CHAPTER 09: IT AND SECURITY PERFORMANCE REQUIREMENTS

9.1. INTRODUCTION

9.1.1. SCOPE

This Chapter provides design guidelines and requirements for designing infrastructure for Information Technology (IT) and Security Systems for the Authority. It is not the intent for this document to replace existing technical specification, more so, to allow technical specification to be written by utilizing these guidelines as a base.

The Consultants shall research and validate the current Basis of Design Manufacturers and Products for acceptability by the Authority prior to product submission, due to the frequent changes with technology.

Architects, engineers, planners, consultants, installers, tenants, and staff are among the intended audience. The result of adhering to this specification is to provide infrastructure that:

1. Is secure;
2. Provides for growth (Scalability);
3. Conforms to industry standards;
4. Implements best practices;
5. Improves reliability;
6. Increases serviceability;
7. Provides physical redundancy;
8. Provides ease of maintenance.

9.2. BASIC COMMUNICATIONS REQUIREMENTS

9.2.1. ADMINISTRATION AND EQUIPMENT MANAGEMENT

9.2.1.1 LABELING

1. General:

   a. All labels shall be computer or label maker generated.

   b. It is recommended that cable labeling conform to Telecommunications Industry Association TIA/EIA-606-B, Administrative Standard for Telecommunication Infrastructure.

2. Conduit:

   a. All conduit runs shall be labeled on origin and destination ends, as well as color coded to align with current Authority color code standards set forth by the Authority. Conduits shall be marked with color coding every ten feet.

3. Fabric Multi-Celled Innerduct in Pull Boxes, Maintenance Holes, and Manholes:

   a. Every fabric multi-celled innerduct installed shall have a brass or plastic tag that contains the origin and destination. These tags shall be placed at both ends and in every pull box, handhole or manhole along the pathway, as well as within RR's/CER's. These tags shall be securely fastened so that they cannot be accidentally removed.

      i. Examples:

         a) RR21 to Server Room

         b) SR01W to RR03W

4. Cables:

   a. All cables including but not limited to, copper, fiber, coax etc., shall be labeled. Final labeling schemes shall be provided on all as-built drawings and printouts.

   b. Coordinate with the ATS Team or I&TS on final labeling scheme.

5. Work Areas:

   a. Work area outlet cabling shall be labeled at each end. Labels shall be installed within 4 inches of the termination points. Labels shall be machine printed, wrap around, self-laminating type labels;

   b. Work area outlets shall be labeled on the front of the wall plate with a pre-approved labeling scheme. Contractor shall coordinate with ATS and I&TS to verify the approved scheme prior to installation;

c. Copper and Fiber Optic patch panels shall be clearly labeled on the front of the patch panel. Fiber optic patch panels shall utilize the manufacturer's labeling template. P-touch type labels are not the preferred labeling method. Coordinate with the Authority on labeling schemes prior to installation;

d. Final labeling schemes shall be provided on all as-built drawings and printouts.

6. Tenant Areas:

a. If Rack Rooms are shared with tenants, provide clear separation via a wire mesh fence and identification of the equipment and terminations, chain link is not the preferred product, Refer to Figure 9.1. on the following page.

9.2.1.2. DOCUMENTATION

1. Sensitive Security Information (SSI) is information controlled under Federal regulation 49 CFR parts 15 and 1520 and the Transportation Security Administration (TSA). Consultants must review the regulations and adhere to the requirements to ensure compliance.

2. Prior to the startup of a system or bringing network devices online, the timely submission of a Port Request Matrix will need to be provided to the I&TS department. I&TS will issue port information, and create VLANs based on information received. Examples of information required to be submitted on the port request form are:

a. Device type and description and location ;

b. IP Address;

c. MAC Address;

d. Make, Model and Serial number of the devices planned for installation;

e. Planned network switch to be utilized.

3. Upon completion of installation and after the final acceptance of all systems, the Installer shall supply a complete set of as-built documentation as follows:

a. Site plan;

b. System block diagram;

c. Interconnection diagram;

d. Dig Alert tickets and Utility Locate documentation;

e. As-built drawings and prints of the conduit installation with routing;

f. Butterfly diagrams of manhole and handhole conduit configurations and cable routing, to include conduit sizes and cable counts;

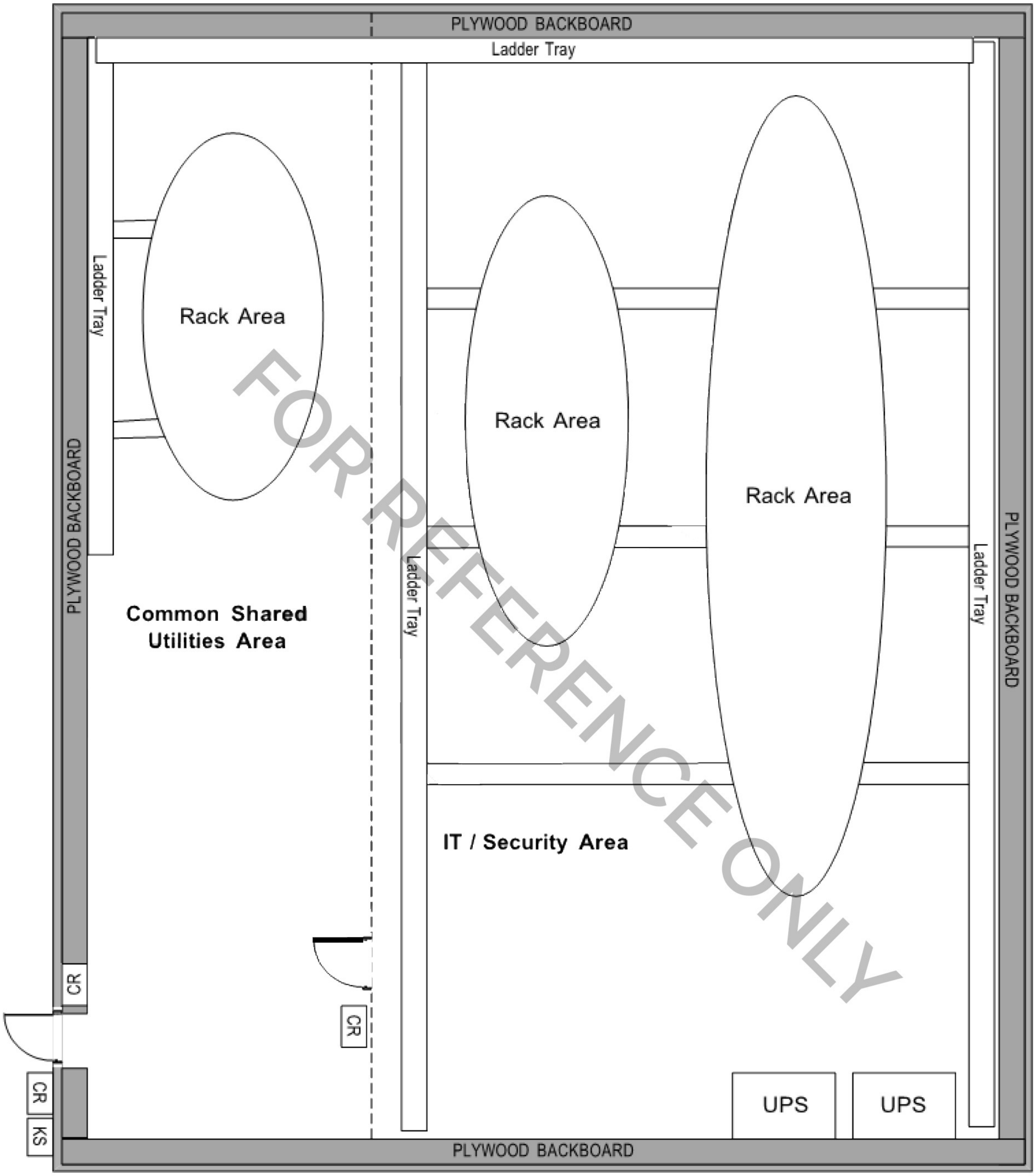


Figure 9.1.: Rack Room Diagram

g. Electronic drawings incorporated into BIM format;

h. Final acceptance test data sheet included cable test results;

i. Updated Material List with quantities, model numbers and serial numbers;

j. End-to-end cable documentation that documents device, patch panel, wall jacks, switch port connectivity and any other connected device in between;

k. Manufacturer manuals/data sheets on all equipment;

l. Manufacturer representatives and telephone numbers;

m. Operation manuals;

n. QA/QC manuals;

o. Quality Management Plan (QMP);

p. Commissioning test forms;

q. Warranty letter and time frame of warranty.

4. The above documentation shall illustrate in detail the interconnection of every component and its correct functional relationship showing the positional and geographical location. The above documentation shall also include the following information:

a. All testing parameters and resulting outputs;

b. All cable numbers

c. All grounding points;

d. All conduit and/or cable tray pathways.

9.3. COMMUNICATIONS SYSTEMS

9.3.1. GROUNDING AND BONDING

1. Ground Bus Bar shall be installed in all Minimum Point of Entry's (MPOE's), Server Rooms, Rack Rooms, and Communication Rooms;

2. Telecommunications Main Grounding Busbar (TMGB) shall be installed in a the MPOE or Server Room (SR) and connect to both building steel and the main electrical grounding entrance facility;

3. Telecommunications Grounding Busbar (TGB) shall be provided in each Rack Room and/or Communication Room and connect to the TMGB via a Telecommunications bonding backbone (TBB).

a. Separate TBB's shall be installed to each level of the building;

b. Telecommunications Grounding Busbar's (TGB's) can be connected in series via the TBB to those rooms residing on the same level of the building;

c. Connections from TBB to TMGB/ TGB shall be irreversible utilizing exothermic welds.

d. TBB's shall be sized to ensure the resistance is 5 Ohms or less. The measurement must be taken from two points within the system. Design must achieve this requirement via wiring size for given distances versus resistance drop.;

4. All equipment racks and/or cabinets and cable try/ladder racks shall be bonded together and then to the TGB using a minimum of a #6 AWG insulted, stranded copper, to be green in color.

5. All bonging connections shall utilize two-hole lugs.

9.3.2. PATHWAYS FOR COMMUNICATIONS SYSTEMS

9.3.2.1. HORIZONTAL DISTRIBUTION

1. The Authority standard for horizontal cabling installations, is a 1" conduit pathway from cable tray to work area outlet. Conduits shall be bonded to the cable tray using compression connectors with bonding fitting and #6 AWG green isolated wire. Conduits shall be no less than 1", however sized appropriately to maintain industry standard fill ratios (40% fill ratio).

   a. Conduits shall not extend more than 100 feet in any one continuous run without a pull-box. Communication conduits shall not exceed a total of 180-degrees bend radius without installation of a pull box. Pull box sizing shall be based on conduit sizes and fill ratios;

   b. Conduits should enter and exit pull boxes on opposite ends of the box; Pull boxes should not be utilized as 90 degree bends;

   c. All conduits shall be marked to identify the type of communications pathway. Markings to occur every 10 feet. Method on how conduits will be identified shall be submitted by the contractor to the engineer or to the Authority for approval.

2. Conduits shall be Electrical Metallic Tubing (EMT) or Rigid steel conduit. No plastic or plastic based materials can be used for pathways, with the exception of underground pathways.

   a. The exception of surface mount wire mold may be considered, however will require pre-approval from the Authority prior to being spec'd or installed;

   b. Flexible metal conduit is not permitted without prior approval from the Authority;. Flexible metal conduit may be used for camera or WAP installations, using a six foot (maximum) whip, from the end of the EMT at the device location.

c. Conduit pathways in the slab are not the preferred method and should be avoided. Designer and contractor to utilize the plenum space.

3. J-hooks are an approved method for providing pathway, however require pre -approval prior to being designed or installed.

4. All communication conduits shall utilize compression fittings, reamed and threaded bushings installed. Throated bushings are not suitable for communications pathways.

   a. Install bushings prior to cable installation to properly protect the cable during placement;

   b. No thread ends shall remain exposed.

5. Antenna farms on the rooftops shall be fed with a minimum of (4) 4" conduits from the radio room.

   a. Conduits shall have long "extra sweeping" bends, which allow cables to fall into a cable tray;

   b. A ruggedized cable tray shall be placed on the roof to allow for antenna cables to be routed to the antenna locations from the conduit locations;

   c. Tray shall be installed using non-penetrating mounts;

   d. Antenna locations shall be placed with 15 foot separation;

   e. Antennas shall use non-penetrating, ballasted mounts Minimum 4 cinder blocks shall be used, however 6 is preferred:

      i. A One Inch thick rubber mat shall be placed between the mount and the roof membrane

      ii. Provide sufficient grounding methods for antennas and cable tray

9.3.2.2. CABLE TRAYS FOR COMMUNICATIONS SYSTEMS

1. Ladder Racking:

   a. Horizontal and vertical ladder cable runway shall be used in all Rack Rooms at the Airport;

   b. Ladder cable runway shall be a standard 18 inches wide and a rung spacing of 12 inches, mounted at least 8' (feet) 6" (inches) above the finished floor. Ideally, ladder cable runways should be mounted at 12 inches above the cabinets being served, with waterfalls installed above each cabinet/rack to maintain proper bend radii of cables;

c. Ladder cable runways installed within Rack Rooms shall be installed above the center-line of the cabinets from wall to wall and tee off at intervals not to exceed six feet. For a row of four cabinets or more, the cable tray shall tee off in at least two locations;

d. Vertical ladder cable runway shall be placed to allow proper cable routing wherever U/G conduits enter a room. Ladder cable runway shall be installed from the floor to the bottom of the horizontal ladder cable runway. Instances where Rack Rooms are stacked in a multi floor environment with sleeve penetrations in the floor and upper deck, ladder cable runway shall be installed floor to ceiling, or from the top of the horizontal ladder rack to the sleeve penetrations above, if the penetrations from floor to floor are not stacked;

e. Ladder cable runway parts and interconnections shall be bonded to a #6 AWG copper conductor and connected to the grounding bus bar.

