

**STATEMENT OF WORK
FOR
PRIVATE WIRELESS NETWORK IMPLEMENTATION
AT
RONALD REAGAN WASHINGTON NATIONAL AIRPORT
AND
WASHINGTON DULLES INTERNATIONAL AIRPORT**



June 2026

Table of Contents

Section 1	Background and Summary of Work.....	1
1.1	Introduction	1
1.2	Current State	1
1.3	Desired End State.....	1
1.4	Scope	3
1.5	Roles and Responsibilities.....	3
1.6	Reference Documents	4
Section 2	Wireless Requirements	5
Section 3	Tasks and Deliverables	7
3.1	Contract Management.....	7
3.2	Design and Construction.....	7
3.3	System Testing and Commissioning.....	9
3.4	Operation Readiness and Transition (ORAT)	10
3.5	Training	11
3.6	Management and Support	11
3.7	Deliverables Table.....	13
Section 4	General Requirements.....	13

Section 1 Background and Summary of Work

1.1 Introduction

Metropolitan Washington Airports Authority (the Authority) oversees the management, operations, and capital development of Ronald Reagan Washington National Airport (DCA) and Washington Dulles International Airport (IAD). Washington Dulles International Airport is located in the heart of the East Coast, just outside downtown Washington, D.C., and serves a growing metropolitan area. IAD sits on 12,992 acres in Loudoun and Fairfax counties in Virginia and includes a Main Terminal, five concourses with 113 airline gates, and four active runways. Ronald Reagan Washington National Airport is located in Arlington, Virginia and sits on 861 acres. DCA features two terminals, with a combined 58 gates, three active runways, associated hangars, maintenance areas, and aircraft support facilities. These two airports, along with their associated airfields and support facilities, utilize cellular service for device connectivity.

1.2 Current State

The existing Neutral Host Distributed Antenna System (NH-DAS) provides cellular connectivity throughout interior spaces at both airports. Coverage includes terminal buildings, concourses, administrative offices, and parking structures. The NH-DAS is currently being expanded to additional facilities throughout both campuses, providing increased connectivity for tenants and the Authority.

Outdoor operational areas across both airport campuses currently lack comprehensive wireless coverage. This includes runways, taxiways, remote campus locations, and airfield facilities. The connectivity gap creates operational challenges for maintenance crews and the real-time monitoring of critical infrastructure across the airfield and extended campus.

The Authority has developed a Private Wireless Network design to provide secure, high-performance connectivity throughout these outdoor areas in support of current airport operations and desired future capabilities.

1.3 Desired End State

The Authority seeks to achieve the following primary objectives through the implementation of a Private Wireless Network:

1. **Enhanced Connectivity and Bandwidth:** Provide high speed, low latency connectivity across the runways and the secured areas of the airport, to support growing demand for data traffic from devices and staff. This project will specifically cover gaps in connectivity throughout the Airfields and remote building areas for Authority devices. At this time, the Authority anticipates needing to connect up to 500 devices to the Private Wireless Network at DCA and up to 1,000 devices at IAD. As needed, the Private Wireless Network must be capable of scaling up the number of connected devices beyond this anticipated amount through the SIM provisioning process.
2. **Network Security and Privacy:** To establish a secure private wireless network infrastructure in the sensitive areas of the airport operations that are isolated from public networks.
3. **Futureproofing for Advanced Technology:** Ensuring that the network is future proofed to integrate with emerging technologies and enhanced operational capabilities.

1.3.1 Network Design

The Authority's Private Wireless Network will utilize a Celona-based Private 5th Generation (p5G) platform operating in the Citizens Broadband Radio Service (CBRS) spectrum. The network

architecture was designed to provide secure, high-performance connectivity throughout the targeted operational areas at both IAD and DCA airports.

Enterprise Edge controller pairs will be deployed in each of the IAD and DCA head-ends. Patch cables are to be provided by the Contractor. Backbone fiber already exists at all AP site locations (see SOW Appendix D). Fiber connectivity will be established from each controller to existing Nexus core switches, with direct fiber links between controller pairs enabling monitoring and state synchronization. From the head-ends, the Enterprise Edge controllers will extend connectivity to Core/Distribution switches located in airport Telecommunication Rooms, which will then connect, through Access Switches to Access Points distributed throughout the campus. These Access Points will distribute signals to antennas delivering RF coverage to end-user devices across the airfield and operational areas.

The Private Wireless Network will integrate with the Authority's instance of Cisco Identity Services Engine (ISE) secure access system, providing Network Admission Control (NAC) to wireless endpoints accessing the network.

The Celona platform will connect to the Authority's existing infrastructure with upstream traffic routing through the Authority's data centers. The system will integrate with the Authority's Entra ID for authentication and access control.

1.3.2 Project Expansion

The Private Wireless Network implementation will be executed in parallel, with a single buildout phase at DCA and in two phases at IAD: a base buildout pilot phase followed by a full buildout expansion.

The base, or active pilot phase will establish the core network infrastructure and deploy a limited number of Access Points (APs) to cover key operational areas. This phase will enable immediate connectivity benefits while allowing the network to undergo rigorous testing and validation in the airport environment. Testing will assess coverage, latency, reliability, and overall performance to ensure the system meets operational requirements before expansion. As the outdoor area at DCA is well-bounded, the base and buildout phases will be consolidated into a single phase. IAD will follow the two-phase approach. The Authority anticipates the buildout phase at DCA and pilot phase at IAD to be completed no more than six (6) months after project kick-off. However, it is expected that the Contractor is able to meet or accelerate this schedule without compromising safety, compliance, or quality.

Following successful completion of the active pilot phase, the full buildout phase will expand network coverage by deploying additional APs throughout both airport campuses. This phase will provide comprehensive coverage across all designated outdoor operational areas, ensuring scalability and network performance to support current and future operational needs. The Authority anticipates the following coverage at each airport after full buildout:

- Primary Coverage (i.e., coverage when all APs are up and running)
 - DCA Buildout: 95.35%
 - IAD Base Buildout: 66.71%
 - IAD Full Buildout: 73.93%
- Secondary Coverage (i.e., coverage when any one AP fails)
 - DCA Buildout: 91.59%
 - IAD Base Buildout: 35.24%
 - IAD Full Buildout: 67.10%

1.4 Scope

As a part of the scope of work, the Contractor shall provide the following:

1. Project Management
2. Procurement of all Private Wireless Components
3. Final Construction Document Submittals
4. Construction and Implementation of Private Wireless Network
5. System Testing and Commissioning
6. Technical Support and Management
7. Warranty and Maintenance Coverage
8. Managed Service and Ticket Escalation

1.5 Roles and Responsibilities

The following table delineates the roles and responsibilities between the Authority and Contractor:

Responsibilities	Contractor	MWAA IT/Engineering & Design Team
Network Design and Architecture	Full 100% Construction Documents. Construction documents shall follow the Airport's Authority design manual: https://www.mwaa.com/business/airports-authority-design-manual	Define requirements, ensure alignment with business needs.
Network Deployment	Procure, ship, install and configure hardware for private wireless network. This includes all required patch cords, mounts, power supplies and other edge devices as required. This includes local COAX wiring to antennas.	Provide access (as required), support integration with existing IT systems. Configure required updates on MWAA enterprise network.
Testing and Optimization	Perform testing, share the test report with MWAA team for approval. If the result does not meet the requirement, the Contractor must remedy the gap.	Monitor and manage.
Training and documentation	Provide training on network infrastructure and tools for monitoring performance	Attend training and disseminate knowledge internally as required.
Support and Maintenance	Issue SIM for MWAA device usage. Provide technical onsite and project managerial support during the buildout phases for both Pilot and full deployment. After transition to operations, provide managed service encompassing network maintenance, network management, ticket escalation, and updates.	Provide list of SIMs required for both IAD and DCA locations. Oversee day-to-day network operations and troubleshoot issues.

1.6 Reference Documents

- 1.6.1 Appendix A: Private Wireless Network Design Package
- 1.6.2 Appendix B: Private Wireless Regulatory Compliance Report
- 1.6.3 Appendix C: RF Signal and Heat Maps
- 1.6.4 Appendix D: AP Site Location Detail Maps
- 1.6.5 Appendix E: AP Inventory Table

Section 2 Wireless Requirements

- 2.1** All specific references in the specifications to codes, rules, regulations, standards, manufacturer's instructions, or requirements of regulatory agencies shall mean the latest edition in print. All installations shall be compliant with the latest versions of all applicable standards. The Private Wireless Network shall comply with cybersecurity and security standards including but not limited to:
- NIST Cybersecurity Framework
 - MWAA Cybersecurity Standards
 - NSA CNSA 2.0
 - General Data Protection Regulation (GDPR) Requirements
 - FCC Regulations for CBRS Operations
- 2.2** The Private Wireless Network shall operate in the Citizens Broadband Radio Service (CBRS) spectrum from 3550-3700 MHz utilizing the n48 band.
- 2.3** All Citizens Broadband Radio Service Devices (CBSDs) shall be properly registered with an FCC-authorized Spectrum Access System (SAS) prior to activation and operation. The Celona platform shall manage automatic registration of each unit to the SAS during initial deployment by submitting FCC ID, serial number, device category, antenna gain, height above ground, indoor/outdoor classification, and other required parameters.
- 2.4** Category B CBSDs shall be deployed for outdoor installations with maximum Equivalent Isotropically Radiated Power (EIRP) of 47 dBm (50 watts) per 10 MHz. All equipment shall carry FCC equipment authorization and include required security capabilities for encrypted Spectrum Access System communication.
- 2.5** Category A CBSDs are not anticipated at this time but may be added to the existing network and Enterprise Edge infrastructure in the future. These additions would cover large open interior areas such as hangars, workshops, and warehouses.
- 2.6** The Private Wireless Network shall not create harmful interference with existing airport wireless systems, operational radio systems, or wide area wireless service provider networks. The Contractor shall validate proper operation without interference during installation and maintain interference-free operation throughout the term of the contract.
- 2.7** The system shall utilize a fault tolerant design, avoiding single points of failure in the network architecture.
- 2.8** The Private Wireless Network shall have adequate capacity to support estimated device usage.
- 2.9** Private Wireless traffic shall be routed over the existing MWAA LAN infrastructure. The Celona platform shall connect to Authority's existing MPLS/VPNv4 infrastructure. Traffic shall route through the Authority's data centers with network segmentation separating operational traffic from management functions.

