SECTION 27 21 00 –DATA COMMUNICATIONS EQUIPMENT (DCE)

1.01 SUMMARY:

A. [A17]**Scope**: Scope of work shall be in accordance with Paragraph 1.01 D. of Section 01 81 26 (*Communications, Control, Safety, and Security Systems*), as required, for data, video, and voice communications, as well as process control systems for the Works.[A17] This Section of the Employer's Requirements shall be read in conjunction with the Sections listed in Table 27 21 00-1.

B. **Related Sections**:

TABLE 27 21 00-1: [A9]Related Sections[A9]

1.	Section 01 81 26	-	Communications, Control, Safety, and Security Systems.
2.	Section 12 59 83	-	Custom System Furniture (ref. Consoles).
3.	Section 25 11 00	-	Data Processing Equipment (DPE).
4.	Section 27 10 00	-	Structured Cabling System for Communications Inside Plant.
5.	Section 27 11 16	-	Cabinets, Racks, Frames, and Enclosures.
6.	Section 27 31 23	-	IP-based Telephone Systems.
7.	Section 27 51 16	-	Public Address Systems.
8.	Section 27 53 13	-	Time Synchronization Systems.
9.	Division 28	-	All Safety and Security Systems.
10.	Section 35 12 00	-	Vessel Detection Systems (VDSs).
11.	Section 40 95 13	-	Process Control Hardware.

1.02 REFERENCE:

A. **Applicable Publications**: Refer to Section 01 81 26 (*Communications, Control, Safety, and Security Systems*), [A9]Paragraph[A9] 1.02.

1.03 REQUIREMENTS:

A. **General Requirements**:

1. **General**: The Contractor shall meet all applicable requirements of Section 01 81 26 (*Communications, Control, Safety, and Security Systems*), [A9]Paragraph[A9] 1.03.

2. **Equipment**:

a. DCE shall be IPv6 (or latest, whichever is the newest), SIP, and VoIP compliant and ready.

b. [A10]Switches[A10] with gigabit interfaces shall be included as part of the transport layer equipment.

c. Hubs shall not be used. Data switches with minimum useful life of seven years shall be used instead.

d. Bridges shall not be used. Routers shall be used instead for internetworking.

3. **Interoperability and Coordination**: New DCE shall interoperate and be coordinated with Employer WAN equipment. Note the following:

a. LAN switches at the WAN edge include Cisco Systems Catalyst 2960 and 6500, or better. If needed, these support replicating traffic from a port to another (span port, or port mirroring). Also, wireless LAN Radios are Cisco Systems Aironet 1300, or better.

b. [A19]The Employer owns a wide variety of WAN and transport equipment, including asynchronous-transfer mode (ATM) (Fore and Marconi) and SONET (Alcatel) at the core, and access concentrators (Tellabs), and routers and switches (Cisco) at the edge.[A19] Since ATM routing is dynamic, the number of switches may vary.

c. [A9]The Employer plans to replace SONET and ATM networks between FY2010 and 2011 with IP/MPLS routers. The Contractor shall offer IP/MPLS routers as required for the new locks. The Employer will provide IP/MPLS routers at Miraflores Building 7D and Gatun Building 24 with 10/100/1000 Mbps Ethernet ports. [A9]

d. [A9]Likewise, the Employer plans to replace Tellabs Martis DXX access concentrators with a newer generation (Tellabs 86xx series or equal) using an IP/MPLS network.[A9] New access concentrators correspond with a convergence strategy to own and operate an integrated carrier grade telecommunications network capable to handle data, video, and voice. [A9]The Contractor shall offer access concentrators as required for the new locks. The Employer has access concentrators at Miraflores Building 7D and Gatun Building 24.[A9]

4. **Networking**:

a. DCE shall enable multi-service networks based on ISO's 7-layer OSI Reference Model (OSIRM).

b. Networks shall support [A9]asynchronous connections, Ethernet, internetworking[A9], IPT, [A9]polices[A9] (with number as required), [A9]packet switching, [A9] QoS, TCP/IP, Virtual Private LAN Service (VPLS), and standard internet/intranet protocols as defined by IEEE and IETF. Also, networks shall support broadcast, multicast, and unicast transmissions.

c. Networks shall have very low BER, jitter, and latency.

d. [A9]WLANs and their security shall be in accordance with IEEE 802.11, or better.[A9]

e. The Contractor shall also consider mobile and nomadic applications of [A10]IEEE 802.16e[A10] compliant WiMax.

f. [A10]Ethernet devices shall comply with IEEE 802.3 for 10, 100, and 1,000 Mbps over UTP cable with or without power over Ethernet (POE), as well as for 1 and 10 Gbps over fiber optic cable. Ethernet repeaters shall not be used.[A10]

g. [A9]IEEE 802.1D compliant spanning trees or better means shall be used as required to improve fault tolerance, allow redundant links, and avoid looping problems.[A9]

B. **Hardware / Equipment and Materials**:

1. **Access [A9]Concentrator Switches**:[A9]

a. Units shall offer low bit rate voice and data ports such as FXO/FXS, [A10]TIA-232,[A10] xDSL, 2W and 4W E&M, over an IP/MPLS network.

