and LANs to which all the hardware devices shall connect.

The system shall be implemented with industry standard general-purpose devices and interfaces. The proposed hardware devices shall be available from at least two different commercial sources (brands) on the market.

All materials and equipment furnished for permanent installation in the work shall conform to applicable standard specifications and shall be new, unused, and undamaged.

2.1.7. Host Servers

communication lines.

Users will be able to preview what changes were made in a project before publishing the project.

All workstations will be notified whenever there are new graphic changes to download.

When connected to an OES system, the GUI distinguishes itself from a real-time connection by the following:

- The title bar contains the words "OES MODE"
- The status bar is colored different.
- In addition, the point control dialogs are further distinguished by colored highlights around the pushbuttons.
- Other applications like the database editor or server manager will also have their applications highlighted in green to let users know they are working in an OES environment.

2.1.40. Quality Assurance System (QAS) Environment

In the QAS environment, users will be able to replicate their entire production environment (servers and applications) in an offline environment that allows users to test hardware firmware updates, operating system patches, software upgrades, updates, and hotfixes. Full regression tests are performed in the staging environment prior to updating the production, offline editing, and training environments to ensure all implementation steps and procedures are accurate.

When connected to a QAS system, the GUI distinguishes itself from a real-time connection by the following:

- The title bar contains the words "QAS MODE"
- The status bar is colored different.
- In addition, the point control dialogs are further distinguished by colored highlights around the pushbuttons.
- Other applications like the database editor or server manager will also have their applications highlighted in blue to let users know they are working in a QAS environment.

Service Line Agreement: 1 year at least

Engineering Training:

Full feature training on SCADA:

- Installation
- DATABASE Configuration
- Graphic Design
- Command Processing
- Command Sequence
- Syntax
- Commissioning
- Test
- Project work

2.1 RTU +Panel +Aux Relays+ Engineering Training

A- RTU

Quantity: 1 Set/Lot (Total 12 Set)

RTUs are used in almost all stations and substations SCADA systems of Afghanistan and proven to work fine and DABS SCADA team can maintain the System properly. It collects field information and send it to Control Centers inside facility and National Load Control Center.
The device shall fulfill all requirements included in this document.
RTU shall be pre-installed inside Panel and its associated Connectors, cable and shall be pre-terminated to terminal Blocks at rear Side of panel.
Manufacturers shall have at least 40 years' experience in remote control systems. Only RTU from International Manufacturers SEL,ABB,SELTA with at least 10 years warranty from manufacturer side shall be supplied. DABS has the right to reject any supplied item not fulfilling the requirements.

NO	ITEMS	PARAMETER
1	RTU frame and core Modules	19 inches rack mount mainframe with Core Modules, sub frame shall be include If the requirement is not full filled with only mainframe.
2	CPU	• Full license for Protocols and I/Os, at least 2 Ethernet ports and 4 Comports.
3	RTU to control centers communication card	IEC 60870-5-104, at least 4 control centers using the protocol.
4	Redundant Power supply	48VDC
5	Digital Input (DI) cards	128 DI 48VDC card
6	Digital Output (DCO) cards	32 DCO 48VDC card
7	Analog Input (AI) cards	at Least 10 Analog input Signals
8	Communication Cards to Analyzers and Relays	Modbus TCP/IP, Modbus Serial and IEC 61850 Cards/Ports with related Serial and Ethernet ports
9	Engineering Software with license and Engineering manuals for software and hardware	Configuration software with full license and manuals,
10	RTU Type	Modular
11	Connectors and Cables	Associated connectors and cables from RTU to Terminal Blocks at back of Panel.
12	SYNCHRONISM	External NTP v4 server shall be included