- 2.10** The Private Wireless Network shall encrypt radio signals at the physical layer between access points and end devices using 128-bit AES ciphering over the air interface. WPA3-Enterprise encryption shall be utilized to protect data in transit with device authentication.
- 2.11** The system shall integrate with the Authority's Entra ID for single sign-on. Role-based access controls shall limit administrative privileges.
- 2.12** The system shall integrate with the Authority's Cisco ISE implementation for Network Access Control.
- 2.13** Traffic shall remain encrypted from the access point through the Enterprise Edge controller to the enterprise network. The platform shall terminate SIM-based authentication at the Edge and integrate with existing enterprise security controls.
- 2.14** The network shall not operate by receiving radio signals from any off-airport cellular towers and rebroadcasting through the infrastructure.

Section 3 Tasks and Deliverables

3.1 Contract Management

The Contractor shall be responsible for the following:

- 3.1.1 Providing an on-site Project Manager (PM) as the primary point of contact for the project buildout phases.
- 3.1.2 The Contractor shall at all times retain a qualified, competent, experienced manager who shall manage and supervise the operation of the system, with authorization to make representations and take ordinary actions. The manager shall generally be available to be contacted by the Authority during regular business hours (between 8:00 AM to 5:00 PM EST). A qualified, competent, and experienced subordinate shall be in charge and available during the manager's absence.
- 3.1.3 The Contractor shall conduct a Project Kickoff within two (2) weeks after Contract Award at which it will review its proposed project plan, project schedule, communications plan, and problem escalation procedures, and introduce Contractor staff.
- 3.1.4 Throughout project execution, the Contractor will be responsible for conducting bi-weekly status review meetings reporting on scope, schedule, resources, and quality and risk mitigation.
- 3.1.5 The Contractor shall provide written weekly status reports.
- 3.1.6 At the discretion of the Authority, a weekly teleconference will be conducted to review the emailed project status reports.

3.2 Design and Construction

- 3.2.1 The Contractor shall provide construction level system design and installation drawings for review by the Authority prior to any system installations. These shall be provided at a 50% and 100% CD level.
- 3.2.2 The Contractor shall be responsible for all drawings, documents, certifications, Professional Engineer (PE) stamps and permits required for Private Wireless Network construction and operation. Along with project drawings, the Contractor shall submit product data information via manufacturer cutsheets or similar literature for any components. All equipment, cables, antennas, and accessories to be installed shall be pre-approved by the Authority prior to installation. System installation shall conform to the pre-approved design and shall meet the requirements in this SOW, unless otherwise approved in writing by the Authority.
- 3.2.3 The Contractor shall be required to create and submit shop drawings and component drawings detailing the exact mounting requirements for each component and device to be supplied by this project as well as detailed information for any casework that is to be installed to support the Private Wireless Network devices.

- 3.2.4 The Contractor shall disclose all materials to be used for system components as part of the system designs and construction plan. The materials should be of first-class quality, safe, fire-resistant, and consistent with the aesthetic and architecture of the airport.
- 3.2.5 To support the distribution of Private Wireless signals, Authority communications infrastructure (i.e., fiber backhaul and network connectivity) will be available to the Contractor. The Contractor shall identify all connectivity requirements to support the proposed design and coordinate with the Authority to ensure fiber allocation.
- 3.2.6 Any additional supporting infrastructure required beyond existing Authority facilities, equipment, fiber and infrastructure, such as wall mounts and outdoor enclosures, shall be provided and installed by the Contractor. Construction shall be executed in phases as outlined in the design documents. All construction activities shall be coordinated with the Authority to avoid operational disruption and ensure integration with airport systems and facilities.
- 3.2.7 The Contractor shall be responsible for all required FAA and FCC submittal creation. As required, documentation shall be provided to the Authority for approval of the use of frequency bands and licenses on Airport property. The Authority will be responsible for the actual submittal of any FAA and/or FCC documentation, as applicable.
- 3.2.8 The Contractor shall be responsible for providing all hardware required for final installation. The Contractor shall construct and install all components of the Private Wireless Network in accordance with the approved design documents, including the Private Wireless Design Package, RF Signaling and Signal Coverage Maps, and associated technical specifications. Design and construction activities shall implement the chosen design approach, including all necessary hardware, mounting equipment, environmental enclosures, and connections required for a fully operational system.
- 3.2.9 The Contractor shall develop a detailed Construction Plan in accordance with Authority standards. The Construction Plan shall specify all installations and shall include any information required by the Authority. The Contractor shall develop a construction schedule covering all construction activities related to the Private Wireless Network. The construction schedule must be aligned and coordinated with Airport Capital Program schedules where required.
- 3.2.10 During construction, the Contractor shall participate in regular construction meetings to ensure coordination with the Authority and any associated projects. The Contractor shall coordinate directly with Airport Capital Program contractors as required.
- 3.2.11 The Contractor shall prepare Method of Procedure ("MoP") documentation for all work that may affect ongoing normal airport operations. The Contractor shall submit and receive Authority approval before any such work is started.
- 3.2.12 Lightning protection arrestors shall be installed per applicable electrical codes and manufacturer specifications for all outdoor antenna installations.

- 3.2.13 All outdoor devices must be professionally installed by CBRS Certified Professional Installers (CPI) who will maintain installation parameter records for FCC inspection. As per CBRS network requirements, the Contractor shall hold ultimate responsibility for CBRS FCC regulatory compliance.
- 3.2.14 Private Wireless Network equipment must be installed in Authority communications rooms or remote network cabinets. The Contractor shall be responsible for performing the appropriate coordination with the Authority to ensure all Private Wireless Network equipment can be accommodated within the Authority's racks, cabinets, and pathways. The Contractor shall be responsible for supply and installation of all equipment cabinets, wall mounts, and pole mounts that may be required in addition to what is provided in the Authority's Telephone Rooms (TRs) and enclosures.
- 3.2.15 Equipment shall be rated for continuous operation under the ambient environmental temperature, humidity, and vibration conditions encountered at the installed location. For devices located in harsh environments such as interior uncontrolled or exterior environments, the Contractor shall provide the necessary industrialization or hardened enclosures to ensure proper equipment operation and performance. Notable for this equipment is the provision of an acceptable IP66 or IP67-rated enclosure for the power supply of the ruggedized outdoor Access Points.

3.3 System Testing and Commissioning

- 3.3.1 The Contractor shall conduct comprehensive testing of all Private Wireless Network components and systems to verify compliance with design specifications and performance requirements. Testing shall validate system functionality, coverage, performance, and integration with existing Authority infrastructure prior to final acceptance and transition to operations. The Contractor shall provide comprehensive test documentation and upon successful completion of all testing activities and Authority review and acceptance, the system shall be transitioned to the Authority .
- 3.3.2 Testing shall include individual component testing of each discrete component upon installation completion. End-to-end system testing shall verify complete signal path integrity from headend controllers through the distribution network. Coverage validation testing shall confirm that RF signal strength and quality meet the requirements specified in the approved RF Signaling Coverage Maps throughout all designated coverage areas at both IAD and DCA airports. Performance testing shall verify that the network meets all specified criteria including throughput, capacity, and quality of service parameters under various pre-agreed testing load conditions. Integration testing shall confirm proper interoperability between the Private Wireless Network and existing Authority network infrastructure, including Cisco ISE Network Access Control.
- 3.3.3 For each test conducted, the Contractor shall prepare a test report certifying successful completion. Test reports shall be delivered to the Authority in electronic format for review and acceptance.

3.3.4 At a minimum, each test report shall contain:

- Summary of test results.
- A list and discussion of all discrepancies between expected and actual results.
- All failures encountered during the test and their resolution.
- Complete copy of test data sheets.
- Signatures of those who performed and witnessed the test.

3.3.5 Test documentation shall accurately reflect the system components and configurations tested. Systems shall not be accepted if test documentation does not correlate with the installed system.

3.3.6 Any discrepancies or issues discovered shall be corrected by the Contractor. The system or service shall be re-tested to validate that the problem has been resolved.

3.3.7 Upon Authority approval of completed testing, the Contractor shall provide comprehensive as-built documentation for all installed systems including final installation drawings, operation manuals, system configuration documentation, and equipment specifications. All documentation shall be delivered in formats approved by the Authority and shall accurately reflect final installed conditions.

3.4 Operation Readiness and Transition (ORAT)

3.4.1 Upon successful completion of construction, system testing, and commissioning, the Contractor shall execute a structured transition process to prepare the Private Wireless Network for operational service. This transition will include the establishment of ongoing management and support services, the implementation of maintenance programs, and the delivery of comprehensive training to MWAA IT staff. The Contractor shall coordinate all ORAT activities with the Authority to ensure a seamless handover from construction to operations and to verify that all necessary infrastructure, processes, and personnel are in place to support continuous network operations throughout the term of the contract.

3.4.2 ORAT process shall also determine cutover procedures to the new network, and onboarding of devices. MWAA IT support shall receive all required training, as needed for operation of the MWAA network. The Authority and Contractor shall walk through simulation of network and device level outages, validating how outage tickets and issue resolution shall be mitigated. Support documentation shall be updated and shared collaboratively with the Authority to memorialize the findings.

3.5 Training

3.5.1 The Contractor shall provide comprehensive training to MWAA IT staff on the operation of the Private Wireless Network. Training shall enable Authority personnel to effectively operate the system, monitor network performance, and coordinate with the Contractor on troubleshooting and maintenance activities. Training shall cover system operation and monitoring using the dashboards and monitoring tools provided by the Contractor, including real-time performance tracking, alert management, SIM issuance workflow, and all functions necessary for oversight of the network.

- 3.5.2 Training shall be delivered through a combination of on-site instruction, hands-on exercises with the system, and comprehensive documentation.
- 3.5.3 Training completion shall be documented with sign-off from MWAA IT management confirming receipt of training materials and hands-on instruction. All training materials including manuals, guides, and recorded sessions shall be provided to the Authority. The Contractor shall make subject matter experts available for follow-up questions and refresher training as needed during the term of the agreement. Training sessions shall be scheduled in coordination with the Authority to minimize disruption to ongoing operations and ensure participation from the relevant staff.