2. Cable Trays:

   a. Cable trays shall be wire basket style cable trays, preferably;

   b. Cable trays shall be a standard of at least 18 inches wide, 6 inches deep and mounted at least 8' (feet) 6" (inches) above the finished floor;

   c. Cable trays shall be metal, suitable for indoors and protected against corrosion by electroplated zinc galvanizing, complying with ASTM B 633, Type 1, not less than 0.000472 inch thick;

   d. If cable tray is installed in an outdoor environment, ensure the coating is suitable to withstand the elements and avoid corrosion;

   e. Cable trays shall be installed above the common corridor. In areas with diverse architecture pre-approval for cable trays must be obtained;

   f. Cable trays parts and interconnections shall be bonded to a # 6 AWG copper conductor and connected to the grounding busbar.

9.3.2.3. UNDERGROUND DUCTS AND RACEWAYS FOR COMMUNICATIONS SYSTEMS

1. Backbone conduits for communications systems shall be 4" conduits;

2. Duct banks shall have a minimum of (4) 4" conduits;

3. Conduit duct banks located on the Airside shall be encased; Encasement shall be dyed orange ion color.

4. Conduit duct banks not located on the airside are not required to be encased, with the exception of providing encasement where conduits make turns;

5. Communication conduit encasements shall be colored orange;

6. The Authority installation standards require underground communications ductbanks to be installed no less than 24 inches below finished grade. Top of the conduit ductbank shall have 24 inches of cover to the finished grade. Exceptions can be made for 18 inches of cover, with proper approval by the Authority prior to installation;

7. Reinforced orange-colored detectable warning tapes shall be installed 12 inches above conduit to prevent accidental dig-ups and interruption of service;

8. Conduits shall have long sweeping bends;

9. Conduits shall have a mule tape installed within them;

10. All Rack Rooms shall connect to the Server Room (SR) with a minimum of four 4 inch conduits;

11. Adjacent Rack Rooms sharing a common wall, shall connect to each other with a minimum of two 4 inch conduit sleeves utilizing the appropriate fire sealing requirement to maintain the current rating of the wall and/or fire suppression requirements;

12. Backbone pathway shall be individual, physically diverse, redundant pathways feeding each Rack Room from the SR utilizing cable tray or conduits as appropriate;

13. Every Rack Room on the level immediately below the rooftop shall provide for connectivity to the rooftop utilizing 4 inch conduits as permitted by the Authority;

14. One 4 inch conduit entering a Rack Room and one 4 inch conduit leaving the Rack Room shall have (3) three-celled fabric ducting (total of nine cells) installed with pull strings with distance in feet. Fabric inner duct shall be 3 inches wide;

15. 2 inch conduits shall have (1) three-celled fabric ducting (total of three cells) installed with pull strings with distance in feet. Fabric innerduct shall be 2 inches wide;

16. Empty conduits shall have approved caps installed after pull strings have been installed. Conduit plugs shall withstand 15 psi of pressure.

17. Conduits with cables installed shall be sealed with a pre-approved method and/or manufacturer approved method (i.e. inflatable bags for conduits with maxcell). Expansion foam is not permitted for use in any application.

18. Distances up to 600 feet in a straight run, can be installed without a manhole or handhole.

    a. Runs that aren't straight will require manholes or handholes placed at a maximum distance of 400 feet apart.

19. Handholes shall be a minimum of 4x6 to ensure proper racking of cable slack.

    a. 25 foot service loop required in all handholes and manholes.

    b. Racking shall be installed in each handhole or manhole.

20. New manhole dimensions shall not be less than 8 feet long x 6 feet wide x 8 feet 6 inches high (8' x 6' x 8'-6"), unless pre-approved by the Authority;

21. Manholes and hand holes shall have ground rods;

22. The Authority does not allow direct burial cables.

9.3.2.4. COMMISSIONING FOR COMMUNICATIONS SYSTEMS

1. Commissioning and testing of all cables shall comply with industry standards related to CAT3, CAT6, CAT6a and Fiber Optic testing parameters.

2. CAT3:

    a. DC loop resistance

    b. Continuity

    c. Length

    d. Attenuation

3. CAT6 and CAT6a Cabling (minimum requirements):

    a. Wire Map

    b. Length

    c. Attenuation

    d. Near-End Crosstalk

    e. Propagation Delay/Delay Skew

    f. Power Sum Near End Crosstalk (NEXT)

    g. Attenuation to Crosstalk Ratio / Power Sum Attenuation to Crosstalk Ratio

    h. Equal Level Far End Crosstalk (ELFEXT)

    i. Alien Crosstalk (AXT)

    j. Return Loss

4. Fiber Optic Testing Requirements:

   a. The Authority has the right to observe and verify all fiber optic tests. The Installer shall notify the Engineer one week prior to testing so that testing can be observed. The Authority will require the Installer to retest at the Installer's own expense if the tests are conducted without properly notifying the Engineer;

   b. Testing of all fiber optic cables shall occur on the reel with an OTDR prior to installations, to ensure there are no damages from the manufacturer. All strands shall be tested, unless otherwise noted by the Engineer or The Authority and test results to be included in the overall documentation provided by the contractor;

   c. The Installer shall use "Two (2) Jumper Reference" when referenced specification is not directed by primary specification to create reference test levels. The reference connections resemble those used during the actual loss test, which means that the same detectors are matched to the same sources for both the reference and the test:

      i. Before starting any new testing session or when a test jumper has been disconnected from the source port of either test set, the two jumper reference shall be repeated.

   d. Test equipment shall be factory calibrated on an annual basis, unless the manufacturer recommends this task to be performed more frequently;

   e. Test equipment shall have the most current calibration date indicated on the equipment:

      i. Evidence of calibration for test equipment shall be provided as part of the contractor's submittal package.

   f. Trained technicians who have successfully attended an appropriate training program and have obtained a certificate as proof thereof shall execute the tests. Certificates shall be provided as part of the contractor's submittal package. These certificates may have been issued by any of the following organizations or an equivalent organization:

      i. The manufacturer of the fiber optic cable and/or the fiber optic connectors.

      ii. Training organizations authorized by BICSI (Building Industry Consulting Services International with headquarters in Tampa, Florida) or by the Association of Cabling Professionals Cabling Business Institute located in Dallas, Texas.

g. Cables shall be tested Bi-Directionally using and Optical Power Meter;

h. Cables shall be tested in a single direction using an Optical Time Domain Reflectometer (OTDR):

   i. Fiber Optic tests shall be performed using both wavelengths.

9.4. STRUCTURED CABLING

9.4.1. COMMUNICATIONS EQUIPMENT ROOMS

1. Important room types in the Airport infrastructure:

   a. Server Room or Computer Equipment Room (SR or CER): SR/ CER is a structured cabling system connection point between entrance cables, equipment cables, inter-building backbone cables, and intra -building backbone cables of the core network. It is the centralized portion of the backbone cabling used to mechanically terminate and administer the backbone cabling, providing connectivity between equipment rooms entrance facilities, horizontal cross- connects, and intermediate cross-connects.

      i. The Airport SR/CER's shall not be placed in the Common Area of the terminals. Back of house in a restricted/secure area is preferred.

      ii. Tenants' SR's shall be placed in their respective leased space.

   b. Rack Room (RR) is a combined shell that houses Security, Information Technology/ Telecommunication, and Common Area systems and equipment in different compartments or segments within the shell. The compartments or segments are separated by a wire mesh fence. Each compartment has an outward swing door that is controlled by Access Control System (ACS) for entry. In addition to voice, data, security and wireless systems, RR's can house equipment for life safety/fire systems, and building automation systems.

      i. Airport RR's shall not be placed in the Common Area of the terminal.

      ii. Airport security equipment and airport network equipment must be housed on the secure side of the wire mesh fence.

iii. A typical RR at the Airport is illustrated in Figure 1 in Section 9.2.

2. The environment surrounding the location of an SR or RR must be free from sources of electromagnetic interference. Wherever RR's are adjacent to electrical rooms with transformers on the opposite walls, install a 1/4-inch copper meshing within the wall to reflect electromagnetic interference / electromagnetic compatibility;

3. It is highly recommended that the immediate environment surrounding a RR should not contain HVAC equipment such as steam boilers, compressors, chilled/hot water pipes, elevator equipment, electrical co-generation equipment or waste processing;

4. SR's and RR's shall not contain any overhead piping systems that contain water, storm drains or other fluid materials. If required to run any of these systems through the SR or RR then a waiver shall be acquired and secondary containment shall be provided;

5. It is highly recommended that the location must be above any potential flood zones, including being located below or adjacent to rest rooms and restaurants. If this is not possible then provisions should be taken within the wall construction containing wet utilities to avoid flooding into the RR. Also provisions should be taken to assure all equipment is not located or mounted within the first few inches of the floor where possible. Additionally, there shall be water and fluid sensors installed within such rooms and integrated with the Building Management System (BMS) for monitoring and alarm of possible flooding and water leaks.

   a. Where RR's cannot be located away from potential flood zones, floor drains are recommended to be installed in adjacent plumbing chases, and concrete curbs should surround the RR, providing additional protection.

6. RR's need to be accessible from a corridor, stairwell, and/or a service elevator large enough for cabinet and equipment loading and servicing;

7. The location and quantity of telecommunications (RR or IT) rooms shall be designed so that the maximum distance from these rooms to any network field device that the room supports shall not exceed 250 feet via the longest possible route (i.e. right angles) traveled by the cable from the room to the field device. This includes all work area outlets, ACS card readers, cameras, access points, displays, antennas, etc.

a. If the distance from the RR to the furthest network field device exceeds 250 feet via the longest possible route, then another RR shall be installed to accommodate the distant field devices to maintain the 250 foot limitation.

b. Authorization may be requested to utilize other transmission media type to exceed 250 feet, however those must be pre-approved by the Engineer or the Authority and not be designed into the initial design.

8. If more than one RR is installed within a building/terminal, then a SR/CER shall be identified which will be larger than the other RR's and serve as the central hub for that building/terminal.

9. In a multi-level building, RR's on different floors should stack on top of each other. Straight vertical cable risers should be established for the purpose of cable routing;

10. Actual RR size shall be determined by the number of racks/cabinets, space needed to access racks/cabinets, space needed for an appropriately sized Room UPS, appropriately sized HVAC equipment, Clean Agent system and bottle(s), or other mechanical or electrical equipment with at least minimum 3' clearance as outlined within specific code requirements, such as the NEC code and BICSI standards:.

    a. The size of a RR that contains active equipment shall never be less than 12'x12'.

    b. Design of a RR should plan for 100% growth.

11. Drop or false ceilings are not permitted;

12. Floor should be covered with static resistant materials and its static resistant properties should be permanent regardless of temperature, humidity, maintenance or traffic:

    a. Flooring must not contribute to static generation.

    b. Flooring must be groundable after it is installed.

13. Floor loading for general RR's shall be designed to support a minimum dead load 100 lb/ft2;

14. Floor loading for SR's/CER's, shall be designed to support a minimum dead load 250 lb/ft2;

15. Minimum ceiling height is twelve (12') feet;

16. Walls of a RR or SR shall have fire rated plywood on all walls mounted vertically starting at 6" above finished floor. Top of plywood should be at 8'6" above finished floor:

    a. Plywood shall be painted sufficiently to not allow bleed through from plywood, of white, low VOC paint leaving the Fire Retardant-Stamp(s) exposed for inspection.

b. Cutouts for electrical switches and outlets shall be provided in the plywood.

18. Minimum door size is 36 inches wide x 80 inches tall, and should swing outward;

19. All doors shall utilize dual ACS card reader for access and exiting, with a electromagnetic lock and panic hardware. ACS doors are not to be integrated with the building fire alarm system;

20. All ACS doors that have door controllers and/or power supplies within them, shall have a key switch override located adjacent to the card reader, which will cut power to the magnetic lock and allow access to the area utilizing a key.

21. Door signage will need to comply with the Authority's practices and shall be indicated by room number and access control code and any other regulatory signage required by the Authority;

22. All RR's serving active equipment shall have dedicated electrical panels located within the RR's;

23. Electrical panels serving active equipment shall be separate from those serving lighting. Lighting panels should not be located within RR's;

24. Except for special power requirements, each individual equipment cabinet or equipment rack shall have two separate, dedicated, 120 VAC, 30 amp circuits feeding them. All outlets shall be isolated ground with twist lock receptacles:

    a. Two (2) PDU's/power strips shall be provided for each rack or cabinet, which shall plug into the 2 dedicated circuits.