[A9]b. Switches shall also offer 10/100/1000 Mbps Ethernet ports.[A9]

c. Equipped number of ports of each type shall be as required for third set of locks communications.

2. **Diagnostic/Security Modems**:

a. Systems with DPE shall include a security type diagnostic modem suitable for occasional remote access for selected technical personnel, including the manufacturer and its local partner.

b. Each modem shall be capable of 56 kbps data transmission, support TCP/IP, have dial-back capability, and require the successful entry of an approved password. These modems shall automatically disconnect if a wrong password is introduced.

c. The Employer prefers modems that can be configured to allow only one attempt, and does not present identification or banners upon connection.

3. **Ethernet Switches**:

a. [A9]Data switches shall enable 100/1000/10000 Mbps Ethernet networking, provide multiple simultaneous paths, and be SNMP compliant.[A9]

b. [A19]Switches shall be connection-oriented with all ports capable of full duplex operation. Switches for PCSs shall be industrial type.[A19]

c. Units shall support IEEE 802.1d compliant spanning tree, inter-switch protocols, MPLS, PoE (on the required number of ports), and trunk protocols such as IGMP version 3 or better.

d. Switches shall have dual power supplies, and redundant Ethernet links between them when connected.

e. [A9]The Employer strongly prefers using router switches capable of the following: [A9]

[A9]1) Dividing internetwork into separate networks for organizational and security purposes.

2) Enabling mesh topology.

3) Filter traffic according to protocols used.

4) Limit broadcast traffic.

5) Use routing information protocol (RIP). [A9]

4. **Fiber Optic Modem (FOMs)**:

a. **General**:

1) [A19]Two different makes and models shall be furnished for Ethernet and ControlNet to reduce common mode failure (CMF).

2) For Ethernet channels, modems shall have two or more 100/1000 Mbps or faster Ethernet ports.

3) The modems shall have diagnostics LEDs, indicating modem power, status, and optical signal condition.

4) Unless otherwise specified, redundant power supplies are desirable for FOMs in process control systems (PCSs), but not required.

5) In locations where up to four FOMS are required, the Employer prefers FOMs that plug directly into PLCs and IOCs.

6) In locations where more than four FOMs are required, the Employer prefers having these installed in chassis with a redundant power supply common to all FOMs. There shall be no need to have individual power supplies for each of these FOMs.

7) FOMs shall have optical signal strength suitable for no less than 5 km of fiber distance and the required bandwidth. [A19]

b. **Diagnostic Commands for FOMs in PCSs**: FOMs shall have interactive diagnostic commands to help locate a communications fault.

These commands shall be accessible via the PLC User Program. The diagnostic commands shall do the following:

1) Enable/disable a trap and hold fault feature, used to locate intermittent communication failures.

2) Activate/deactivate network fault test (simulate a fault).

c. **Fault Prediction**: FOMs shall have in-line optical signal strength monitoring, with the capability of providing discrete output signals for PLCs, indicating weak signal strength and signal fault. Each modem shall also have available an analog output signal for PLCs and tests, indicating the optical receive signal strength in dB.

d. **Fault Tolerance**: FOMs shall have dual communication channels, configurable as self-healing rings with online diagnostic monitoring, capable of high speed communication recovery around points of failure.

5. **Firewalls**:

a. [A19]Units shall perform packet filtering from the least to the most trusted network device. [A19] Traffic shall be stopped or allowed to proceed based on source and destination addresses, network protocol, and port number.

b. Firewalls shall perform stateful packet inspection (SPI) by keeping track of the larger context or state of transmissions, and stopping abnormal sequences.

c. Appliances with IDS, IPS, and VPN integrated solutions shall be Cisco ASA 5540 or approved equivalent, and shall be furnished instead of software applications for the same purposes.

d. Firewalls shall support up to 1,000 simultaneous connections and be NSA certified.

e. Units shall work as application level firewalls. Units capable of the following additional features are preferable:

1) Breaking the networking session between two end points at the proxy to ensure information technology security.

2) Helping hide internal network details from non-authorized users and intruders.

3) Providing circuit-level proxy service using SOCKS, UDP, or both, and distributing workload reducing the likelihood of firewall overload.