3.6 Management and Support

- 3.6.1 The Contractor shall provide comprehensive operational management of the Private Wireless Network throughout the term of the contract, functioning as a managed service provider responsible for all aspects of private wireless network operations and administration. The Contractor shall maintain continuous oversight of network performance, manage system resources, and ensure optimal service delivery to support Authority operations. The Contractor shall manage the complete SIM lifecycle for all MWAA devices, including provisioning, activation, configuration, deactivation, and deprovisioning of SIMs upon Authority request.
- 3.6.2 Authority staff shall submit new device on boarding to the Contractor. The Contractor shall develop a standardized form and intake process for new devices which are onboarded to the network. This shall include provisioning of both physical and eSIM devices.
- 3.6.3 The Contractor shall actively monitor the Private Wireless Network to track system health, performance metrics, and service availability. The Contractor shall provide the Authority with access to dashboards and monitoring tools for visibility into network status and performance. Network monitoring shall enable proactive identification of capacity constraints and performance degradation before they impact operations. The Contractor shall perform system administration functions including user management, device management, network configuration, security policy enforcement, and integration management with Authority infrastructure. All management functions shall be coordinated with the Authority to align with airport operational needs.
- 3.6.4 All services related to the Private Wireless Network shall be performed to the industry standard for similar operations and in a manner deemed acceptable to the Authority.
- 3.6.5 The Contractor shall provide routine and emergency maintenance and active monitoring of the Private Wireless Network during the entire term of the contract. The Contractor shall be solely responsible for all maintenance and repair associated with the Private Wireless Network. Routine maintenance for repairs must be performed on a regular basis to ensure safe and operational equipment.
- 3.6.6 In the event that an emergency repair is required, the Contractor shall notify the Authority of the repair situation as soon as possible. Following such notice, the Authority may inspect the repair work and require alterations if the repair is not satisfactory.

- 3.6.7 The Contractor shall maintain a documented incident response plan that defines incident classifications levels, response procedures, escalation protocols, and post-incident reporting requirements. Critical incidents affecting network availability shall be escalated to the Authority immediately with root cause analysis provided following resolution.
- 3.6.8 The Contractor shall provide live technical support accessible by toll-free number 24 hours per day, 7 days per week. Support personnel shall be qualified to troubleshoot and resolve network issues remotely or dispatch on-site technicians as needed.
- 3.6.9 The Contractor shall provide a ticketing system accessible to the Authority 24 hours per day, 7 days per week. The Contractor shall acknowledge all tickets, provide responses, and resolve requests in a timely manner. SIM provisioning requests shall be submitted through the ticketing system and processed in a timely manner. The Contractor shall support both physical SIM and eSIM provisioning methods based on MWAA device requirements. All provisioned physical SIMs shall be delivered configured and ready for deployment.
- 3.6.10 The Contractor shall have available qualified and properly trained personnel in adequate numbers to provide routine maintenance and to respond to any emergency outages. Personnel shall adequately and safely carry out such services in a courteous, prompt, and efficient manner adequate to meet reasonable user demands. The Contractor shall provide adequate means for the Authority to contact and obtain live human service support on a continuous basis to address technical questions and issues.
- 3.6.11 The Contractor shall establish procedures for handling customer complaints. The Contractor shall respond to every complaint, written or oral, within a timely manner and shall make good faith efforts to explain, resolve, or rectify the cause of the complaint. The Contractor shall provide the Authority with a copy of each such complaint and its response thereto upon request by the Authority.
- 3.6.12 The Private Wireless Network shall maintain a minimum service availability of 99.9% uptime, measured monthly. Planned maintenance windows approved by the Authority shall be excluded from uptime calculations.
- 3.6.13 The Contractor shall provide the Authority with access to real-time monitoring dashboards with data export capabilities and analytics tools to support operational analysis and planning. Dashboards shall display at a minimum:
- Network health status.
 - Per-AP performance metrics.
 - Throughput and latency measurements.
 - Historical performance data.
 - Ticket volume and resolution metrics.
 - SIM provisioning activity.
 - Capacity utilization metrics.

3.6.14 The Contractor shall provide monthly performance reports to MWAA IT management staff summarizing network performance, operational metrics, and any significant incidents or maintenance activities during the reporting period.

3.6.15 Technical support shall be available to MWAA IT staff for questions regarding network operation, performance issues, system monitoring, and configuration needs. The Contractor shall provide incident response, ticket escalation, and troubleshooting services to identify, diagnose, and resolve network problems, service disruptions, and performance degradation. Support services shall include remote diagnosis and resolution as well as on-site technical assistance when required. All active tickets shall be managed in an open platform in which the Authority has access and visibility.

3.7 Deliverables Table

3.7.1 The following table summarizes the principal deliverables associated with the Private Wireless Network implementation and ongoing managed service requirements described in this Statement of Work.

Section	Deliverable	Description	Timing / Frequency
3.1	Project Kickoff Package	Project plan, schedule, communications plan, escalation procedures, and contractor staffing introduction.	Within two weeks after contract award.
3.1	Status Reporting	Written weekly status reports and materials supporting bi-weekly project review meetings.	Weekly and bi-weekly throughout project execution.
3.2	Design Submittals	50% and 100% construction documents, shop drawings, product data, component details, permits, certifications, and PE-stamped materials as required.	Prior to installation and as required during design approval.
3.2	Construction Execution Package	Construction plan, coordinated schedule, methods of procedure, and all required installation materials and infrastructure for a complete buildout.	Before and during construction.
3.3	Test and Commissioning Reports	Component, end-to-end, coverage, performance, and integration testing results, including discrepancies, resolutions, data sheets, and sign-offs.	At completion of testing and prior to acceptance.
3.3	As-built Documentation Package	Final installation drawings, operation manuals, system configurations, and equipment specifications reflecting the installed environment.	Upon successful testing and before transition to operations.

3.4	ORAT Transition Package	Cutover procedures, device onboarding approach, outage simulation outcomes, and updated support documentation for handoff to operations.	At transition from implementation to operations.
3.5	Training Package	On-site instruction, hands-on exercises, manuals, guides, recorded sessions, and training completion sign-off.	Before operational handoff and as needed during the agreement term.
3.6	Operational Support Package	Monitoring dashboards, standardized onboarding forms, incident response procedures, ticketing access, SIM lifecycle support, and 24x7 support services.	Throughout the operational term of the contract.
3.6	Monthly Performance Report	Summary of network performance, service metrics, significant incidents, maintenance activities, and operational trends.	Monthly during managed service operations.

Section 4 General Requirements

- 4.1** Construction activities shall follow the requirements outlined in the Airports Authority Design Manual - <https://www.mwaa.com/business/airports-authority-design-manual> and comply with Authority's Building Code Department <https://www.mwaa.com/business/building-codes-environmental-department> .
- 4.2** The Contractor shall ensure, at Contractor's sole cost and expense, all employees obtain an Airport-issued ID badge and shall ensure all employees wear and display in an acceptable manner their Airport ID at all times while on Airport property. Employees must fully comply with all applicable TSA regulations regarding conduct and access to the Airport Operating Area.
- 4.3** The Contractor shall monitor the movement of its vehicles or equipment to minimize conflict with other functions and users of the Airport and shall coordinate its use of the Airport with the Authority, airport tenants, and other users. The Contractor shall be responsible for all requirements associated with driving on the airfield (insurance, training, etc.).
- 4.4** The Contractor agrees that it shall be responsible for ensuring that its employees abide by all applicable federal, state, local, and Authority laws, rules and regulations including, without limitation, the Airport's Rules and Regulations, Order & Instructions, and all applicable FAA, CBP, TSA, and Authority security rules, regulations, plans orders, directives, requirements, and procedures.
- 4.5** The Contractor shall have all staff attend all required safety briefings required for site access. The Contractor shall coordinate the site access and all installations with the appropriate contractor prior to installation. Personal Protective Equipment (PPE) shall be properly worn by all personnel in accordance with applicable safety requirements and job-specific hazards.
- 4.6** Installers shall comply with Occupational Safety and Health Administration (OSHA) regulations for tower work. This includes fall protection, climbing, and tethering requirements.
- 4.7** The Contractor shall promptly repair, at its sole expense, any damage to Authority facilities caused by the Contractor or any Contractor agent.
- 4.8** The Contractor shall coordinate with the Authority on a timely basis regarding access through Airport facilities to accomplish the equipment turnover, construction, installation, or testing.

Private Wireless Network Design Package

MWAA

10/10/2025



Table of Contents

Section 1 Design Overview 4

Section 2 Local Physical Diagram 5

Section 3 Logical Diagram 6

Section 4 Technical Specifications 7

Table of Figures

Figure 1: Overall Network Reference Architecture 4

Figure 2: AP Network Physical Connection 5

Figure 3: Network Logical Diagram..... 6

Section 1 Design Overview

MWAA's private wireless network will use a Celona-based platform operating in the Citizens Broadband Radio Service (CBRS) spectrum from 3550-3700 MHz at IAD and DCA. Mobile users, fixed assets and any other IT related asset which can utilize wireless communications will utilize this private network for communications. It shall enable local routing of traffic to MWAA enterprise applications, along with internet access as required.

Each airport will deploy Enterprise Edge controller pairs in a high-availability configuration at the IAD and DCA headends. Single-mode fiber will provide primary connectivity from each controller to the Nexus 7710 core switches, while dedicated direct fiber links between controller pairs enable heartbeat monitoring and state synchronization. From the head-ends, the Enterprise Edge controllers will extend connectivity to access switches located in airport Telecommunication Rooms, which will then connect to Access Points (APs) distributed throughout the campus. These Access Points distribute signal to antennas to deliver RF coverage to end-user devices.

The Celona platform will connect to MWAA's existing MPLS/VPNv4 infrastructure and terminate (SIM cards at the enterprise edge. Traffic will route through MWAA's Richmond and Ashburn data centers. Network segmentation will separate operational traffic from management functions. Role-based access controls will limit administrative privileges, and the system will integrate with MWAA's Entra ID for single sign-on. WPA3-Enterprise encryption will protect data in transit with device authentication.