25. There shall be 120 VAC, 20 amp, non-switched, double duplex receptacles installed every six (6) feet along the walls of the room, for convenience power;

26. All electrical panels in RR's shall be fed from a UPS system that is also connected and backed up by the emergency generator to the building. The panels that are connected to the UPS shall be labeled as being connected to emergency power. All UPS shall have the Emergency Power Supply feed as fallback feed.

27. UPS within rooms shall provide standby power for all networked equipment within the room, to include security door control panels and power supplies

for electromagnetic locks, which will be further backed up by the emergency generator;

28. Generator and UPS installations shall be sized for the load they are expected to serve, plus fifty (50) percent. Generator power must be sustainable for a minimum duration of four (4) hours. In the event of an outage lasting longer than four hours, additional fuel will be required;

29. UPS's shall be sized to handle the load for a given TR or SR for a minimum of 1 hour;

30. UPS's shall have an Ethernet communications port for LAN management to allow for remote monitoring;

31. Lighting shall provide a minimum of 50 foot candles measured at three foot three inches (3' 3") above the finished floor. The Lighting shall be positioned to allow for adequate lighting in front and back of cabinets/racks;

32. 10,000 BTU's of heat dissipation per cabinet shall be used as a minimum for planning purposes with a set of redundant air conditioning units. HVAC designer shall coordinate actual HVAC requirements with the Authority's I&TS and shall be provisioned for 24 hour 365 day, continuous service;

33. A thermostat shall be provided within the RR. Room over-temperature and cooling unit failure shall be alarmed at the Facilities Management Office, and the Central Utility Plant (CUP). These should utilize the BAS for notifications.

34. Temperature monitor shall be installed in all RR's and SR's, which will be connected to the ACS door controller, and provide alarms within the Security Operations Center,.

35. Inside temperature shall be maintained between 68 ˚F to 72 ˚F, and between 30% - 55% relative humidity;

36. At a minimum, a Clean Agent Fire Suppression System shall be installed for all RR's and SR's:

    a. If the Authority Having Jurisdiction (AHJ) requires additional protection beyond a clean agent system, a pre -action sprinkler system is acceptable.

    b. A "Wet to the Head" sprinkler systems should be avoided when designing a SR or Rack Room.

    c. If a Pre-Action system is required by code, sprinkler head placement design should be performed to minimize any sprinkler head placed directly above equipment cabinets or racks.

37. All SR's and RR's shall be equipped with a VoIP telephone. The communication apparatus shall be situated adjacent to the door and in close proximity to the Clean Agent pull stations and abort control.

38. All SR's and RR's shall have cameras mounted on the outside and interior of the room unless waived (approved) by AVSEC and Public Safety Department as well as the I&TS Department. Contractor shall field coordinate with AVSEC Authority for interior camera placement. SR and RR doors may also be connected to a biometric reader for entry and exit as approved and required by AVSEC/PS;

39. All Generator, UPS, HVAC units should have proper conduits to support Ethernet connectivity for BMS and security operations center for control and monitoring.

9.4.1.1. COMMUNICATIONS ENTRANCE PROTECTION

1. Where copper cable pairs are placed underground and between buildings, electrical protection from lightning for every pair with solid state type protectors at both ends, is required.

2. Furnish and install the appropriate amount of multi-pair protector panels with 110 connector system and all related components

9.4.1.2. COMMUNICATIONS CABINETS, RACKS, FRAMES AND ENCLOSURES

1. Provide freestanding equipment cabinets to store computer, data storage, networking and security equipment in the data centers computer rooms and equipment rooms. Each cabinet enclosure shall have a rectangular frame and removable top panel, side panels and doors. Installed cabinets shall include thermal, power, and cable management accessories that control airflow through the cabinet and keep network and power cables separate and organized;

2. Currently, the Authority has standardized on the CPI Cabinets, white in color; for rooms needing cabinets installed. Where rooms design with rely racks, the Authority has standardized on the CPI 19" wide 6" deep rack, utilizing double sided vertical managers on either side of the racks.

3. The cabinet frame shall include leveling feet and casters. The cabinet frame shall support 3000 lb (1360 kg) of equipment when supported on leveling feet and secured to the structural floor. The cabinet frame shall support 2250 lb (1020 kg) of equipment when moved or supported on casters;

4. Each cabinet shall include two pairs of equipment mounting rails. Mounting rails shall clamp to the side supports located near the top, middle and bottom of the frame and shall be fully adjustable in depth to provide front and rear support for equipment. Equipment Mounting Rails shall be spaced horizontally to support 19" (482.6 mm) wide EIA/ECA-310-E compliant rack-mount equipment and shall provide a minimum of 38" (965 mm) of rail-to-rail depth for equipment. Mounting rails shall be square-punched according to the EIA/ECA-310-E Universal hole pattern with equipment mounting holes on alternating 5/8" – 5/8" – 1/2" (15.9 mm – 15.9 mm – 12.7 mm) vertical hole centers. Square-punched holes shall accept cage nut hardware with various threads. Rack mount spaces or units (U) shall be 1-3/4" (44.45 mm) high and shall be marked and numbered on the mounting rails. Numbering shall start at the bottom of the rail. Mounting rails shall provide 42U for equipment;

5. Adjacent cabinets containing like equipment do not require separate side panels; only side panels on the ends;

6. Adjacent cabinets containing unlike equipment (i.e. security and LAN), must be physically separated with side panels;

7. The cabinet shall be a minimum of 79.3" (2013 mm) high by 23.6" (600 mm) wide by 39.4" (1000 mm) deep when casters, doors and side panels are installed;

8. Each cabinet shall have (2) full-length, minimum 12-receptacle, 110VAC, 30A, power strip with a 9 foot power cord on either side, at the rear of the cabinet:

   a. The cabinet shall include PDU mounting brackets. The brackets shall be L- shaped, shall attach to the rear right or left corner of the cabinet frame and shall include tool -less mounting points for two vertical rack-mount power distribution units (PDUs) or power strips. The brackets will orient the PDUs/power strips so that the outlets on the PDUs/power strips face the center of the cabinet frame;

   b. PDU cords shall be long enough to plug into the receptacle at the top of the cabinet, or into a rack mounted UPS (if one is designed as such).

9. Each installed cabinet shall be equipped with an integrated vertical cable manager to organize network cables. The vertical cable manager shall attach to the side of the equipment mounting rail in the cabinet. The vertical cable manager shall have cable openings along the side that align with each rack-mount unit (U) space on the mounting rail. The openings shall be

sized to allow 24 patch cords to enter each rack-mount unit (U) space. The cable openings shall be separated by plastic T-shaped cable guides to route cables into each space. Frames or Cabinets shall have sufficient space to access vertical cable management. This may require wider cabinets, or adjustment of the rails to ensure access can be achieved;

10. Each installed cabinet shall be equipped with a rack-mount horizontal cable manager to organize cables in the rack-mount unit spaces above and below each patch panel or network switch within the cabinet. The horizontal cable manager shall be 19" EIA rack-mount and 2U high. The horizontal cable manager shall be a single-sided U-shaped trough with a front-facing snap on cover. Plastic T-shaped cable guides along the top and bottom edge of the cable manager shall divide cable openings that allow cables to exit or enter the top or bottom of the manager. The cable manager shall be made of plastic, at least 5.9" (150 mm) deep and shall be sized to hold 24 patch cords per rack-mount unit (U) space;

11. Provide hardware for attaching ladder rack (cable runway) to the top of the cabinet. The hardware shall attach the ladder rack in parallel (side-to-side) orientation and will elevate the ladder rack a minimum of 2" (50 mm) above the cabinet.

12. Outdoor IT Design Requirements

a. Outdoor IT Enclosures shall be NEMA 4 Enclosure with a 3-point locking latch which can accept a standard Medeco locking hasp. Enclosure shall be a minimum of 36"W X 36"H X 12"D. This size requirement can be reviewed during design phase when active and passive requirements which need to be housed in the enclosure are known. There shall also be a plywood or metal backboard preinstalled within the enclosure in order to mount equipment. All conduits shall enter from the bottom of the enclosure.

b. Outdoor enclosure doors, center section and wall section are provided with ground studs to facilitate proper bonding and grounding of the cabinet.

c. Outdoor enclosure shall contain seamless, foam-in-place gasket prevents contaminants from entering the cabinet.

d. Enclosures shall be installed so that the hinged front section can be opened and rotated to its fullest extent allowing full access to equipment.

e. Any active equipment placed in an Outdoor Enclosure shall be "hardened" and capable of operating without dedicated cooling and ventilation.

f. Outdoor Enclosures shall be supported by a 12 Strand SM fiber from the nearest Rack Room.

9.4.1.3. COMMUNICATIONS TERMINATION BLOCKS AND PATCH PANELS

1. All fibers shall be terminated with standard LC connectors in fiber patch panels:

   a. The Authority currently standardizes on Corning for all fiber optic cabling applications.

2. All CAT6 Data Unshielded Twisted Pair (UTP) cables shall be terminated on CAT6 RJ45 (or manufacturer specified) patch panels inside the equipment rack.:

   a. The Authority currently standardizes on CommScope Uniprise CS37P or Systemax as their connectivity solution.

3. Wi-Fi connectivity shall utilize CAT6a UTP cables, and be terminated on separate CAT6a RJ45 patch panels than other CAT6 cabling:

   a. The Authority currently standardizes on CommScope Uniprise or Systemax as their connectivity solution.

9.4.1.4. COMMUNICATIONS COPPER BACKBONE CABLING

1. Where Voice over Internet Protocol (VoIP) is specified, verify design criteria involving copper cabling;

2. Install sufficient pairs of UTP from the MPOE or SR, to all other RR's, to cover current and future needs of telephone services and data circuits for the area served by that particular RR.

   a. Pair count requirements per RR will be determined on a case-by-case basis, however a minimum of 50-pair will be required.

3. Sufficient telephone wire-pairs from telecommunications service provider shall also be brought into the MPOE of the building to cover current and future needs of telephone wires and data circuits for the building. Design of conduits and rooms need to account for these needs;

4. Copper backbone terminations shall be performed on 110 style, 300 pair blocks.

   a. 66 blocks may be used for airlines and in certain MPOE locations. Verify with Airline tenant and/or Authority prior;

5. Voice tie cables from the 110 fields to the rack shall be in a minimum of 50 pair increments and terminate on voice

grade patch panels with two pairs per port.

a. Voice patch panels shall not be the circuit board style panels. Patch panels must have the flexibility to have pair allocated to all pins to provide various pinout options, based on circuit types (i.e. ISDN, T1… etc.);

6. Copper backbone connections feeding the RR from a SR or CER or MPOE and voice tie cables can be terminated on the same 300 pair block, however cables being fed from the RR to other locations, such as tenants, should be terminated on a separate block;

7. Wire management for cross connect wires shall be provided above and below (and in between where applicable) the 300 pair blocks.

9.4.1.5. COMMUNICATIONS OPTICAL FIBER BACKBONE CABLING

1. A minimum of 72 strand single mode fiber cables are required for intra-building connections. (per redundant path).

   a. This applies to connectivity between SR/CER's to RR's;

   b. This applies to connectivity between a building central connectivity room and outlying RR's or IDF's.

2. Inter-building fiber connectivity shall be coordinated with the Authority prior to the design being finalized.

   a. Installers are required to be an active and current member of the Corning NPI program to provide a 25 year warranty upon successful completion of an installation and review of test results.

3. Fiber connectivity must support a minimum of 10Gb with future abilities to support 40Gb and 100Gb bandwidth requirements.

4. Backbone fiber cable composition shall be loose buffer tube. Each buffer tube shall contain 12 strands of fiber.

5. Fibers Optic cables shall have a service loop coiled in each manhole and on each end inside communication rooms. These cables shall be dressed neatly and secured to the inside walls of the manholes utilizing a cable management system within the vault (i.e. racking) or fastened neatly and securely to ladder racking within RR's.

6. 50 foot service loops to be provided within each manhole and 25 foot service loops to be provided in each hand hole and inside communication rooms.

   a. Service loops to be coiled neatly and secured to racking within the manhole or hand hole.;

b. Service loops inside communications rooms can be secured to plywood backboards or to the ladder racking. Confirm with the Authority during field installation.

7. Fibers optic cables that are run underground shall have three labels attached. One label shall be attached on the spare coiled-up fiber or in the center between the entrance and exit of the manhole. One label shall be attached within twelve inches of the entrance and one label within twelve inches of the exit of the conduits in the manhole.

9.4.1.6. COMMUNICATIONS OPTICAL FIBER SPLICING AND TERMINATIONS

1. Fusion spliced connectorized pigtails shall be used as a means of cable termination, and spliced to the cable. Connectors shall not be installed and polished in the field.

   a. Single-mode, 2 meter length, ultra PC polish, LC connector, fusion spliced, heat shrink protected on the splice;

   b. Pigtail, fan out kits and tight buffer slack shall be housed in slack cassettes within the fiber enclosure.