[A9]f. Ports shall be 1 Gbps Ethernet or better, and overall throughput shall be no less than 1.5 Gbps. [A9]

6. **Gateways**:

   a. Units shall acts as an entrance to another network, and be application specific as required.

   b. Gateways shall provide all the interconnectivity normally provided by routers, and conversion between the 7 layers of OSIRM. Units shall also provide conversion to other protocols if required to join disparate protocols.

7. **Routers**:

   a. Routers shall support large packet sizes, static routing, and multiple protocols simultaneously. Units shall automatically discover the address of devices connected to a network of routers.

   b. Units shall use standard routing protocols to interpret packets, forward them to a specific destination, and continuously monitor the state of links that interconnect routers in a network or the links with other networks. Routing of such packets from network node to node shall be based on packet defined protocol information, including least cost routing, minimum delay, minimum distance, and least-congestion conditions.

   c. Routers shall be capable of converting to a WAN protocol such as TCP/IP for transfer over a WAN link, and forwarding no less than 200,000 IP packets per second. Units shall also handle both connection-oriented and connectionless network services.

   d. Units shall create and maintain a table of the available routes and their conditions, and use this information along with distance and cost algorithms to determine the best path or route for a given packet. Routers shall also retain dynamic knowledge intelligence, discover network topology changes, and provide rerouting based upon dynamic routing tables.

   e. Routers shall be of scalable design, and may be included as part of a network switch. Units shall be software based to facilitate future revisions and upgrades.

   f. Units shall use physical data link and network layers to provide addressing and switching functionality. Routers shall be capable of limiting the number of hops.

   g. Routers shall interconnect dissimilar media via media conversion as required.

8. **SAN Switches**:

   a. Units shall include full fabric and performance monitor licenses as required.

b. Switches shall support multi-path between multiple servers and storage devices.

9. **Signal Converters**: Shall be furnished as required.

10. [A16]**Software**: Shall be as required to meet these Employer´s Requirements.[A16]

11. [A3]**WiFi Equipment**: Shall be [A9]IEEE 802.11[A9] compliant, and have protected and secure access (WPA2 or newer).[A3]

12. [A10]**WiMax Equipment**: All WiMax equipment for the new locks shall be IEEE 802.16e compliant, Wave 2 verifiable, and have protected and secure access.[A10]

13. [A5]**Media Converters**: Shall be adequate for the applicable cable types and distances.[A5]

C. **Installation**:

1. **General**:

a. Unless otherwise specified, DCE shall be rack mounted.

b. The Employer will apply internet access, network security, and password governance and security policies as deemed necessary.

c. The Employer will also assign dynamic and static IP addresses as required.

2. **Ethernet Switches**: Shall be used to connect DPE in LAN segments.

3. **Diagnostic/Security Modems**:

a. Unless a secure VPN connection is provided, such modems shall be used to allow the system manufacturer enter into it to resolve a major problem as a last resource. This rule applies after acceptance or beneficial occupancy, whichever comes first, and does not preclude possible connections that the Contractor may need.

b. If included in the design, such modems shall normally be turned off and disconnected to avoid possible hackers and unauthorized connections.

4. **Fiber Optic Modems (FOMs)**: Shall be installed in machinery or control rooms, in or near the corresponding Ethernet switch or PLCs.

5. **Firewalls**:

a. [A19]Firewalls shall be installed in the demilitarized zone so that there is no direct traffic flow between operations and enterprise zones.[A19] Firewalls shall be configured so that they implement the first line of defense, appear as a black hole to potential intruders, do not tell anything about themselves, and do not reveal internal network details.

b. Units shall also be configured to ignore PING, WHOIS, and other nosy requests for information.

c. Units shall not reside on a shared platform and shall not be permissible by default.

d. Units shall be configured to allow the minimum necessary number of simultaneous connections.

6. **Gateways**:

a. Gateways shall be furnished as required to control access and pass data between networks, including a network with Ethernet and another network with other protocol(s).

b. Enough units shall be provided as required to prevent network congestion.

7. **Routers**: Shall be used to communicate different network segments, and to guide traffic on the correct path (among several different ones usually available) across the complete inter-network to their destination.

8. **SAN Switches**: Shall be installed at Employer designated data center(s).

9. **Signal Converters**: Shall be furnished as required.

10. [A3]**WiFi and WiMax Equipment**: Shall be installed as required to achieve the coverage required by Section 35 12 00 (*Vessel Detection Systems*). WiMax shall be the first choice for VDSs.[A3]

1.04 DESIGN CRITERIA/SYSTEM PERFORMANCE:

A. **General**:

1. **Problem to be Solved**: DCE shall solve the following business needs:

a) Provide adequate means to safely and quickly communicate data, video, and voice signals between two or more points.