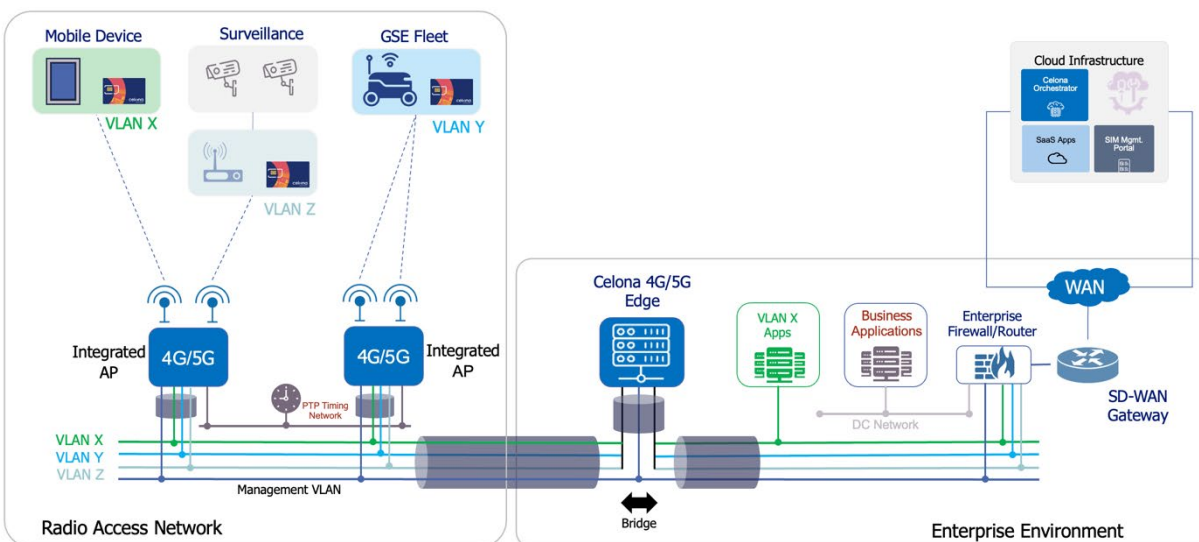


Figure 1: Overall Network Reference Architecture

Section 2 Local Physical Diagram

The Access Point (AP) Network Physical Connection Diagram provides a comprehensive visual representation of the wired and/or wireless infrastructure supporting the private wireless network deployment at MWAA Airports (DCA and IAD). The physical diagram depicts the actual specific components put together to enable the Access Points to function in their deployed state.

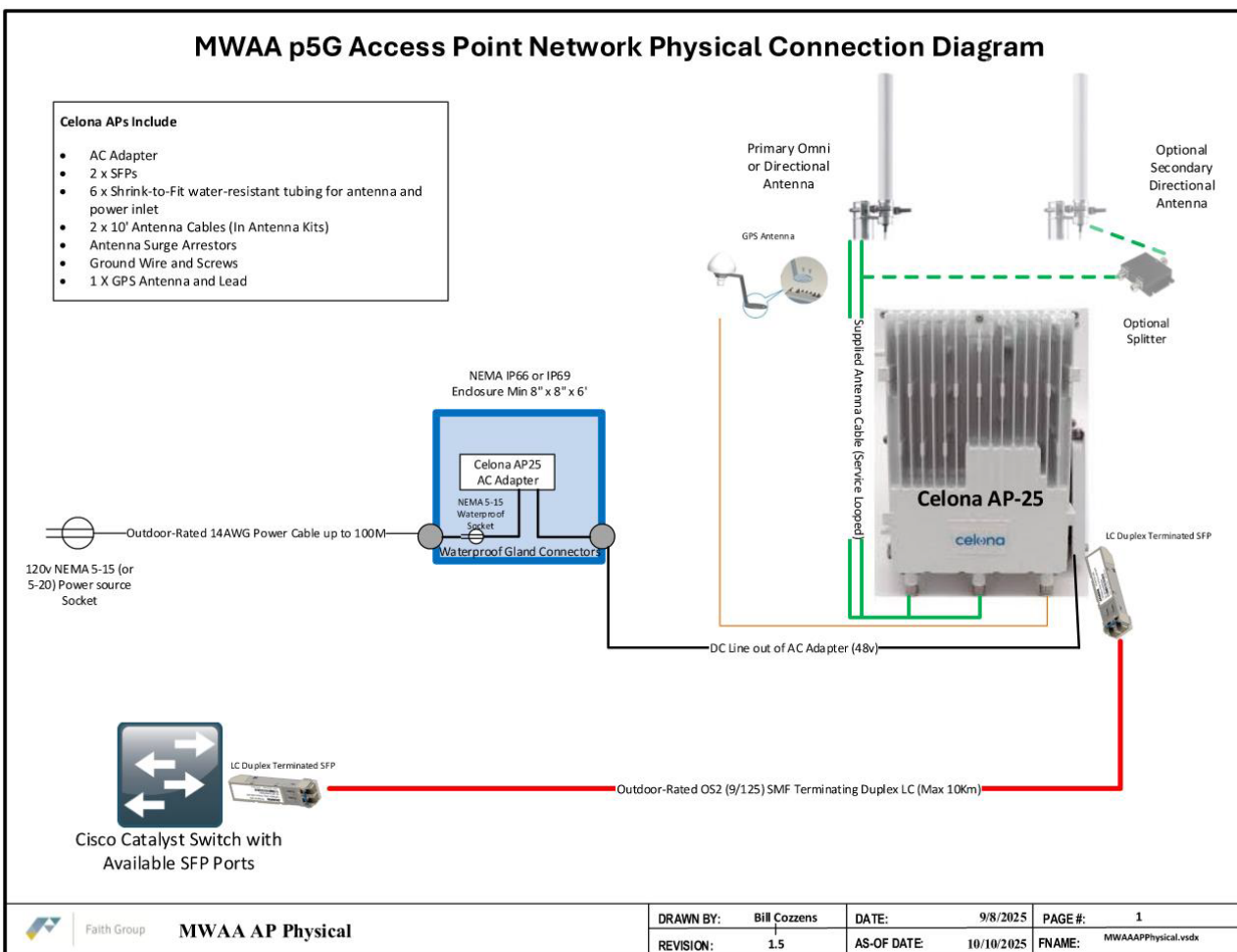


Figure 2: AP Network Physical Connection

Additional design notes include:

- The Celona AP-25 shall be placed in MWAA IDF rooms or mounted to exterior poles where no local rooms exist. CoaX cables shall be extended from the Celona AP to antenna mounting points on existing structure.
- All locations identified within the design have available local power and enclosures. Throughout the DCA campus, these power adapters shall be placed in the existing PIDS enclosures or IDFs, where power is currently available.
- APs shall be mounted in a ventilated location, in order to dissipate heat.
- APs consumed approximately 100W of power.

Section 3 Logical Diagram

The logical diagram describes the functional interrelationships between the components that compose the solution. Private wireless traffic shall be routed over the existing MWAA LAN. Each Airport shall receive two Celona enterprise edge devices.

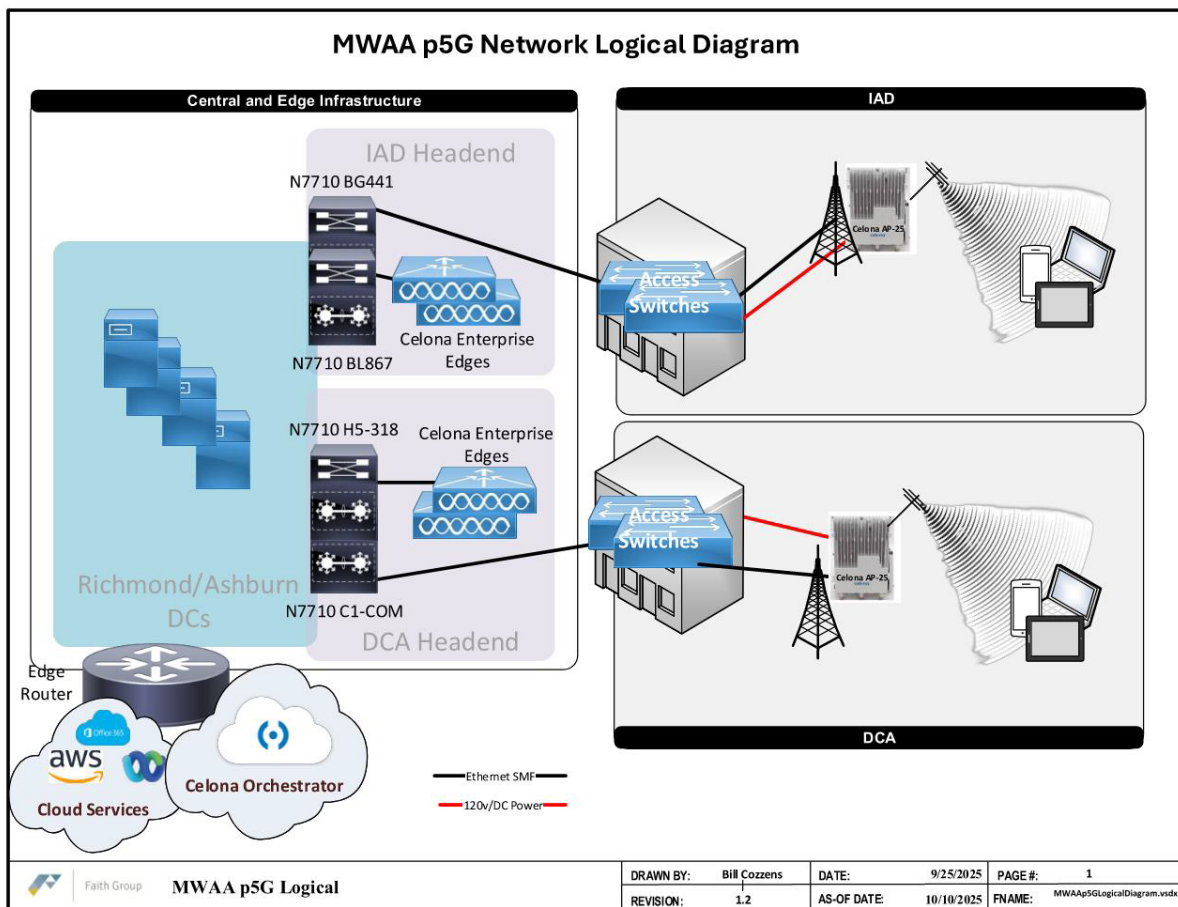


Figure 3: Network Logical Diagram

MWAA shall be responsible for configuration of the network. Celona Orchestrator, which is a cloud-based platform, shall monitor and control all of the APs and SIMs. It shall function as a centralized platform for management of the Celona APs. ISP connectivity shall also be required on the network, to support routing of devices to cloud based platforms.

The initial systems which would require communication over the Private Wireless system would include:

- Maintenance and Operations iPads – General connectivity for applications
- Video Surveillance Cameras
- Utility Meters
- Mobile Vehicles and Assets
 - o To be supported via a Cradlepoint or other similar mobile solution on the system.