2. Blue-colored adapters shall be used for single-mode connections.

3. If splicing fiber using a splice case:

   a. Use metallic splice trays that contain 24 splices with foam combs and pads for fiber strain relief;

   b. Trays shall be stackable, contain a plastic polycarbonate protective cover, and have a hole in the center for vertical and horizontal mounting;

   c. Splice cases shall be water tight and re-enterable. Secure all cables in the splice case and end plates in accordance with manufacturer's specifications, ensuring a watertight seal.

   d. Exercise special care when assembling the case as to not damage any conductors and/or splice modules. Splicing technicians must have a manufacturer's installation certification for the splices and splice cases being installed;

   e. The splice enclosure shall not be flooded with encapsulate;

   f. Perform a pressure test each case for leaks at 12 psi, ensuring a watertight seal;

   g. Bond the cable's metallic sheath/ shield (if armored) to the metallic splice case with the bonding bar assembly provided with the splice case, and in accordance with manufacturers specifications.

4. Mechanical splices are not permitted at the Airport.

    a. In the event of an emergency to repair a mission critical segment of cable, or mission critical system, mechanical splices may be acceptable until such time a permanent solution can be put in place.

9.4.1.7. COMMUNICATIONS COPPER HORIZONTAL CABLING

1. The Authority's current preferred structured cabling system is the CommScope Uniprise 400Mhz solution or Systimax 500MHz solution. Contractors installing either of these structured cabling solutions (or equivalent), must be certified and an active member of their respective certified installer programs and shall provide a 25 year warranty on the installed structured cabling system.

    a. The Authority's horizontal PDS cable jacket shall be green in color;

2. CAT6 cables shall be used as a universal cable for all TELECOMMUNICATIONS needs, including telephone, data, fax, video, audio, low voltage lighting, etc. CAT6, 4- pair, UTP cables shall be installed at all conceivable required locations and for future expansion needs;

3. CAT6A cabling shall be used when providing connectivity for Wireless Access Points (WAP's);

4. Each location shall be installed with a minimum of two, CAT6, UTP cables.

5. Wireless Access Points shall have a minimum of two "CAT6A" UTP cables. Both cables should be plugged into both access point and the switch.

6. A pull cord (nylon; 1/8" minimum) shall be co-installed with all cable installed in any conduit;

7. Cables shall be installed in continuous lengths from origin to destination (no splices) except for transition points, or consolidation points, which must be approved by the Engineer and the Authority.

    a. Authority standard is a maximum 250 foot permanent link segment;

8. Cables shall not be attached to or laying across ceiling grid wires, lighting fixture wires seismic control wires, conduits, air ducts or any other utilities that may reside in the ceiling plenum. If cable is not installed within conduit or cable tray, appropriate support systems must be installed;

9. CAT6 or CAT6a cables installed within underground conduits must be outside plant rated. Where the manufacturer can't provide an outdoor rated cable at the required bandwidth and only can provide a cable at a lesser or higher bandwidth, a lesser bandwidth should not be considered.

10. Outdoor CAT6 or CAT6a cables shall be grounded via a primary or/and secondary method based on the application."

9.4.1.8. COMMUNICATIONS OPTICAL FIBER HORIZONTAL CABLING

1. Before installation, while the fiber optic cable is still on the reel, the Installer shall test each individual fiber strand with an OTDR for transmission anomalies and length. Single-mode fiber shall be tested at 1310 nm, and multi-mode fiber shall be tested at 850 nm.

   a. The Authority has the right to observe and verify all tests. The Installer shall notify the Engineer one week prior to testing so that testing can be observed.

2. Pre-installation test results shall be recorded and given to the Engineer in electronic form with the software to view the test results if necessary. These results shall be given to the Engineer prior to installation. There shall be no deviation from these initial test procedures;

3. Fiber optic cables that are run underground shall have three labels attached. One label shall be attached on the spare coiled-up fiber or in the center between the entrance and exit of the manhole. One label shall be attached within twelve inches of the entrance and one label within twelve inches of the exit of the conduits in the manhole;

4. Both Single Mode and Multimode connectors shall be LC type connectors;

5. All fiber must be terminated and labeled, unless specified by the Engineer;

6. All test equipment shall be calibrated by a certified laboratory, or the manufacturer annually and such certification shall be submitted to the Engineer prior to testing and include the following:

   a. Date of calibration;

   b. Calibration due date;

   c. Identification of the organization performing the calibration;

   d. Calibration shall be traceable to the National Institute of Standards and Technology (NIST). Calibration intervals shall be based on the type of tool and records of the tool calibration. Intervals may be lengthened or shortened on the basis of stability demonstrated over previous calibration periods.

9.4.1.9. COMMUNICATIONS FACEPLATES AND CONNECTORS

1. Work area outlets shall contain (6) 8-position RJ45 type modular jacks positions in single faceplate for used with snap-in jacks accommodating any combination of Unshielded Twisted Pair (UTP), optical fiber, and coaxial work area cords, regardless of the number of cables being installed;
    a. All unused ports shall be blanked out for future use.
2. Stainless steel faceplates may be required when required to maintain proper architectural appearances;
3. Work area outlet boxes shall be flush-mounted and located adjacent to a power receptacle;
4. Work area outlets shall be neatly and professionally labeled at the outlet (machine printed using adhesive-tape label for cable), on the front of the wall plate or under the clear snap in label covers, as well as in the RR.
    a. Faceplates should identify the RR the cable originates from, the Cabinet it is terminated within, the patch panel shelf, and the patch panel port number.

9.4.1.10. COMMUNICATIONS CONNECTING CORDS, DEVICES, AND ADAPTERS

1. Must be of the same grade and manufacturer as the horizontal cabling. i.e. CAT6 or CAT6A:
    a. Data/Ethernet cords: Blue
    b. VoIP cords: Blue
    c. WAP connections: White
    d. Servers and switches: Yellow
    e. Security: Red
2. Cross-Connect Color Coding:
    a. Standard POTS lines shall utilize White/Blue wire;
    b. Data circuits shall utilize Yellow/ Blue wire
3. Single-mode and Multimode jumpers shall be LC type, unless otherwise required for equipment interface;
4. For single fiber circuits, use single strand (simplex) jumpers. For duplex fiber circuits, use zipcord jumpers;
5. Media converters are recommended to be chassis mount.

a. In cases where chassis mount converters cannot be utilized, media converters must be placed and secured on a shelf within a cabinet or rack.;

b. The Authority currently standardizes on Transition Networks converters.

9.5. DATA COMMUNICATIONS

9.5.1. DATA COMMUNICATIONS SWITCHES

PLEASE SEE NOTE 01 AT END OF 9.5

The Authority's network utilizes Cisco's Software Defined Network (SD-Access) for its campus network. The following guidelines reference equipment that satisfy the requirements of an SD-Access network. Every bill of Material for IT equipment needs to be approved by the Airport Authority IT Department before the purchase order can be executed.

1. For distribution Switch Layer, the Authority currently uses the Cisco 9500X/ 9606R (chassis) with C9600X-SUP-2 for the Distribution Layer. Collaborate and coordinate with I&TS for the exact equipment model to be chosen based on requirements and design specifications prior to procurement.

2. For Software Defined Networking access switches, the Authority currently utilizes the Cisco C9300X access switch model. SFP modules shall be provided by the Contractor and fully populate the switch, based on type. Verify during design and prior to procurement the need for 1G, 10G, 25G, 40G or 100G uplinks.

   a. C9300X-48HX: 48 Cisco UPoE+, 48x 10G Multigigabit (100M, 1G, 2.5G, 5G, or 10 Gbps) w/W 90WUPOE+

   b. C9200CX 12 Port Data: 12 x1G data; 2x 1G CU and 2x SFP + uplinks; UPOE+ powered

   c. C9300X-NM-4C: 4x100/40G QSFP network module

   d. C9300X-NM-2C: 2x 100/40G QSFP network module

   e. C3900X-NM-8Y: 8x 25/10/1G network module

   f. IE-3400 ruggedized switch

   g. GLC-LH-SMD (1GB SFP)

   h. SFP-10G-LR (10GB SFP)

   i. QSFP-40G-LR4 –S (40GB SFP)

   j. SFP-10/25G-LR-S

3. Network switches being implemented at the Airport shall have 25% spare capacity upon completion of the installation. A new switch will be provided whenever the 25% is impacted.

   a. This also applies to existing switches being utilized. When the 25% spare capacity is encroached upon, a new switch shall be provided.

4. Network switches shall have redundant and diverse network paths from the access to the distribution layer, whenever possible

5. Network switches shall have dual power supplies. Collaborate and coordinate with ADC and/or I&TS when utilizing equipment that cannot meet this requirement.

   a. Power supplies shall plug into different circuits within the cabinet they are installed in

6. At the time of writing Security and Admin networks physically reside on separate network switches. The Authority is currently undergoing an initiative to combine the Security and Admin networks on to one switch where feasible. Verify and coordinate with ADC and I&TS during design and prior to procurement.

7. Label all network switches and patch cords. Naming convention will be provided by I&TS.

   a. Label network equipment (front and back);

   b. Label copper/fiber patch cords on both ends (each end has the next hop) so that the label is visible as much as possible

The Authority utilizes DNA software subscription for Software Defined Networking devices and Smartnet for both SDN and non-SDN devices as follows:

1. Smartnet: core, distribution, routers, firewall, 24x7x4.

   a. 5 year SNTP (SMARTnet 24x7x4) - Advance Replacement parts on a Four-Hour Response basis twenty-four (24) hours per day, seven (7) days per week, including Cisco observed holidays access switches 8x5xNBD.

2. Access switches (8x5xNBD)

   a. 5 year SNT (SMARTnet Standard 8x5xNBD) - Where Next Business Day delivery is available, an Advance Replacement will ship to arrive the next Business Day provided that Cisco's determination of Hardware failure has been made before 3:00pm Depot Time. If Customer makes a request after 3:00pm Depot Time, Cisco will ship the Advance Replacement the next Business Day.

3. Software Subscription: Cisco DNA 5 year licenses:

a. For the Cisco C9300X-48HX switch, the associated licenses that need to be purchase are:; DNA Advantage per switch, 100 ISE-A, 100 Stealthwatch flow licenses, and Thousand Eyes license

b. For the Cisco C9200CX 12 Port Data UPOE+ powered switch, the associated licenses that need to be purchased: DNA Advantage per switch, 25 ISE-A, 25 Stealthwatch flow licenses, Thousand Eyes licenses

c. For Cisco 9136 AP Series and IW9167EH-AP, the associated licenses that need to be purchased are: DNA Advantage per AP, 25 ISE-A, 60 Month DNA spaces—ACT level license per AP license

4. Verify and coordinate with ADC and I&TS during design and prior to procurement, the switches needed to perform the intended scope of work.

5. Due to how technology progresses, this section shall be reviewed quarterly to determine if updates are required. Coordinate with ADC and I&TS for review.

9.5.2. DATA COMMUNICATIONS WIRELESS ACCESS POINTS

PLEASE SEE NOTE 01 AT END OF 9.5

The Authority uses Cisco products to support WiFi through the terminals and around the campus. The following points layout the equipment and guidelines for WiFi infrastructure. Please note each building will be different and they each need to be looked at on a case-by-case basis for which density is required.

1. Indoor Wireless Access Points:

   a. Cisco Catalyst 9136 Series

2. Outdoor Wireless Access Points:

   a. Cisco Outdoor AP Model: Cisco IW9167EH-AP

3. Access points are placed in all SR/CER/RR's:

4 Coverage areas are classified four ways; Ramp Coverage, Low Density areas, Medium Density and High Density areas. Refer to Charts in Section 9.5.2.for further information.

   a Ramp Coverage: Typically covered with two or three AP's using outdoor rated omnidirectional and directional AP's and ensuring coverage f rom the tail of the aircraft to the building. Coverage is intended for use by Airline ground service technicians and airline staff. Both sides of the aircraft need coverage.

      i. Airport WIFI is not designed to provide coverage inside an aircraft, however signal bleed may occur.

   b. Low Density Coverage: Classified as all non-passenger related office space and/or non-essential airport operations areas;

WI-FI Users	How Defined
Passengers while in transit	Signal strength no less than –67dBm Overlapping coverage may occur with an overlapping AP no less than—75dBm

WI-FI Users	How Defined
Non Passenger Vendor/Tenant Occupied Spaces Non-Essential Airport Operations Areas	Signal strength no less than –75dBm

c. High Density Coverage Areas where high density of users will congregate (hold rooms, food courts, etc.) Users in this anticipated to be streaming internet content, see table below.