2. **Restrictions to be Considered**:

a) [A20]Networks shall have no oversubscription.[A20]

B. **Design Criteria**:

1. LAN shall meet the requirements of BICSI [A10]NDRM[A10] and IEEE standards.

2. Unless otherwise specified,

a. [A9]MAN and [A9] WAN topology shall be semi-meshed or fully-meshed.

b. New WAN equipment shall interconnect to Employer WAN as required.

c. LANs shall be dual-redundant.

3. Networks shall be designed so that these can change in terms of expandability, scalability, and evolution.

[A9]4. Spanning trees shall be established in accordance with IEEE 802.1D to allow networks with a topology that contains physical loops to remain free of looping problems.

5. Switched virtual circuits (SVSs) shall be used in connection oriented packet switching networks when needed to establish temporary connections dynamically. This shall be done without manually reconfiguring the network.

6. Virtual LANs (VLANs) shall be used when necessary to connect a group of hosts with a common set of requirements that communicate as if they were attached to the same LAN, regardless of their physical location. In switched networks, this shall establish a hierarchical network and organize into manageable broadcast domains and multicast groups. VLANs shall have the same attributes of a physical LAN, be configurable via software, and be in accordance with IEEE 802.1Q.

7. Quality of service (QoS) shall provide resource reservation control mechanisms in accordance with the applicable requirements of [A10]IEEE 802.1D [A10] and 802.11 for the following:

a. To provide different priority to different applications, users, or data flows, and

b. To guarantee a certain level of performance to a data flow, including the required bit rate, delay, jitter, packet dropping probability, and/or bit error rate. [A9]

[A10]8. Premises equipment shall be capable of tolerating the jitter and wander created by the transport network. [A10]

C. **System Performance**:

1. DCE shall be adequate for safely delivering multiple data, video, and voice services required for operations of the third set of locks.

2. Networks shall be adequate for the expected traffic characteristics, considering required applications, burstiness (peak rate/average rate), delay tolerances, error control (i.e., CRC), interfaces, priorities, protocols, response times, throughput, and total capacity.

3. [A10]Should WiMax be used, its coverage shall include the most likely areas of future fourth set of locks. [A10]

1.05 SUBMITTALS: The following shall be submitted for substantiation purposes:

A. **Design**: The following shall be in accordance with Section 01 81 26 (*Communications, Control, Safety, and Security Systems*), [A9]Subparagraph 1.05 D.:[A9]

1. [A20]Calculations (considering no oversubscription), including –[A20]
   a. Communication channel loading and throughput estimates.
   b. [A10]Link budget (including gains and losses) and signal to noise (S/N) ratio calculations, if and as applicable.[A10]
   c. Required bandwidth estimates under low, normal, and high network activity conditions.
   d. Reliability.
2. CPM diagram, with monthly updates.
3. Descriptive literature.
4. Device configuration files.
5. Disaster prevention plan (DPP).
6. Disaster recovery plan (DRP).
7. Drawings.
8. IT security methods.
9. Proposed governance and security policies.
10. [A19]Protection methods for corrosion, ESD, fungus/humidity, lightning/surge, power distortion and harmonics, radio-frequency interference/electromagnetic interference (RFI/EMI), thermal, and vibration.[A19]
11. Quality assurance and control plans.
12. Routing tables.
13. Specifications.
14. SWOT analysis.
15. [A20]ISO 20000 certificates for DCE manufacturers (preferable), to ensure an ITIL style help desk.[A20]

B. **Re-submittals Just Prior to Purchasing Materials**: All items in A. above that have changed from original submittal shall be resubmitted in a Design Conference in accordance with Section 01 81 26 (*Communications, Control, Safety, and Security Systems*), Paragraph 1.05.

C. **Upon Receipt of Shipped Items in Panama**:

1. Instruction manuals for administration, installation, maintenance, and operation.

2. Packing lists.

D. **Prior to Issuance of Taking-Over Certificate**:

1. [A17]As-built drawings, including IP addresses.[A17]
2. List of recommended spare parts.
3. Software licenses.
4. Test reports.

1.06 QUALITY ASSURANCE: Shall include the following in accordance with Section 01 81 26 (*Communications, Control, Safety, and Security Systems*), [A9]Paragraph[A9] 1.06:

A. Factory Quality Control Tests (FQCT).

B. Final Field Inspection Tests (FFIT).

C. Technical Support.

D. Warranty.

E. [A3]Drawings, including the applicable WiFi and WiMax coverage maps.[A3]

END OF SECTION

[A9]**THIS PAGE NOT USED** [A9]