Section 4 Technical Specifications

The Technical Specifications provide key details that help describe the operating standards that the solution incorporates, both from a sourcing as well as an interoperability standpoint.

Network

Enterprise Edge V2 Nodes

- Network:
 - One (1) 1G Base-T (Intelligent Platform Management Interface)
 - Two (2) 1/10G Base-T
 - Two (2) 10/25G SFP+
 - Two (2) 1/10G Base-T
- Power
 - Dual 500W Power Supplies
 - Power Cables for NEMA 5-15P supplied

AP Network Interfaces

- 1GE 1GBASE-T (RJ-45)
 - Exclusive either/or.
 - Generally not in use, preference is SFP+
- SFP+ 1GE
 - Duplex LC Fiber presentation.
 - SFPs (Provided) are generally Accelink RTX191-400 or later equivalent.
 - Max supported distance (shorter (<200M) highly recommended) 10KM
 - Fiber Supported=1310nm SingleMode.

Antennas

AP Antenna Cables

- 2 x 10 Foot is baseline of what is supplied.
 - Detailed final design layout by contractor to determine final exact length for antenna Coax.
- If custom cable:
 - 50-ohm, LMR-400,
 - Connector is N-Type Threaded. Male on AP.
- GPS Jumper Cable is supplied.
- If Sectors are split with two antennas,
 - Splitter (CN-ANT-SPL) is required

Antenna

- Depending on designated coverage, three types of antenna will be used:
 - Omni-directional antenna with 3.3-3.8GHz frequency range, horizontal/vertical polarization type, 13 dBi gain, 7 degree vertical beamwidth, 360 degree horizontal beamwidth, 1 degree electrical downtilt, 30 dB port isolation, and 2 x Type N Female

connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.

- 90-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45-degree slant, 16.7 dBi gain, 6.5-degree vertical beamwidth, 45-degree horizontal beamwidth, 2-degree electrical downtilt, 31 dB front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.
- 33-degree sector antenna with 3.5-4.2GHz frequency range, polarization type of 45-degree slant, 18.8 dBi gain, 8-degree vertical beamwidth, 33-degree horizontal beamwidth, 4-degree electrical downtilt, 35 dB front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.

Power

AP Power Supply:

- Power Draw:
 - 100W Maximum, generally at power-on.
- Plug Types:
 - Power Source End: NEMA 5-15P 120v
 - Extendable with 14AWG Power cable, terminating NEMA 5-15R,
 - Max length 100m.
 - Ground terminal needs to be earthed.
- AP End: 48vDC, custom female double spade connector.
 - AP has dual male spade connector.
 - Mid-cable gland connector provided.

Private Wireless Regulatory Compliance Report

Metropolitan Washington Airports Authority

October 10, 2025



Table of Contents

Section 1 Introduction and Summary 1

Section 2 Design Approach and Network Compliance 1

Section 3 FCC Compliance 2

3.1 Frequency Bands and Deployment 2

3.2 Spectrum Access System Operations 2

Section 4 FAA Compliance 3

Section 5 Privacy Compliance..... 3

5.1 General Celona Privacy Compliance..... 3

5.2 General Data Protection Regulation (GDPR) Compliance 4

Section 6 Security Compliance 4

6.1 Cisco ISE Integration 4

6.2 eSIM/MDM Integration 4

6.3 Encryption/CNSA 2.0 5

Section 7 Installation Compliance 5

Table of Figures

Figure 1 - Private Wireless Network Architecture 2

Section 1 Introduction and Summary

This document provides an overview of the many different levels of regulation and compliance which apply to the new Private Wireless environment. The sections are focused on the following core areas:

1. Design Approach and Network Compliance
2. FCC Compliance
3. FAA Compliance
4. Privacy Compliance
5. Security Compliance
6. Installation Compliance

As indicated in the following report, there are no major known compliance issues or regulatory compliance challenges with the deployment of the proposed Private Wireless Solution. The deployment shall follow standard practices and submittals, as outlined in the report. The FCC's CBRS regulatory framework is well-established with clear coordination procedures through the Spectrum Access System (SAS), and the Private Wireless system will integrate with MWAA's existing security and network infrastructure. Required FAA filings will follow standard airport construction approval processes already familiar to MWAA operations.

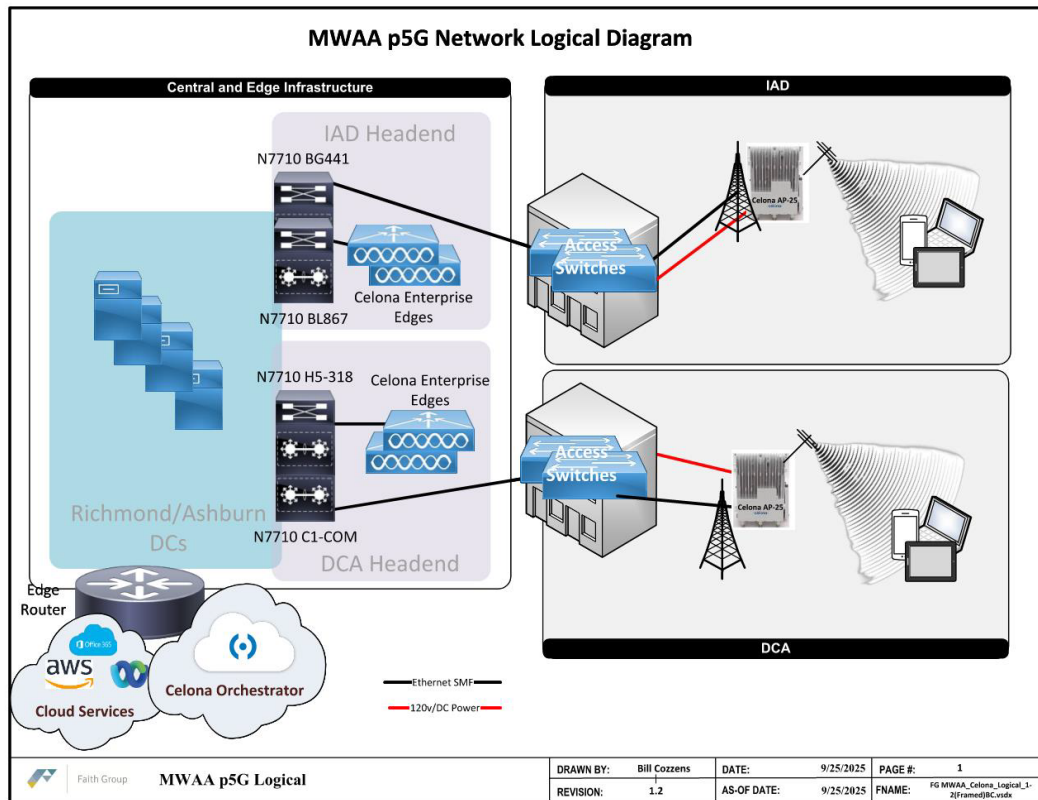
Section 2 Design Approach and Network Compliance

MWAA's private wireless network will use a Celona-based platform operating in the Citizens Broadband Radio Service (CBRS) spectrum from 3550-3700 MHz at IAD and DCA. Mobile users, fixed assets, and any other IT related asset which can utilize wireless communications will utilize this private network for communications. It shall enable local routing of traffic to MWAA enterprise applications, along with internet access as required.

Each airport will deploy Enterprise Edge controller pairs in a high-availability configuration at the IAD and DCA headends. Single-mode fiber will provide primary connectivity from each controller to the Nexus 7710 core switches, while dedicated direct fiber links between controller pairs enable heartbeat monitoring and state synchronization. From the head-ends, the Enterprise Edge controllers will extend connectivity to access switches located in airport Telecommunication Rooms, which will then connect to Access Points (APs) distributed throughout the campus. These Access Points distribute signal to antennas to deliver RF coverage to end-user devices.

The Celona platform will connect to MWAA's existing MPLS/VPNv4 infrastructure and terminate (SIM cards at the enterprise edge. Traffic will route through MWAA's Richmond and Ashburn data centers. Network segmentation will separate operational traffic from management functions. Role-based access controls will limit administrative privileges, and the system will integrate with MWAA's Entra ID for single sign-on. WPA3-Enterprise encryption will protect data in transit with device authentication.

The Celona Assure service will provide continuous monitoring, automatic updates, patch management, and incident response support. The controller configuration will allow for service to be maintained if one unit fails. The network architecture design meets NIST Cybersecurity requirements, MWAA cybersecurity standards, and Transportation Security Administration (TSA) Cybersecurity requirements.

Figure 1 - Private Wireless Network Architecture

Section 3 FCC Compliance

3.1 Frequency Bands and Deployment

The CBRS framework in Title 47 Code of Federal Regulations (CFR) allows private wireless in the 3550-3700 MHz band through a three-tier system. Incumbent federal users receive first priority, Priority Access License (PAL) holders come second, and General Authorized Access (GAA) users operate opportunistically in remaining spectrum. GAA users accept interference from other GAA users but receive protection from harmful PAL interference through SAS coordination. The deployment will operate in GAA tier on the n48 band, which covers the full 3550-3700 MHz range in time-division duplex mode.

Category B Citizens Broadband Radio Service Devices (CBSDs) permit outdoor installation with maximum EIRP of 47 dBm (50 watts) per 10 MHz. The Celona access points carry this certification and include required security capabilities for encrypted Spectrum Access System (SAS) communication. All equipment undergoes FCC equipment authorization procedures before deployment.

3.2 Spectrum Access System Operations

All CBSDs device must operate under an FCC-authorized SAS. The Celona platform will register each unit to the SAS automatically during initial deployment by submitting FCC ID, serial number, device category, antenna gain, height above ground, indoor/outdoor classification, and other parameters. The SAS will check

this data against protection criteria for incumbent users, PAL holders, and other GAA users before authorizing operation.

Spectrum grants define the specific frequency range, maximum Equivalent Isotropically Radiated Power (EIRP), and grant duration for each device. Devices cannot transmit outside these parameters and must stay silent during power-on until the SAS grants authorization. If SAS communication drops for an extended period, transmission must stop. Any changes to the installation parameters will require updated registration with the SAS. The Celona platform will manage this process automatically if changes occur. Devices will maintain a heartbeat mechanism with the SAS, typically communicating every 60 to 240 seconds depending on SAS requirements. During these exchanges, each device will confirm continued operation within grant parameters and receive updates to operating instructions.