Parameter	Description	Value—Large Gate ~800 Sq. Ft	Value—Small Gate ~400 Sq. Ft
Number of Passengers	Normal Operations	175	100
Number of Passengers	Peak Operations	350	200
Number of Devices per Passenger	Average	2	2
Total Number of Devices	Peak Operations	700 / Gate	400 / Gate
Association Take Rate	Percentage of devices associated to network	75%	75%
Max Associations	Peak Operations	525 / Gate	300 / Gate
Device Duty Cycle	Devices actively sending / receiving traffic at any moment in time	25%	25%
Active Devices	Peak Operations	132/ Gate 119 operating at 5GHz 13 operating at 2.4GHz	75 / Gate 68 operating at 5GHz 7 operating at 2.4GHz
Active Devices per AP	Target Value	30 / AP	30 / AP
Number of AP's	= Active Devices/AP	4 / Gate	2.3 / Gate

d. Medium Density Coverage Classified as areas where passenger traverse, yet will not require a higher level of bandwidth. Is meant to provide seamless coverage to allow a client to remain online as they move about the terminals. Medium density AP's located neat hold rooms, which are higher density area, may serve as reserve capacity during peak operations within a higher density zone;

9.5.3. DATA COMMUNICATIONS DESKTOPS

The Authority has standardized on small form factor PC's for day-to-day users, FIDS, and security application workstations. Dell is the manufacturer deployed at the Airport.

Workstations:

1. Dell OptiPlex 3050 Small Form Factors 8 GB Memory
2. Intel i5-7500T Processor
3. 500GB Hard Drive

9.5.4. DATA COMMUNICATIONS HARDWARE

1. Servers:
   a. CISCO UCS / B200 Series M5 Blades or newer
   b. Dell VxRail PF570F
   c. RAM 512 GB
   d. No Disk,
   e. HP ProLiant DL 380 G9 or newer (high end)
   f. HP ProliantDL60 G9 or newer (low end)
   g. Ram 132 GB minimum
   h. 3(300 GB 10k RPM) disk raid 5 minimum
2. Software:
   a. Windows Server 2019 Standard and Data Center
   b. SQL Server 2019 Enterprise or newer
   c. SQL Cal or Per processor licenses
   d. VMware 6.7 or newer
   e. Veeam 10 or newer (Backup Software)
   f. Veeam One (Monitoring software)
   g. HP data protector 9.09 for physical servers
   h. Symantec Antivirus 14 or newer
3. Appliances:
   a. Infoblox (DNS/DHCP) Appliance

b. Forcepoint Solution V5000G5 or newer (Web filter)

4. Storage Solutions:

a. Primary 6 Node

b. NetApp: AFF200 or better SSD (4) drives and 40 TB capacity preferred

c. NetApp FAS2600 series for Backup and replication 120 TB or Greater

5. Backup Solutions:

a. FAS2600 series for Backup and replication for VMware

b. Cloud Backup Solution

9.5.5. TELEPHONE SYSTEM

The Authority currently utilizes the Cisco VoIP telephone system. The table shown to the right describes, in general, where VoIP phones and other telephone services are required.

1. Analog Voice Gateway:

a. Currently, IT&S are using VG310. Collaborate and coordinate with I&TS for the exact and latest equipment model to be chosen based on requirements and design specifications prior to procurement.

2. VoIP Phones:

Location	Quantity	Type
Ticket Counter 2 position counter	1	VoIP
Ticket Counter Model T Counter	1	VoIP
Gate Counter	1	VoIP
Gate Counter Lift Podium Passenger	1	VoIP
Boarding Bridge Server Room / Rack	1	VoIP
Room Main Electrical	1	VoIP
Rooms Elevator	1 2	VoIP POTS
Fire Alarm Control	2	POTS
Panels SSCP Lane—Red	1 per lane	Analog
Phones Executive Offices	1	VoIP
Offices and Cubicles	1	VoIP
Conference Rooms	1	VoIP Conference Phone

a. Currently, IT&S are using the 8000 series. Collaborate and coordinate with I&TS for the exact equipment model to be chosen based on requirements and design specifications prior to procurement.

**NOTE 01— It is a mandatory requirement for all Cisco equipment to be purchased or sourced through Authorized Cisco Channel Gold Partners. The latest list of gold partners can be found at the URL below:

https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/openBasicSearch.do?dtid=odiprc001257

The Bill of Material needs to be approved by the Airport Authority IT Department before the Purchase Order can be executed.

The Contractor/Vendor must comply with one of the following:

1. Contractor/Vendor shall certify that it is an Original Equipment Manufacturer ("OEM") Authorized Channel Partner as of the date of the submission of their offer, and that it has the certification/specialization level required by the OEM to support both the product sale and product pricing, in accordance with the applicable OEM certification/specialization requirements.

2. The Contractor/Vendor confirms to have sourced (or will source) all OEM products submitted in this offer from the OEM or through the OEM's authorized Channels only, in accordance with all applicable laws and current OEM's applicable policies, at the time of purchase. Unless otherwise specified, Contractor/Vendor shall warrant that all products are new and in their original box. Where applicable, Contractor/Vendor shall provide the Airport Authority with a copy of the End User license agreement, and shall warrant that all OEM software is licensed originally to the Airport Authority as the original licensee authorized to use the OEM Software.

The Cisco equipment must be registered as follows:

• End Customer and End User must be registered to SAN DIEGO AIRPORT AUTHORITY

• Smart Licensing must be registered to SAN DIEGO AIRPORT AUTHORITY

• Smartnet must be registered to SAN DIEGO AIRPORT AUTHORITY

9.5.6. AUDIO AND VISUAL PAGING

1. The paging system serves as a key element necessary to deliver a fully-integrated environment to the Airport. The system is a highly available, extremely flexible and deliver information and support services to both the traveling public and airport and airline personnel, as well as integrating certain functions and

activities with other systems within the Terminal, based on rules-driven management.

2. The PA system is designed to serve public area needs and will be designed as a microprocessor-based Internet Protocol (IP) system that automates the initiating and retrieval of announcements, including audible and visual announcements.

3. Fire alarm announcements will be provided by the Fire/Life-Safety System. An interface between the fire alarm system and PA system will mute the PA systems upon a fire alarm signal to the PA system.

4. Currently, the Audio Paging System (APS) and the Visual Paging System: in the Airport Terminals is an innovative Electronic Designs, Inc. paging solution and integrates with the following airport systems:

    a. Electronic Visual Display System (EVIDS):

        i. The EVIDS system utilizes triggers and other inputs, including zone information, from the PA system to distribute and display visual paging messages on EVIDS monitors. Visual paging messages are displayed on EVIDS monitors, ensuring ADA compliance.

    b. Airport Operational Database (AODB) and Resource Management System (RMS):

        i. The AODB is utilized for the purposes of developing flight schedules through the FIDS contained within the AODB. Information regarding flights, including gate announcements, gate changes, departure time, boarding status, etc., are generated by the AODB/FIDS, including updates based on events. The PA system shall integrate to the AODB and RMS for current information to be used in generating automated announcements based on flight schedules and changes.

    c. Master Clock:

        i. The PA system shall utilize the reference timing signals from the Master Clock system to trigger time-based announcements, and for announcing current time.

5. The paging system also utilizes an ambient noise analysis system to monitor background noise allowing the system to automatically raise and lower the volume of announcements.

6. The system utilizes digital microphones, as well as digital on-demand amplifiers and equalizers

7. Paging system has multiple servers, all with the ability to function as a fall back server, providing multiple levels of redundancy

8. The PA system provides the following types of announcements and services, across approximately 107 zones:

   a. Individual Terminal announcements, both automatically and manually generated;

   b. Terminal-wide announcements;

   c. Selective zone announcements, including baggage claim areas, passenger hold room areas, ticketing areas, etc.;

   d. Pre-recorded security and safety announcements which are triggered based on time and schedules;

   e. Emergency announcements, including audible instructions;

   f. Background music;

   g. Visual paging

9. Announcement and Paging Functions and Capabilities: The PA system has the following capabilities:

   a. Prioritization of messages, based on a rules set with manual override capability. This shall be priority based on message source and type, time-based events (e.g., flight boarding) with TSA Security Announcements and flight boarding being top priority:;

   b. Generation of pre-recorded and live messages from multiple sources, including the Airport Operations Center, gates, and other authorized locations and telephones within the airport;

   c. Generation of pre-recorded standard messages, with the insertion of airline name, flight number, gate number, status, and time to be inserted automatically;

   d. Message triggering based on time and date, specific events, and manual selection;

   e. Store-and-Forward capability: System shall allow for a user or operator to assemble, edit, coordinate and manipulate messages while a zone is busy

   f. Messages can be queued, recorded, stored and played back at regular intervals;

   g. Automated and manual capability to select distribution, repetition, and intervals of repetition for messages;

h. Coordination between audible and visual paging to ensure simultaneous announcement and display;

i. Generation of automatic announcements for gate changes and other flight-related announcements;

j. Generation of boarding process announcements, including boarding process instructions, pre-boarding announcements, and boarding sequence announcements;

k. Insertion of emergency and security announcements at a priority level over other pages and announcements.

10. Microphone Stations & Locations: Microphone Stations are designed to provide access to multiple zone configurations that are patterned after existing microphone devices. Handheld, handsets, or gooseneck mountings will be used.

    a. Majority of newer microphone stations are freestanding units sitting atop counters at ticketing and/or gates.

11. Microphone stations will include a microprocessor based IP handheld microphone with four zone selection buttons, incorporating green and red LED lights to indicate ready state or busy state as appropriate. A microprocessor based interface at each station will communicate with the master station to monitor each microphone state.

12. Functions are intended to allow voice paging and selection of up to four (4) zone combinations appropriate to each station's location. Additional microphone station functions will include:

    a. Initiating a playback sequence;

    b. Stopping a playback sequence;

    c. Recording a message;

    d. Monitoring a message.

13. Microphone stations are located at the following locations:

    a. Ticket counters;

    b. Gate counters;

    c. Gate counter ticket lift podiums;

    d. Baggage service offices.

14. Paging communications are distributed across the Airport LAN, utilizing 3-4 VLAN's, which distribute the number of devices evenly across the network to avoid collisions.

15. Speech-to-Text capabilities currently are not included, however the system is capable of this upgrade in the future.

9.5.7. MULTIMEDIA / CONFERENCE ROOMS

Conference rooms must have the following technology incorporated:

1. Conference voice telephone capability;
2. Large wall mounted LCD display or video projector with powered retractable screen (depending on size of room, larger rooms require projectors);
3. Screen sharing/presentation projection capability (laptop to large room screen), via wireless connection;
4. For conference rooms with fixed furniture (tables) integrated power and data connections are required;
5. Power and data connections in floor boxes distributed to provide adequate coverage for meeting presenters/ collaborators/audience members;
6. Designated rooms will have video teleconferencing capabilities with consideration to placement and use of integrated microphones, speakers, and cameras, depending on room size
7. Room scheduling screens connected to Microsoft Outlook mounted outside conference room doorway;
8. WiFi network capability

9.5.8. ACCESS CONTROL SYSTEM

General

1. The current access control system at the Airport is Identiv/Hirsch Electronics system. The current software version is Velocity Version 3.8.5
   a. The security access control system is a PC-based modular and network capable system utilizing one or more PC-based workstations, field installed controllers and card readers utilizing the Airport's converged TCP/IP local area network.
   b. Velocity server operates utilizing Windows Server 2019 Enterprise.
   c. Client workstations operate using Windows 10 Enterprise.
   d. Server operating system utilizes Microsoft SQL Server 2019.
2. Current system is integrated with the HID SAFE Identify Management Software.
3. Network components must have redundant and diverse network

connections from the access layer to the distribution layer.

4. For portals not requiring biometrics, as shown in Figure 2 on the following pages, provisions for future expansion to support biometrics identity verification shall be provided.