Federal radar systems, primarily Navy shipborne units and Department of Defense installations, hold primary rights to the 3550-3700 MHz frequencies. When these systems activate, they take priority over all other CBRS operations. Environmental Sensing Capability (ESC) sensors deployed along coasts and near federal installations continuously monitor radar activity. When federal radar operations are detected, the SAS immediately calculates which devices must modify operation to protect the radar. The SAS will move affected devices to different channels within the 3550-3700 MHz band, reduce transmit power, or suspend grants until federal radar activity ceases. The Celona Enterprise Edge controllers will handle channel switching and load balancing across available spectrum to maintain network service during these transitions.

Section 4 FAA Compliance

All access points and antennas will be mounted to existing structures, will not raise the height of any structure, and will not cause any sightline interference with ATC towers. Nonetheless, all construction or alteration of structures on airport property will require FAA approval through Form 7460-1, regardless of height. Filing requires at least 45 days advance notice before construction with location coordinates, site elevation, total structure height, antenna radiation center heights, and effective radiated power.

CBRS operations in 3550-3700 MHz range require no FAA RF coordination beyond the construction approval process. The 500 MHz frequency separation between CBRS and FAA radars operating in 4.2-4.4 GHz provides adequate protection, ensuring no interference.

Section 5 Privacy Compliance

Celona Private 5G Solutions meet or exceed a variety of privacy standards, which directly or indirectly apply to MWAA. Celona does not collect any Personal Health Information (PHI) and is HIPAA-Compliant by default. Celona products are SOC II certified and compliant.

5.1 General Celona Privacy Compliance

The Celona platform collects Customer Personal Data in three categories. User Data includes administrator information collected during registration including name, email address, company details, and IP addresses from Orchestrator login sessions. Device Data consists of technical identifiers from connected devices: IMSI, IMEI, SIM ID, ICCID, and IP addresses. Whether this qualifies as personal information depends on device assignment. MWAA-managed devices typically won't have subscriber-level associations, and the Celona system cannot identify individual subscribers using only the device identifiers it collects. Subscriber

names and related information stay with the cellular carriers. Packet Data refers to network traffic information that the Edge Appliance collects when requested by the customer. This primarily relates to LTE control messages using the S1AP protocol. Personal devices connecting to the network may introduce personal data through this channel. Data collection is limited to traffic passing through MWAA's Edge Appliance deployment.

5.2 General Data Protection Regulation (GDPR) Compliance

Celona processes personal data according to documented customer instructions and functions as a data processor under GDPR. Processing occurs solely to deliver Celona products and services. Sub-processor agreements restrict personal data usage, and Celona provides notification when adding new sub-processors. Celona does not sell any user data.

Technical and organizational measures protect personal data in the system. Personnel accessing this data are subject to confidentiality obligations. Cross-border data transfers use mechanisms required by applicable law. Data deletion follows terms established with each customer.

The Data Processing Agreement contains the data privacy and protection terms governing Celona's handling of customer personal data. All customer orders operate under the DPA. One DPA covers the relationship between MWAA and Celona.

Section 6 Security Compliance

6.1 Cisco ISE Integration

The Celona platform integrates with the Cisco Identity Services Engine (ISE) for network access control and policy enforcement. The integration splits authentication and authorization functions. SIM-based authentication occurs directly on the Celona Edge through HSS functions. Cisco ISE handles authorization through RADIUS.

When a device connects to the network, authentication happens first using SIM credentials. The Celona Edge then initiates an authorization request to Cisco ISE. The request includes device identifiers using either IMEI for device-based authorization or IMSI for SIM-based authorization. Cisco ISE matches these identifiers against configured policies and returns the appropriate device group assignment.

The device group determines network and security parameters. Once assigned, the Edge automatically configures QoS settings, admission controls, and VLAN segmentation based on the device group. This approach will allow MWAA to use a single policy engine to authorize devices across the Private Wireless network. Cisco ISE is able to send Change of Authorization or Disconnect commands to the Edge in response to security incidents. This will allow the system to quarantine devices at the network edge.

6.2 eSIM/MDM Integration

The Celona platform supports CBRS credential provisioning through both physical SIM cards and embedded SIM profiles. The platform works with SIM provisioning services to prepare credentials for deployment. MWAA IT will be able to request credentials through standard workflows and receive either physical SIMs or activation codes for over-the-air eSIM provisioning.

The platform integrates with standard Mobile Device Management (MDM) systems to support automated provisioning workflows. For dual-SIM devices that require both MNO and CBRS connectivity, the Mobile Network Operator (MNO) credential typically resides in the physical SIM slot while CBRS credentials can be added as eSIM profiles. This configuration keeps MNO network certification independent from enterprise network provisioning.

6.3 Encryption/CNSA 2.0

Private wireless networks encrypt radio signals at the physical layer between access points and end devices. The Celona platform uses 128-bit AES ciphering over the air interface. This quantum-resistant cryptography meets NSA CNSA 2.0 requirements. The platform implements enhanced key derivation and rotation protocols where master keys remain on the network side and are never transmitted during authentication exchanges. Device identities are concealed during initial connection setup through subscription concealed identifier technology.

Traffic remains encrypted from the access point through the Edge controller to the enterprise network. The platform terminates SIM-based authentication at the Edge and integrates with existing enterprise security controls. This allows encrypted cellular traffic to flow directly into protected VLANs and network segments without requiring additional tunneling or encryption layers.

Section 7 Installation Compliance

All outdoor devices must be professionally installed by Certified Professional Installers (CPI) who will maintain installation parameter records for FCC inspection. External antennas will be installed with proper orientation and isolation to minimize interference with existing airport wireless systems.

Installers will comply with Occupational Safety and Health Administration (OSHA) regulations for tower work. This includes fall protection, climbing, and tethering requirements. Lightning protection arrestors will be installed per applicable electrical codes and manufacturer specifications for all outdoor antenna installations. All installation contractors will undergo TSA security screening and obtain Security Identification Display Area (SIDA) badges for unescorted access to secure areas at both MWAA airports.

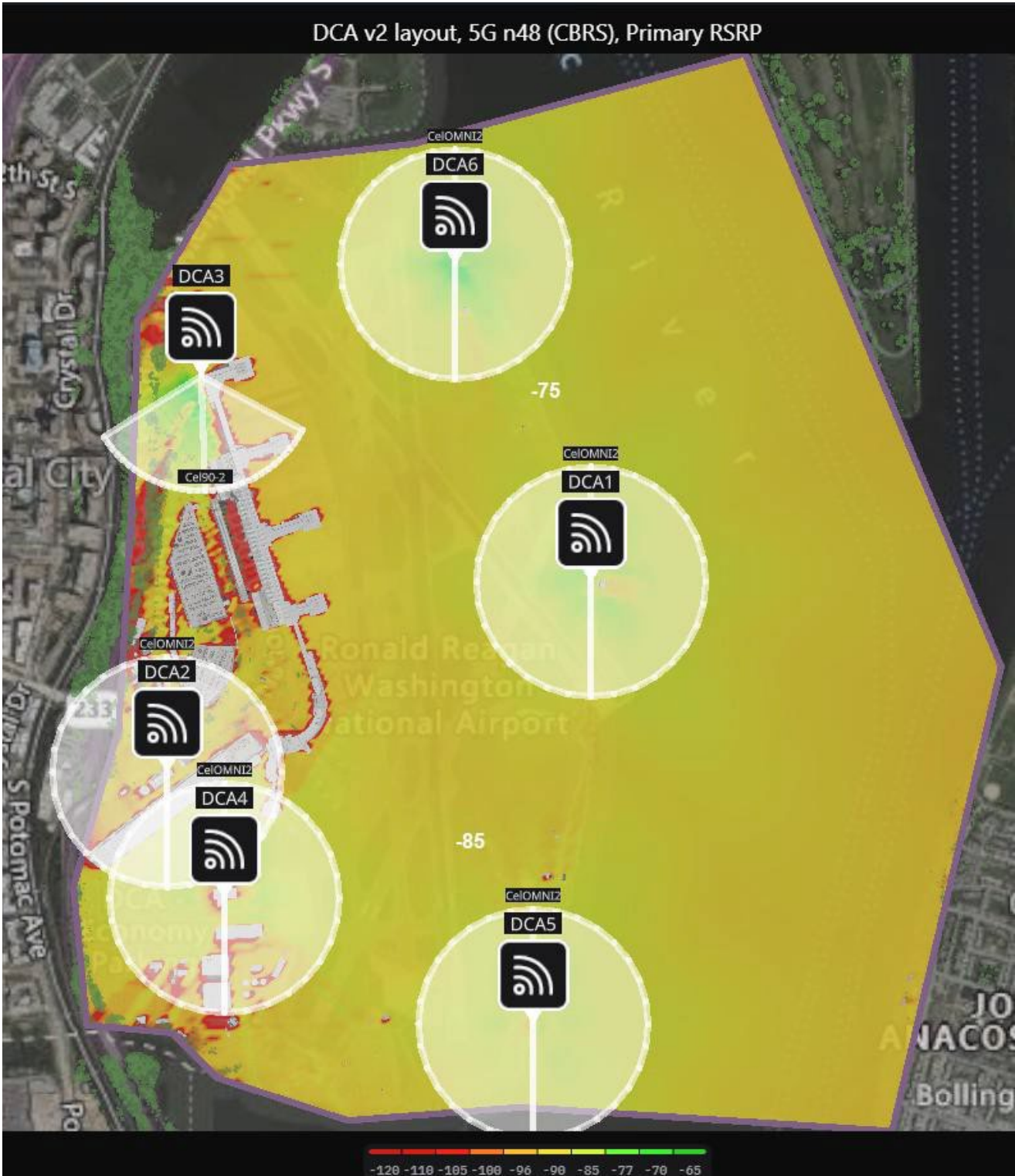


Figure 1-DCA Full Buildout RSRP



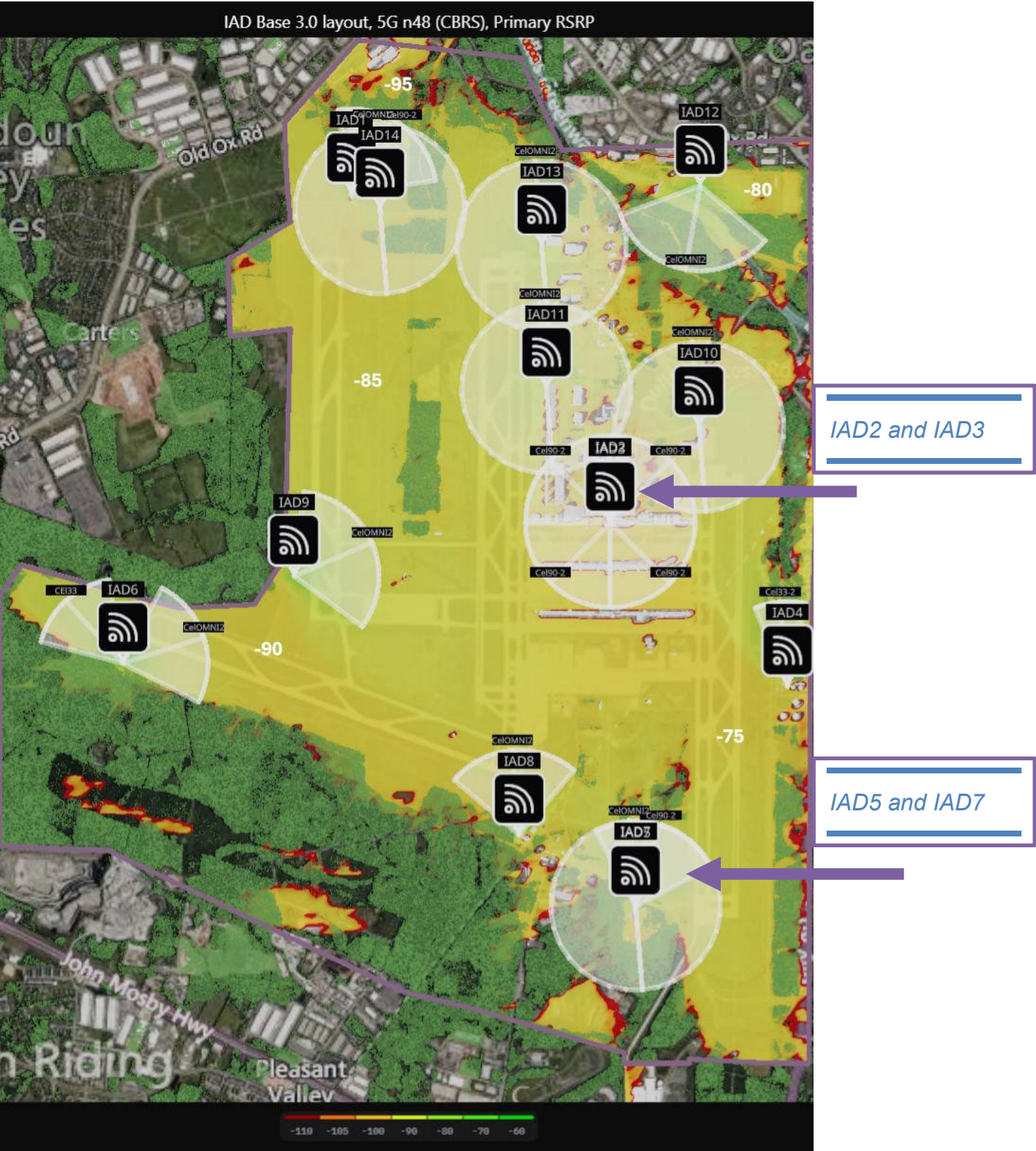


Figure 3 - IAD Full Buildout RSRP

SOW Appendix D: AP Site Location Detail Maps

DCA Buildout

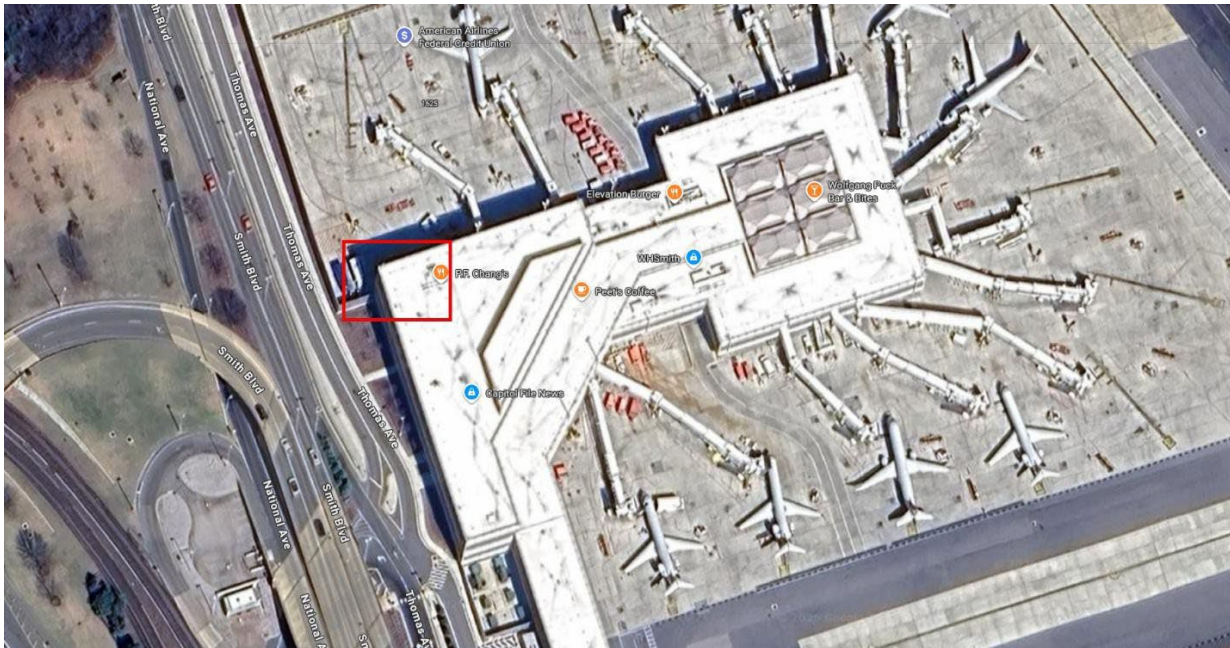
DCA1: North Boathouse, Camera Pylon



DCA2: Central Utility Plant Tower



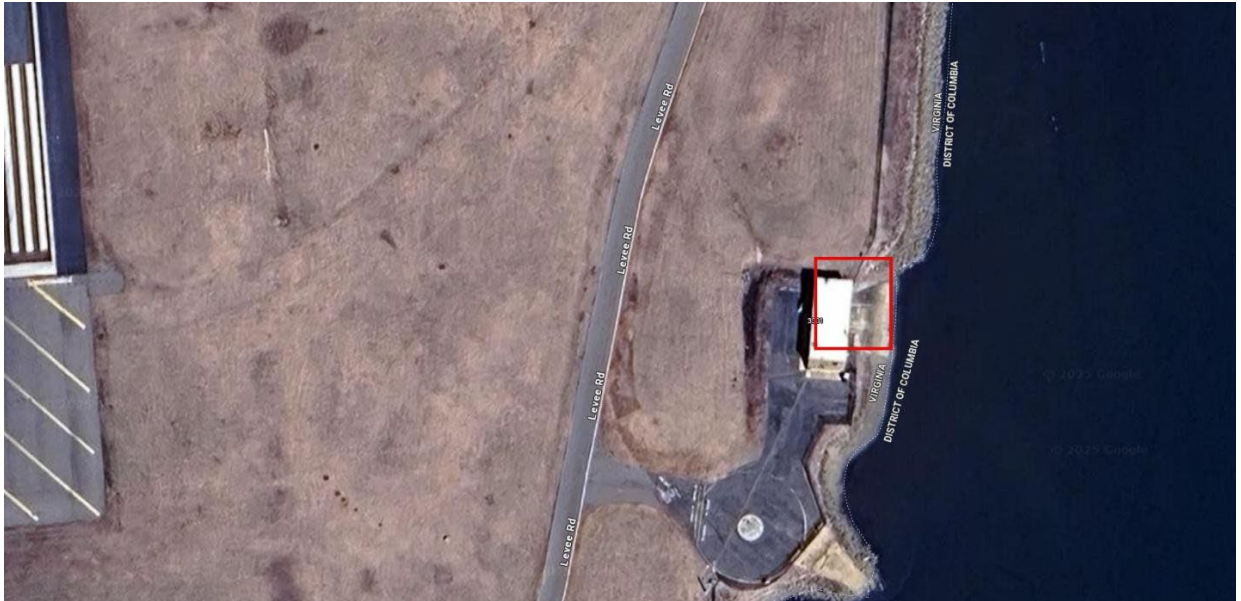
DCA3: Terminal C, Northwest Vertex



DCA4: ARFF Station 301, Hose Tower



DCA5: South Boathouse



DCA6: Levee Road, Camera Pylon at 38.86062168398527, -77.03678022574346

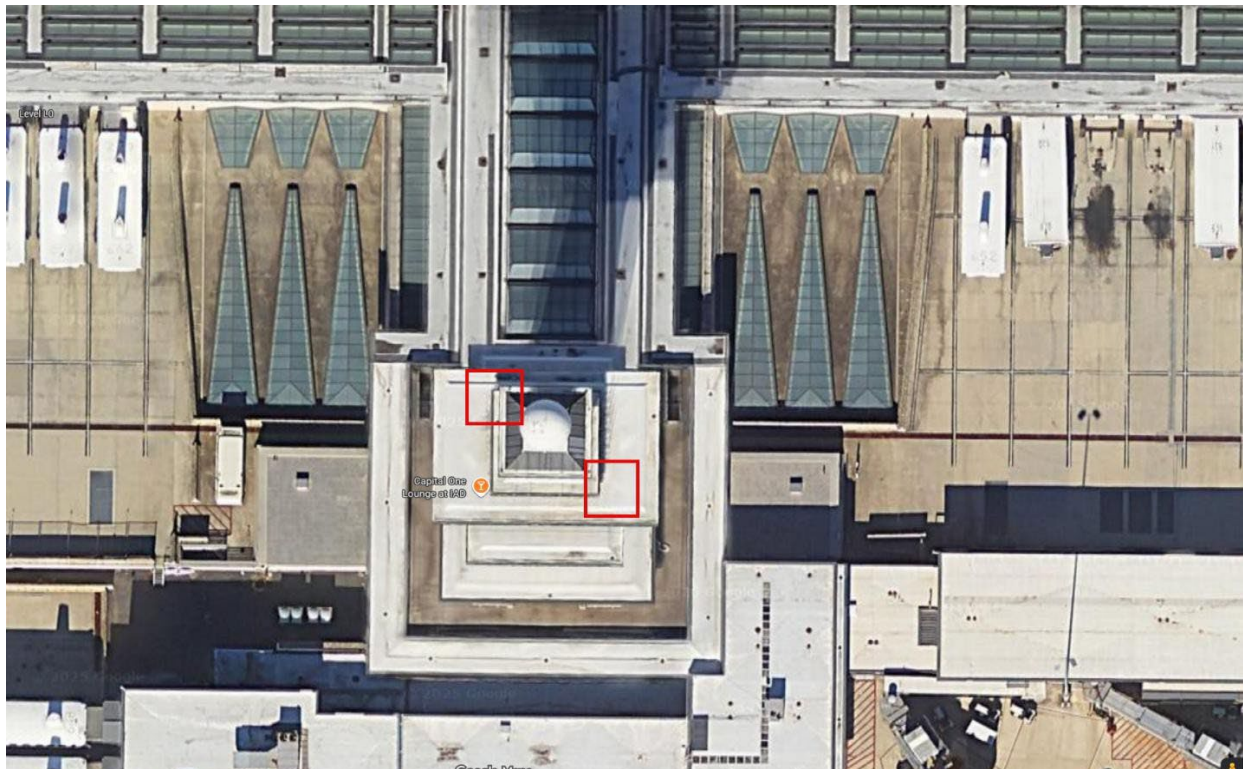


IAD Buildout

IAD1: ARFF Station 304, Hose Tower



IAD2 and IAD3: Old IAD ATC Tower, Deck 3, NW Vertex and SE Vertex



IAD4: Backup Radio Tower, by Fuel Farm



IAD5 and IAD7: South 800MHz Radio Tower



IAD6: Camera Pylon, off of Vortac Rd



IAD8: ARFF Station 302, Northwest Vertex



IAD9: Camera Pylon, off of Instrument Rd



IAD10: Dulles Jet Center, near Wind Sock Dr



IAD13: UA Hangar, Southwest Vertex



IAD14: North 800MHz Radio Tower



Project	network	ap_name	latitude	longitude	mounting_h eight	mounting_ location	model_name	manufacturer	sector_name	antenna_model	antenna-description	transmit-gain (dBi)	antenna_a azimuth	antenna_d owntilt	bands	transmit_ power_m w	transmit_ power_d bm	channel	channel_frequency_ mhz	channel_bandwidth
DCA Buildout Draft 3-2BC	Cellular	DCA1	38.85262214730554	-77.0323867	6.1	Pole	AP 25	Celona	CeIOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	0	0	n48	5012	37	AP25CAR-STD-PCI2	3650	40
DCA Buildout Draft 3-2BC	Cellular	DCA2	38.84782952374957	-77.04603027	45.72	Pole	AP 25	Celona	CeIOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	0	0	n48	5012	37	AP25CAR-STD-PCI0	3570	40
DCA Buildout Draft 3-2BC	Cellular	DCA3	38.85780099690887	-77.044935	9.14	Pole	AP 25	Celona	CeI90-2	CN-ANT-120D	120-degree sectorized antenna with 2 N-Type Connectors and 14.5 dBi gain	14.5	178	0	n48	5012	37	AP25CAR-STD-PCI1	3610	40
DCA Buildout Draft 3-2BC	Cellular	DCA4	38.84465323485602	-77.04418651	9.14	Pole	AP 25	Celona	CeIOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	0	0	n48	5012	37	AP25CAR-STD-PCI6	3650	40
DCA Buildout Draft 3-2BC	Cellular	DCA5	38.841484002632775	-77.034246	9.14	Pole	AP 25	Celona	CeIOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	0	0	n48	5012	37	AP25CAR-STD-PCI3	3610	40
DCA Buildout Draft 3-2BC	Cellular	DCA6	38.86061454882149	-77.03676172	3.05	Pole	AP 25	Celona	CeIOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	0	0	n48	5012	37	AP25CAR-STD-PCI4	3610	40

Project	network	ap_name	latitude	longitude	mounting_height	mounting_location	model_name	manufacturer	sector_name	antenna_model	antenna_description	transmit_gain_dbi	antenna_azimuth	antenna_down_tilt	bands	transmit_power_mw	transmit_power_dbm	channel	channel_frequency_mhz	channel_bandwidth
IAD_Buildout_Draft_5.6BC	Cellular	IAD1	38.97530579092493	-77.47138277	9.14	Pole	AP 25	Celona	Cel90-2	CN-ANT-90D	90-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45 degree slant, 16.7 dBi gain, 6.5 degree vertical beamwidth, 45 degree horizontal beamwidth, 2 degree electrical downtilt, 31 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.	16.7	36		0 n48	5012	37	AP25CAR-STD-PC14	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD2	38.952034001467226	-77.447805	48.77	Pole	AP 25	Celona	Cel90-2	CN-ANT-90D	90-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45 degree slant, 16.7 dBi gain, 6.5 degree vertical beamwidth, 45 degree horizontal beamwidth, 2 degree electrical downtilt, 31 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.	16.7	315		0 n48	5012	37	AP25CAR-STD-PC11	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD2	38.952034001467226	-77.447805	48.77	Pole	AP 25	Celona	Cel90-2	CN-ANT-90D	90-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45 degree slant, 16.7 dBi gain, 6.5 degree vertical beamwidth, 45 degree horizontal beamwidth, 2 degree electrical downtilt, 31 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.	16.7	45		0 n48	5012	37	AP25CAR-STD-PC11	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD3	38.95189070279576	-77.4478135	48.77	Pole	AP 25	Celona	Cel90-2	CN-ANT-90D	90-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45 degree slant, 16.7 dBi gain, 6.5 degree vertical beamwidth, 45 degree horizontal beamwidth, 2 degree electrical downtilt, 31 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.	