5. Refer to Door Type & Operational Role Charts as shown in Figure 9.2. on following pages for door requirements.

9.5.9. DOOR CONTROLLERS

1. Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels and similar data downloaded from the central station or workstation.

   a. Currently the Authority uses the MX -8-S3OB with expansion boards: RREB, AEB, REB8

   b. Controllers utilized battery backup to provide 90 minutes of run time during an outage;

   c. Controllers shall restore communications within 10 seconds after a network interruption;

   d. DC line supervision will provide alarms to the Security Operations Center (SOC) in the event of an interruption;

Figure 9.2.: Door Type and Operational Role

ID	Door Type & Operational Role	Biometrics	Other Considerations
A1	**Doors – Public to Secure Areas** To electronically secure, monitor, record and grant access control of locked doors leading from public areas to secure areas including open/closed conditions and to prevent unauthorized attempts to access through them.	Yes, from Public to Secure Only	
A2	**Doors - Public to Sterile Areas** To electronically secure, monitor, record and grant access control of locked doors leading from public areas to sterile areas including open/closed conditions and to prevent unauthorized attempts to access through them.	Yes, from Public to Sterile Only	
A3	**Baggage Belt Doors** To electronically secure, monitor, record and grant access control of these baggage belt doors including open/closed conditions and to prevent unauthorized attempts to access through these openings in attempt to reach the secured area.	NO	Only Persons having PACS smartcards should be able to open a baggage belt from a secured area.
A4	**Doors leading to tenant leasehold with subsequent access to secure areas** To electronically secure, monitor, record and grant access control of locked doors leading from public areas to tenant leaseholder with subsequent access to secure areas including open/closed conditions and to prevent unauthorized attempts	NO	
A5	**Elevator doors from public to sterile areas** To electronically secure, monitor, record and grant access control of elevator doors per floor leading from public areas to sterile areas including open/closed conditions and to prevent unauthorized attempts to access through them.	YES, from Public to Sterile only	

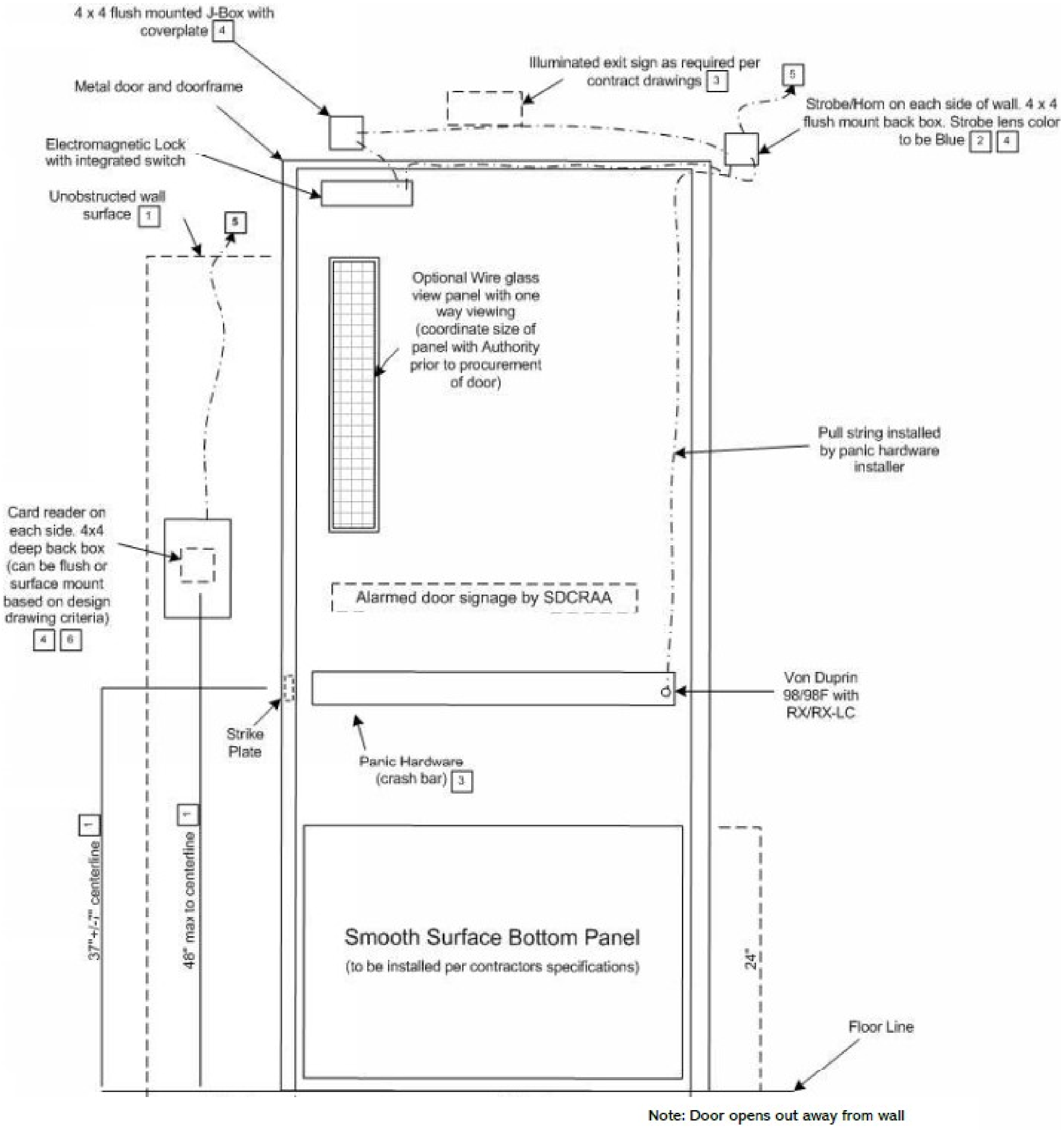
Figure 9.2.: Door Type and Operational Role (continued)

ID	Door Type & Operational Role	Biometrics	Other Considerations
A6	**Elevator doors from public to secured/AOA areas** To electronically secure, monitor, record and grant access control of elevator doors per floor leading from public areas to secured /AOA areas including open /closed conditions and to prevent unauthorized attempts to access through them. Additions of motion sensors to cab as needed.	Yes, from Public to Secured	
A7	**Vehicle or Pedestrian Gates** To electronically secure, monitor, record and grant access control of vehicle and pedestrian gates leading from public areas to secured/AOA areas including open/closed conditions and to prevent unauthorized attempts to access through them.	YES	Anyone entering a secured area, whether on foot or in a vehicle, must present his/her PACS smartcard and biometric to gain access.
A8	**Monitored roof hatch/door alarm point** To electronically monitor, and record doors leading from any area to the roof including open/closed conditions and to detect unauthorized attempts to access through them.	N/A	
A9	**Manually activated emergency alarm point. (SSCPs & Parking Lot Attendant Exit Posts)** To electronically monitor and record manually activated emergency button type alarm resulting in the dispatch of HPD to specific location. (Typically found at SSCPs and other locations as designated	N/A	
A10	**Cargo Bay Portals—Public to Secure / AOA Areas** To electronically secure, monitor, record and grant access control of cargo portals leading from public areas to tenant leaseholder with subsequent access to	YES	

Figure 9.2.: Door Type and Operational Role (continued)

ID	Door Type & Operational Role	Biometrics	Other Considerations
A11	**Doors from sterile to secure areas** To electronically secure, monitor, record and grant access control of locked doors leading from sterile areas to secure areas including open/closed conditions and to prevent unauthorized attempts to access through them.	Install capability; however, future regulations will dictate.	
A12	**Door from public to restricted areas** To electronically secure, monitor, record and grant access control of locked doors leading from public areas to restricted areas including open/closed conditions to prevent unauthorized attempts to access through them.	NO	Restricted areas are not a TSA designation. These are established by the Authority and are defined in the Airport Security Program (ASP).
A13	**Doors from restricted to public areas** To electronically secure, monitor, record and grant access control of locked doors leading from restricted areas to public areas including open/closed conditions and to prevent unauthorized attempts to access through them.	NO	
A14	**Doors with the Federal Inspection Services Facility (FIS)** To electronically secure, monitor, record and grant access control of locked doors to and from the FIS areas including open/closed conditions and to prevent unauthorized attempts to access through them.	NO	Current ACS within the CBP space is a discreet system from the Airport system, yet still maintained by the Authority.
A15	**Doors to Communication Facilities** To electronically secure, monitor, record and grant access control of locked doors to communications facilities including open/closed conditions and to prevent unauthorized attempts to access through them.	NO	

Figure 9.3.: Door Type and Operational Role


4 x 4 flush mounted J-Box with coverplate 4
Metal door and doorframe
Illuminated exit sign as required per contract drawings 3
5
Strobe/Horn on each side of wall. 4 x 4 flush mount back box. Strobe lens color to be Blue 2 4
Electromagnetic Lock with integrated switch
Unobstructed wall surface 1
5
Optional Wire glass view panel with one way viewing (coordinate size of panel with Authority prior to procurement of door)
Pull string installed by panic hardware installer
Card reader on each side. 4x4 deep back box (can be flush or surface mount based on design drawing criteria) 4 6
Alarmed door signage by SDCRAA
Von Duprin 98/98F with RX/RX-LC
Strike Plate
Panic Hardware (crash bar) 3
1
37"+/-1" centerline
1
48" max to centerline
Smooth Surface Bottom Panel
(to be installed per contractors specifications)
24"
Floor Line
Note: Door opens out away from wall

Notes:

1. Accessibility requirement
2. Verify location of J-Box in Field with panic hardware installer
3. CBC code requirement
4. Coordinate location and height above floor with security contractor, card reader (48"max) strobe/horn (80" max), each installed on both sides of door
5. Conduit run to 4x4 J-Box by general contractor. Coordinate size of conduit and location of J-Box with security installer
6. Card Reader – Hirsch SP47 ScrambleProx 8332ABT0000
7. Locking hardware to be Schlage, large format with interchangeable cores

   e. Provide alarm to the SOC ion disturbances in circuit signals;

2. Provide one and two-way communications with access control devices such as card readers, keypads, biometric identity verification stations, magnetic latches, gate and door operators, duress buttons, foot pedal alarms and exit push buttons.

3. Must operate as a standalone portal controller utilizing downloaded data in the event loss of communications occurs between the controller and the control station.

4. Must maintain time and date and location stamp for each transaction.

5. Receive inputs from entry control devices to change modes between access and secure.

6. Grant, deny, or differentiate access and mask intrusion alarms for authorized entries.

7. Provide door prop alarms when portal is held open longer than the schedule time allowed.

   a. Audio/visual devices do not alarm on door prop alarms

8. Power to be NFPA 70, Class II power supply transformer with 12 or 24 volt ac secondary battery backup and charger.

   a. Batteries are premium, valve-regulated, sealed lead acid complying with UL 294;

   b. Spill proof;

   c. Single state, constant voltage current battery charger;

   d. Battery to provide 90 minutes of run time;

   e. Dynamic battery load testing to be available for monitoring at the control center and have automatic disconnection of the controller when batter voltage drops below controller limits and report to central station.

9.5.10. AUDIO/VISUAL DEVICES

1. Current device is a Cooper Wheelock, Series AMT Multi-tone Strobe;

2. Lens color to be Blue;

3. Devices shall be mounted above the door or in the ceiling above the door;

4. Power supplies shall be Altronix AL600ULACM..

   a. This applies to A/V and Mag lock power supplies.

9.5.11. CARD READERS, CREDENTIAL READERS AND KEYPADS

1. Reader enclosures must be suitable for the planned mounting surface whether it is an indoor controlled environment, indoor uncontrolled environment or outdoor environments;
2. Readers should utilize backboxes manufactured by the manufacturer for the intended application:
    a. Flush Mount;
    b. Surface Mount;
    c. Semi-Flush Mount;
    d. Weatherproof;
    e. Pedestal Mount.
3. Caution should be taken when connecting the conduit with a threaded bushing to the backbox, as to not interfere with the depth of the reader and its circuit board when attached to the front of the box;
4. Readers currently used:
    a. Hirsch, ScrambleSmartProx, Indala, 8332ABT0000;
5. Readers shall be able to read credential cards from direct contact, to between 1.4 to 2 inches from the reader;
6. Readers shall have visual and audible indicators for access granted, access denied and user prompts;
7. Keypads shall provide means for users to access a portal by entering a unique code for multifactor authentication;
8. Keypads shall provide a means for users to indicate a duress situation by entering a unique code;
9. Readers are installed on both sides of all ACS portals, unless pre-approved and prior coordination has taken place with the AvSec department;
10. For rooms where ACS controllers are located inside (i.e. Rack Rooms), a key switch override shall be installed to bypass the reader and interrupt power to the magnetic lock, allowing access to the room.
    a. Biometric Identity Verification Stations shall be customized to the Authority's requirements. Units shall be able to integrate with current access control management system (s). Units shall be approved by the Authority.
11. Refer to Figure 9.3. for locations of equipment.
12. Readers must use the OSDP protocol for communications between the reader and door controller.

9.5.12. BIOMETRIC IDENTITY VERIFICATION STATIONS

The Authority has not adopted a biometric solution at this time, however all portals should be biometric ready by supplying the necessary cabling and infrastructure near the door reader location. Biometric Identity Verification Stations shall be customized to the Authority's requirements:

1. Units shall be able to integrate with current access control management system(s);
2. Units shall be approved by the Authority.

9.5.13. PUSH-BUTTON SWITCHES

1. Products used at the Airport are: Securitron Magnalock Corporation and Safety Technology International switches
    a. Powered from their associated controllers using DC control;
    b. Be able to be installed in indoor controlled and non-controlled environments, as well as outdoor environments;
    c. Mounting types can be surface or flush mount.

9.5.14. DOOR AND GATE HARDWARE INTERFACES

1. Von-Duprin panic hardware shall be used on all doors requiring access control:
    a. Hardware shall be equipped with two internal switches (the RX-2 model);
    b. Hardware has internal switches tied to the ACS to release the magnetic locks in the event of an emergency;
    c. Panic hardware may be wired to provide "Request to Exit" functionality without an audible alarm.
2. Electromagnetic locks shall be monitored for 'door secure' utilizing end -of-line resistors:
    a. Power and signal shall come from the controller
    b. Magnetic locks are Schlage
3. Vehicle gates accessing the AOA shall interface with the automatic gate controls and be connected to and monitored by the security ACS;
4. All door hardware, regardless of type, shall have the ability to be manually locked in the event the magnetic lock fails.

9.5.15. FLOOR-SELECT ELEVATOR CONTROL

1. Elevator access shall be integrated into the ACS;

2. ACS shall enable and disable car calls to each floor and to floor select buttons;

3. Credential access to specific floors is provided by the Authority ACO;

4. System controller shall record all elevator access data;

5. Floor select elevator control shall allow for manual override from a workstation PC, either by individual floor or by elevator cab;

6. Readers should be placed on the exterior near the call button, as well as a reader on the interior of the cab:

    a. Coordination with the elevator provider will be required to ensure adequate cabling is provided in the traveling cable to support the car reader.

9.5.16. VIDEO AND CAMERA CONTROL

1. ACS must be integrated Velocity Vision VMS and utilize Scale Computing as the host for video recorders..

2. Alarm events for door prop and door forced must appear on the workstation monitor within the SOC.

3. Alarm events, such as door open to long and door forced, require the corresponding applicable camera feed to appear on the VMS.

9.5.17. CABLES

1. All security cables and wiring shall be installed within metal raceways, unless pre-approved by the Authority.

2. Paired Reader Cables:

    a. 2 pair, 18 AWG, bare copper conductors, PP insulation, conductors twisted into pairs, multiple pairs cables together, overall shield and drain wire and rip cord;

    b. Cables installed within underground conduit must be outside plant rated.

3. ACS Equipment Cable:

    a. 2 pair, 22 AWG, bare copper conductors, PP insulation, conductors twisted into pairs, multiple pairs cables together, overall shield and drain wire and rip cord.

4. Copper CAT 6 UTP Cable:

    a. Refer to section regarding Communication Horizontal PDS cabling standards

5. Elevator Interface Cable:

    a. 10 conductor, 18 AWG bare copper conductors, PP insulation with a rip cord.

6. Input or Duress Cable:

   a. 4 conductor, 22 AWG, bare copper conductors, PP insulation.

7. Magnetic Lock or Output Cable:

   a. 4 conductor, 16 AWG, bare copper conductors, PP insulation, and overall shield and drain wire.

8. Auxiliary Output Cable:

   a. 4 conductor, 16 AWG, bare copper conductors, PP insulation with a rip cord.

9. Local Output cable:

   a. 2 conductor, 16 AWG, bare copper conductors, PP insulation with a rip cord.

10. Local Input Cable:

   a. 4 conductor, 22 AWG, bare copper conductors, PP insulation with a rip cord.

9.5.18. INSTALLATION AND PROGRAMMING

1. Coordinate with Aviation Security and Public Safety department via design coordination meetings to determine programming needs

   a. Verify and match existing conditions, with regards to programming and functionality of devices;

   b. Door settings and programming shall be performed based on door type and use;

   c. Alarm silencing;

   d. Zone and Holiday times;

   e. Prepare and install alarm graphics

2. Prepare plans for testing, commissioning and demonstration of system operations.

3. All security cables shall be installed within homerun metal conduit from device location, to Rack Room.

   a. Conduit from a Rack Room to a common area within a space, can be up sized to provide pathway for multiple devices and split out utilizing an appropriately sized junction box, then utilizing 1" conduit to the end device location

4. Cables installed within underground conduit must be outside plant rated.

   a. OSP installations need pre-approval by the Authority prior to being designed/implemented.

5. Boxes and enclosures containing security system components or cabling, that are easily accessed by the public shall be locked with an Authority approved method.

a. Junction boxes concealed above the ceiling in public spaces are not considered accessible.

6. Install end-of-line resistors at the field device location, not at the control panel location.

7. Ground cable shields, drain conductors and equipment to eliminate shock hazards and to minimize ground loops, noise, cross talk and potentially any other interference.

8. Label each terminal strip and screw terminal in each cabinet, rack or panel and provide door schedule inside each Controller.

9.5.19. AED (AUTOMATED EXTERNAL DEFIBRILLATOR)

1. AED devices deployed across terminals at the Airport are integrated with the ACS with annunciation in the SOC when AED cabinets are accessed;

2. AED's will be placed in locations outlined by the local building code;

3. AED cabinets shall be provided with:

   a. Philips HeartStart Defibrillator, the FRX model;

   b. Philips Fast Response Kit (part numbers can change). Please ensure the kit contains the following;

      i. 2 pair of hypoallergenic gloves

      ii. Pocket breathing mask

      iii. Paramedic scissors

      iv. Gallant chest hair razor

      v. Large extra absorbent paper towel

      vi. Items contained in a 5 1/2" x 9 1/2" zippered pouch which can be attached to the handle of the AED carrying case - Color red

   c. North American Rescue (NAR) – Four (4) Bleeding Control Kits per cabinet (part numbers can change). Please ensure the bleed control kits contain the following;

      i. NAR INTERMEDIATE (this include the chest seals)/Public Access Individual bleeding control kit—vacuum sealed;

      ii. One (1) C-A-T® Tourniquet

      iii. One (1) NAR Responder Emergency Trauma Dressing (ETD)

      iv. Two (2) NAR wound packing gauze

      v. One (1) HyFin® Compact, vent twin pack

vi. Two (2) pair, responder nitrile gloves, large

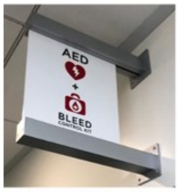
vii. One (1) responder trauma shears, 7.25 inches

viii. One (1) NAR survival blanket

ix. One (1) permanent marker, small

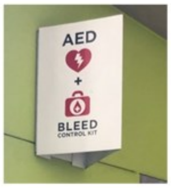
x. One (1) instruction card

d. AED + Bleed Control Kit signage,



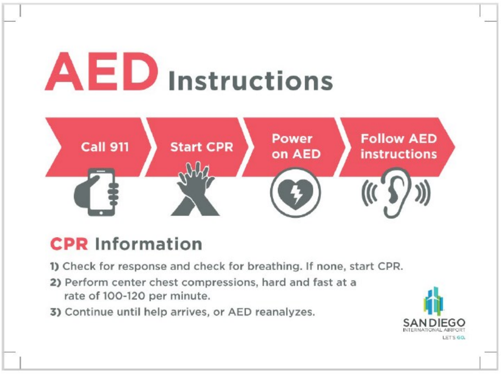
New Terminal 1
and
New Administrative Offices

OR



Terminal 1 Parking Plaza

e. AED Instructional Signage, Komatex PVC (waterproof material), size 8"x5" with rounded corners, font may be no smaller than 14



AED Instructions

Call 911 | Start CPR | Power on AED | Follow AED instructions

CPR Information

1) Check for response and check for breathing. If none, start CPR.
2) Perform center chest compressions, hard and fast at a rate of 100-120 per minute.
3) Continue until help arrives, or AED reanalyzes.

SAN DIEGO
INTERNATIONAL AIRPORT
LET'S GO.

f. AED Cabinet—HeartStation model: RC2000R, recessed mount (also, need a proper AED bracket and the keyway keyed to the current H2055 key for each cabinet) Cabinet needs to have a security tie-in with SOC - color white

9.5.20. INTRUSION DETECTION SYSTEM (IDS)

1. Current system in place at the Airport is the Integrated Security Corporation Infinity 2020;

2. Future systems are the Future Fiber Technology (FFT). System, unless authorized by AVSEC and IT&S.

2. Additional area control technologies should be compatible with the current IDS and will supplement it to form an integrated access control/ area control security system;

3. The IDS shall be designed to provide essential information on intrusions so that Airport Security can discriminate between true security threats and anomalous false alarms;

4. The IDS must be configured to tolerate vibrations caused by jet blasts near the RON parking areas along the perimeter and vibrations generated through sound waves to minimize false alarms;

5. Within the Airport's fenced perimeter, the system shall detect, assess, and

track multiple alerts, alarms, and intruders in multiple segments of the perimeter simultaneously, including any diversionary tactics;

6. The system is required to provide real-time target detection and target assessment, day and night and in conditions of poor visibility, including fog;
7. System must be capable of withstanding vast environmental changes without degradation of mechanical or electrical operations;
8. The system must be modular, microprocessor based, have intrusion sensors and detection devices with communications links to perform monitoring, alarm and control functions;
9. The positions and areas of coverage of all sensors and all detected and tracked targets is required to be displayed in the SOC real time against a geo-referenced background.
   a. Alarm signals must display on the master graphical control unit and actuate audible and visual alarms, within the SOC.
10. Alarms indicating abnormal conditions must have a distinct and discreet audible from standard alarms;
11. System must interface with the ACS to provide alarm events and alarm instructions;
12. System must interface with the Video Surveillance system for camera call ups upon alarm events;
13. Video analytics must be integrated into the system to provide ability to view and track movement along the perimeter;
14. Interior components must be housed in a minimum of a NEMA 250, Type 12 enclosure;
15. Exterior components must be housed in a minimum of a NEMA 250, Type 4X enclosure;
16. Thermal imaging cameras may be co-located with the DVS cameras on pan-tilt platforms for augmented night target assessment capability, where DVS cameras are blinded by strong point light sources, and for assessment during times of poor visibility.
    a. Thermal cameras shall be required. Designer/Contractor shall coordinate with the Authority on current equipment type;
    b. Parapet mounting hardware shall be Pelco PP100;
    c. Wall mount hardware shall be Pelco WM2000;

   d. CCTV power supplies shall be Altronix WPTV244300UL;

   e. SightSensor 340 meter range, 13 degree field of view GPS thermal analytic target sensor shall be SightLogix NS340-000;

   f. SightSensor 340 meter range, 24 degree field of view GPS thermal analytic target sensor shall be SightLogix NS180-000;

   g. SightSensor 340 meter range, 36 degree field of view GPS thermal analytic target sensor shall be SightLogix NS120-000;

   h. Pre-terminated cables for Sightlogix are Sightlogix SL-CAB-050. Footage may vary based on mounting requirements;

   i. Sight Monitoring software for GPS mapping is SightLogix SL-SM-CS;

   j. Sight Tracker GPS based PTZ controller is SL-ST1-DS-000.

17. Modifications to the perimeter fence shall align with current standards of fence construction and should integrate IDS capability at the earliest point in time.

   a. Change of Condition documentation shall be submitted to the Authority 90 days prior to any modification of the perimeter fencing.

9.5.2.1. INTRUSION DETECTION VEHICLE CONTROL SYSTEM

1. Manned guard posts are required to have a protected guard booth, where guards can perform their functions in safety. Requiring that a guard leave a booth to check credentials is to be minimized;

2. Guard booths are to be provisioned with bi-directional voice, data and video communications with the SOC along with DVS monitoring capabilities, as well as network access for validating credentials;

3. All gates should be equipped with access control card readers, cameras for coverage of the approaches to the gates and physical entry through gates; and lighting to permit the DVS cameras to perform properly on a 24x7 basis;

4. Design should allow for operation of manned and unmanned gates;

5. Unmanned gates may require enhanced access control through the use of biometrics;

6. Manned gated shall have the capability to operate as unmanned gates if needed.

9.6. VIDEO SURVEILLANCE

9.6.1. SYSTEM PARAMETERS

1. All device cabling shall be installed within homerun metal raceway. Conduit from a Rack Room to a common area within a space, can be up sized to provide pathway for multiple devices and split out utilizing an appropriately sized junction box, then utilizing 1" conduit to the end device location;

2. Current system in place at the Airport is a Velocity Vision system, using Scale Computing as the storage solution. Design should include the extension of the existing system, unless otherwise approved by the Authority;

3. Ensure all video transmission signals are present on NVR's, as well as viewable within the SOC;

4. Equipment located in public environments shall be protected by anti -tamper enclosures and monitoring devices and located on the Secured Area side of the gate;

5. Control station is a preconfigured PC with Velocity Vision software version 5 for use with digital recorders and video servers that allow full administrator functionality;

6. The use of a hardened media converter is acceptable with this application. The Authority currently uses Cisco switches and media converters;

    a. If multiple connections must be converted, a chassis mount product is preferred;

    b. If chasses mounts are not utilizes, media converters must be places on a rack mount shelf;

9.6.2. CAMERAS

1. Cameras are required to be mounted to allow clear fields of view without obstructions. Cameras shall be mounted at adequate height to provide the best field of view.

    a. Coordination with Stakeholders will be required, prior to final design, for final camera locations and field of views; See Figure 9.4. for suggested locations.

    b. Install cameras with 84 inches minimum clearance below cameras and their mounts;

    c. Approximate distances to be covered:

        i. 10 feet for checkpoints

        ii. 50 feet for perimeter gates

        iii. 50 feet or less for gate hold rooms

        iv. 75 feet or less for corridor views down a concourse

Figure 9.4.: Camera Locations and Operational Roles

ID	Operational Role	Priority	FPS/Storage
C1	**Perimeter Security (Vulnerable Areas)** For surveillance of the perimeter and adjacent areas of vulnerability Varying conditions at the perimeter demand different cameras with a mix of radar, daylight, and thermal cameras. Evaluate cameras v/s radar for applicability at specific spots on perimeter.	HIGH	10 fps / 90 days
C2	**AOA – Vulnerable Points (Secured Area)** To observe, detect and record vulnerable points within the AOA that compromise the secure area perimeter AOA Secured Perimeter = Perimeter Boundary There are vulnerable conditions at the Southwest and Northeast East areas	HIGH	10 fps / 90 days
C3	**Security Screening Checkpoint (SSCP)** To observe and record all patrons proceeding through SSCP to the sterile area, prevent thefts, prevent bypassing of SSCP (including breach through exit lanes), and provide identifying images of persons causing terminal security breaches. Evaluate use of Video Analytics for Exit Lane Coverage. Current security project effort does not provision for cameras for the exit lanes check point. Consider retrofitting for existing exit lanes for standardization. Evaluate design schemes for better facility design support for electronics. Dependent on TSA design guideline.	HIGH	30 fps / 90 days