16.7	225		0 n48	5012	37	AP25CAR-STD-PC12	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD3	38.95189070279576	-77.4478135	48.77	Pole	AP 25	Celona	Cel90-2	CN-ANT-90D	90-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45 degree slant, 16.7 dBi gain, 6.5 degree vertical beamwidth, 45 degree horizontal beamwidth, 2 degree electrical downtilt, 31 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.	16.7	135		0 n48	5012	37	AP25CAR-STD-PC12	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD4	38.94022799946445	-77.431664	36.58	Pole	AP 25	Celona	Cel33-2	CN-ANT-33D	33-degree sector antenna with 3.5-4.2GHz frequency range, polarization type of 45 degree slant, 18.8 dBi gain, 8 degree vertical beamwidth, 33 degree horizontal beamwidth, 4 degree electrical downtilt, 35 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.	17	355		0 n48	5012	37	AP25CAR-STD-PC10	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD5	38.92456500347188	-77.445513	45.72	Pole	AP 25	Celona	Cel90-2	CN-ANT-90D	90-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45 degree slant, 16.7 dBi gain, 6.5 degree vertical beamwidth, 45 degree horizontal beamwidth, 2 degree electrical downtilt, 31 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.		18		0 n48	5012	37	AP25CAR-STD-PC15	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD6	38.94186900340959	-77.49219499	6.1	Pole	AP 25	Celona	CEI33	CN-ANT-65D	65-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45 degree slant, 17 dBi gain, 6 degree vertical beamwidth, 62 degree horizontal beamwidth, 38 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.	17	317.7		0 n48	5012	37	AP25CAR-STD-PC18	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD6	38.94186900340959	-77.49219499	9.14	Pole	AP 25	Celona	CelOMNI2	CN-ANT-90D	90-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45 degree slant, 16.7 dBi gain, 6.5 degree vertical beamwidth, 45 degree horizontal beamwidth, 2 degree electrical downtilt, 31 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.	16.7	72.1		0 n48	5012	37	AP25CAR-STD-PC18	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD7	38.924651	-77.44551	45.72	Pole	AP 25	Celona	CelOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	355.4		0 n48	5012	37	AP25CAR-STD-PC1	3670	40

Project	network	ap_name	latitude	longitude	mounting_height	mounting_location	model_name	manufacturer	sector_name	antenna_model	antenna_description	transmit_gain_dbi	antenna_azimuth	antenna_down_tilt	bands	transmit_power_mw	transmit_power_dbm	channel	channel_frequency_mhz	channel_band_width
IAD_Buildout_Draft_5.6BC	Cellular	IAD8	38.92965600253963	-77.456124	9.14	Pole	AP 25	Celona	CelOMNI2	CN-ANT-90D	90-degree sector antenna with 3.3-3.8GHz frequency range, polarization type of 45 degree slant, 16.7 dBi gain, 6.5 degree vertical beamwidth, 45 degree horizontal beamwidth, 2 degree electrical downtilt, 31 db front to back ratio, and 2 x Type N Female connectors. Each antenna comes with an accessory kit of two surge protectors and two 10-ft LMR400 antenna cables.	16.7	355.4		0 n48	5012	37	AP25CAR-STD-PC17	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD9	38.94807999388774	-77.476613	9.14	Pole	AP 25	Celona	CelOMNI2	CN-ANT-120D	120-degree sectorized antenna with 2 N-Type Connectors and 14.5 dBi gain	14.5	66.6		0 n48	5012	37	AP25CAR-STD-PC13	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD10	38.95871599696203	-77.439734	9.14	Pole	AP 25	Celona	CelOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	355.4		0 n48	5012	37	AP25CAR-STD-PC12	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD11	38.96145900215246	-77.453632	9.14	Pole	AP 25	Celona	CelOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	355.4		0 n48	5012	37	AP25CAR-STD-PC13	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD12	38.97586000236532	-77.439619	9.14	Pole	AP 25	Celona	CelOMNI2	CN-ANT-120D	120-degree sectorized antenna with 2 N-Type Connectors and 14.5 dBi gain	14.5	190		0 n48	5012	37	AP25CAR-STD-PC10	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD13	38.97162400025355	-77.454059	9.14	Pole	AP 25	Celona	CelOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	355.4		0 n48	5012	37	AP25CAR-STD-PC19	3670	40
IAD_Buildout_Draft_5.6BC	Cellular	IAD14	38.97421900201545	-77.468783	48.77	Pole	AP 25	Celona	CelOMNI2	CN-ANT-OMNI	Omni-directional antenna with 2 N-Type connectors and 13 dBi gain	13	355.4		0 n48	5012	37	AP25CAR-STD-PC16	3670	40