Figure 9.4.: Camera Locations and Operational Roles (continued)

ID	Operational Role	Priority	FPS/Storage
C4	**In-line Baggage** To deter, observe and record employee theft activity, monitor continuous proper operation of conveyor system and observe any breach activity through baggage system portals to baggage check -in and baggage claim Scope included in Project one for existing facilities.	HIGH	15 fps for nondiverted belt sections / 90 days 30 fps for diverter belt sections / 90 days
C5	**Baggage belt doors** (Curbside, Ticketing, and Baggage Claim) To observe and record any attempt to access secure area from public areas by general public or intruder (1542) (2 Cameras; one on the outside and one on the inside of the door)	HIGH	10 fps / 90 days
C6	**Doors from public to sterile areas** To observe and record unauthorized access to sterile area from public areas by unauthorized persons and provide identifiable images of the unauthorized user (1542) High Priority by Default Need mega pixel cameras on all doors Apply video analytics on the sterile side for piggy backing, tail gating and loitering. (2 Cameras on the door)	HIGH	15 fps / 90 days

Figure 9.4.:Camera Locations and Operational Roles (continued)

ID	Operational Role	Priority	FPS/Storage
C7	**Doors from public to secure areas** To observe and record unauthorized access to secure area from public areas by unauthorized persons and provide identifiable images of the unauthorized user (1542) High Priority by Default Need mega pixel cameras on all doors Apply video analytics on the secure side for piggy backing, tail gating and loitering. (1 Camera on the secure side of door)	HIGH	15 fps / 90 days
C8	**Elevators doors from public to secure areas** To observe and record any attempt to access secure areas from public areas by unauthorized users in and around elevators (1542) Currently condition - only one elevator now that is public to secure Apply video analytics for tailgating, piggy backing and loitering (1 Camera on the secure side of door)	HIGH	15 fps / 90 days
C9	**Elevators doors from public to sterile areas** To observe and record unauthorized access to sterile areas from public areas by unauthorized users Apply video analytics for tailgating, piggy backing and loitering (1 Camera on the sterile side of door)	HIGH	15 fps / 90 days

Figure 9.4.: Camera Locations and Operational Roles (continued)

ID	Operational Role	Priority	FPS/Storage
C10	**Vehicle or pedestrian gates** To observe and record access through gate checkpoints, provide security for gate guards, and display nearby threats. High priority by default	HIGH	10 fps / 90 days
C11	**Emergency Doors from public area to secure area (1542 type doors)** To observe and record any attempt to access secure area by unauthorized users of these unlocked (?) doors (2 cameras; one on the outside and one on the inside of the door)	HIGH	30 fps / 90 days
C12	**Terminal Bldg. Main Entry/Exits** To observe and record all patrons and their belongings entering and exiting terminal main entrances Camera is inside focused on the entry door	MEDIUM	15 fps / 90 days
C13	**Doors from CBP/ FIS to public area** To observe and record attempts to re-enter exits from CBP area (1 camera on the public side of door)	HIGH	30 fps / 90 days
C14	**CBP/FIS Primary Booths** To observe and record each arriving international passenger as they are processed into the United States Apply CBP Standards for FIS areas	MEDIUM	30 fps / 90 days

Figure 9.4.:Camera Locations and Operational Roles (continued)

ID	Operational Role	Priority	FPS/Storage
C15	**CBP/FIS Baggage inspection Station** To observe and record an international passenger's individual baggage inspection process as described by published CBP FIS ATDS design guideline.	MEDIUM	30 fps / 90 days
C16	**Doors from Restricted area to secure area** To observe and record any attempt to access secure area from Restricted areas by unauthorized users or general public Restricted Area is defined as any areas on airport properties that general public are not allowed (1 camera on the secure side of door)	HIGH	15 fps / 90 days
C17	**AOA – Ramp Side (Domestic) (Secured Area)** To observe and record local ramp side activities including baggage transportation, fire emergency, evacuation, jetways and planes Useful for general surveillance	MEDIUM	15 fps / 90 days
C18	**AOA - General Areas (Secured Area)** To provide general surveillance overview, assist in dispatch of authorities, allow AOA safety enforcement, and the tracking of suspect persons or vehicles entering the AOA from controlled ports. General Surveillance with a need for one camera per gate	MEDIUM	15 fps / 90 days

Figure 9.4.: Camera Locations and Operational Roles (continued)

ID	Operational Role	Priority	FPS/Storage
C19	**Public - Ticketing** To observe and record public ticketing lines and activities, monitor crowd levels and observe suspicious bags or persons Should include Video Analytics that tracks separation from article, bag left behind, etc.	HIGH	30 fps / 90 days
C20	**Public – Curb Side** To observe and record public curbside people, unattended bags, manage traffic flow, observe illegally parked vehicles, and observe terminal evacuations.	MEDIUM TO HIGH	Passive Recording—15 fps / 90 days Active Recording—30 fps / 90 days
C21	**Public - Baggage Claim** To observe and record baggage pickup, unattended baggage and theft activity	MEDIUM TO HIGH	15 fps / 90 days
C22	**Doors from sterile to secure areas** To observe and record any attempt to access secure area from sterile areas by unauthorized persons (1 Camera on the restricted side of door)	HIGH	30 fps / 90 days
C23	**Doors from Public to Restricted areas** To observe and record any attempt to access Restricted area from public areas by unauthorized person	MEDIUM	15 fps / 90 days

Figure 9.4.:Camera Locations and Operational Roles (continued)

ID	Operational Role	Priority	FPS/Storage
C24	**Restricted area** To observe and record activity within a Restricted area. Dependent on situation, case specific	MEDIUM	15 fps / 90 days
C25	**Public area** To deter criminal or disruptive behavior, observe and record general activities, unattended baggage, suspicious articles or persons, crowd control and evacuation management Vulnerable areas other than curbside and parking lots	MEDIUM TO HIGH	15 to 30 fps / 90 days
C26	**Sterile area** To deter criminal or disruptive behavior, observe and record general activities, unattended baggage, suspicious articles or persons crowd control, evacuation management, and breach investigations	HIGH	Passive Recording—15 fps / 90 days Active Recording—30 fps / 90 days
C27	**Elevators doors from public to public areas** To observe and record general activity and public movement around elevators (2 Cameras; one on each public floor to view	LOW	15 fps / 90 days
C28	**Elevator doors from sterile to secure areas** To observe and record any attempt to access sterile areas from public areas by unauthorized users in and around elevators	HIGH	30 fps / 90 days

Figure 9.4.: Camera Locations and Operational Roles (continued)

ID	Operational Role	Priority	FPS/Storage
C29	**Doors to Passenger loading bridges (Jetway doors involving International flights** To observe and record unauthorized attempts to access loading bridges/jetways from sterile area passenger gates	HIGH	30 fps / 90 days
C30	**Public doors leading to tenant leasehold (restricted area) with subsequent access to secure area** To observe and record an unauthorized entry to tenant areas (Not typically PACS doors) (1 Camera on the restricted side of door)	HIGH	Passive—15 fps / 90 days Active—30 fps / 90 days
C31	**Public Parking Lots** A discreet system from the Airport Vicon CCTV system. To observe and record criminal activity and traffic accidents, manage evacuations, and emergency phone activity	-	30 fps / 90 days
C32	**Emergency Doors from sterile/restricted/FIS to secure area** To observe and record any attempt to access secure area by unauthorized users of these unlocked doors (1 Camera on the secure side of door)	HIGH	30 fps / 90 days
C33	**Public Escalators** To observe and record accidental slip and falls, personal attacks, unattended packages, and crowd management Handled by The Authority	Case specific	15 fps / 90 days
C34	**CBP/FIS Area** To observe and record general public activities in the CBP	MEDIUM	30 fps / 90 days

9.7 TELECOMMUNICATION SERVICES

9.7.1 Shared Tenant Services

Per the Lease, the Authority can provide telecommunications, data network and shared airport tenant services through our STS (Shared Tenant Services) offering. STS provides a portfolio of technology solutions that deliver competitive products and services to Concessionaires at the San Diego International Airport. Concessionaires can elect to purchase Internet, telephone, and television services from STS or purchase services directly through the providers.

STS provides Concessionaires with low-cost services and high-quality customer service. The cost of equipment, line, carrier services and maintenance are distributed across the STS Concessionaires that subscribe to the service. Concessionaires find this program appealing for a variety of reasons including, the convenience of one stop shopping for all communication needs and reduced operating costs.

STS offers numerous technology systems to benefit Concessionaires including:

1. Gigabit Ethernet data network
2. An extensive infrastructure network of fiber optic cable and copper wire
3. Voice over IP telephone services for local and long-distance dialing
4. Multiple television channel packages
5. A superior WIFI network
6. Cable wiring and installation
7. A customer-oriented services provisioning group and billing system

Shared tenant Services Offerings & Rates

Services	Rates
Network	
Network Access 1Gb (Point to Point and/or Internet)	$175/mo.
Network Access 1Gb Switch Port	$15/port.
Public Static IP Address	$25/mo.
Dedicated Wi-Fi SSID—localized to tenant space	$70/mo.
Terminal Wide Wi-Fi SSID–broadcasted throughout terminal	$500/per terminal/mo.
Intra-terminal Dark Fiber Lease (Subject to availability)	$175/pair/mo.
Inter-terminal Dark Fiber Lease (Subject to availability)	$300/pair/mo.
Phone	
IP Telephone Service (Includes license, local and long-distance calling, voicemail, and optional analog dialing)	$58/mo.

TV	
CATV Service (Includes 1 TV set, receiver support and coax cable support)	$90/mo.
CATV Service—Hospitality (Includes 3 TV sets, receiver support and coax cable support)	$165/mo.
Support Services	
Technical Support (Minimum charge 2 hours)	$125/hr.

Concessionaire will be responsible for the initial cost of installation and all associated equipment and cabling. The prices listed above are the monthly recurring charges for the services provided and support only. There is no obligation to purchase any STS service. Concessionaires may elect to purchase services from other providers. The STS services are subject to the terms of use in the STS Agreement.

How To Order Shared Tenant Services:

To order STS, please contact ComSAT AV, our contracted STS provider, at 619-795-9444 ext. 1103 or send an email to rybanez@comsatav.com. ComSAT AV will review with you the services offered, answer any questions you may have, and conduct a job walk to understand the scope of services requested. They will provide the STS Agreement for you to review and sign. Once executed, it typically takes two weeks for services to be established.

Ongoing Support for Shared Tenant Service

If you are experiencing issues with the provided STS, please contact 619-795-9444 ext. 1103 or send an email to rybanez@comsatav.com. Support is available 24/7/365.

9.7.2 Alternative Telecommunication Providers

Concessionaires can elect to purchase Internet, telephone, and television services directly through providers without subscribing to STS. AT&T is the current LEC (Local Exchange Carrier) for network services at the airport. Concessionaires may order services from their preferred vendors, but AT&T is the last mile carrier.

Guidelines for Services

1. Concessionaire shall not install their own high-speed wireless local area network without the written consent of Authority in advance and all construction work is subject to a Concessionaire Improvement request process, as determined and approved in the sole discretion of the Authority.
2. Each Concessionaire will have access to telephone, IPTV, and internet services from a local telecommunication closet. A 2”

terminal. Conduits going back to RR shall land in the space allocated for Concessionaire with the RR. This is not a reserved space to house network gear pr servers and its intended to only obtain connectivity from STS or LEC services.

3. If Concessionaire elects to contract for telecommunications services directly with LEC providers, the LEC will deliver services to the nearest MPOE (Minimum Point of Entry). At the Concessionaire's sole expense, the Authority's cable installer, currently ComsatAV, will work with the LEC to extend services to the nearest RR. ComsatAV will install cable from the nearest RR to Concessionaire via 2" conduit for a fee or Concessionaire can elect to use their own cable provider to run cable from the Concessionaire space through the 2' conduit to the RR. Concessionaires contractor is not permitted to go beyond the RR.

4. If Concessionaire desires to install Wireless Access Points (WAP) to build a "Wi-Fi Network" within the Concessionaire space, for the use by Concessionaire and its employees, Concessionaire shall seek Authority approval and coordinate with the Authority IT Department to ensure there isn't signal clashing, and that assignments are accounted for accurately.

5. Music, video, and television entertainment systems are permitted; however, the volume of sound must be strictly controlled to limit the levels to Premises and not intrude into adjacent spaces or public areas. The Terminal Paging System and Emergency Messaging System must be clearly heard without interference from Concessionaire sound systems. The noise from any Premises to the exterior shall not exceed 6 dBA above the ambient level. The ambient level is anticipated to be 50 dBA, therefore, the maximum level for the Premises is not to exceed 56 dBA. Concessionaire is responsible for obtaining permission to transmit any copyrighted music, including but not limited to, radio broadcasts, recorded music, and television broadcasts, in the Premises at the Airport in compliance with all laws.

6. Concessionaires will not be allowed to install their own roof top satellite dish. The Authority has implemented IP based TV and services through Shared Tenant Services.