STATEMENT OF WORK

TELECOMMUNICATION SYSTEMS SUPPORT SERVICES

2012
TABLE OF CONTENTS

SECTION I - STATEMENT OF PURPOSE 3

SECTION II - BACKGROUND 4

SECTION III - ACS OVERVIEW 5
01 Airports Communications System (ACS) History 5
02 ACS Infrastructure 5
03 ACS Service Offering 6
04 Volume Statistics 6

SECTION IV - ONGOING CHANGES TO THE AIRPORTS AUTHORITY ENVIRONMENT 7

SECTION V - SCOPE OF SERVICES 8
01 Introduction 8
02 Transition Services 8
   A Develop and submit transition plan 8
   B Evaluate and document technical infrastructure 9
   C Review/Update/Develop procedures manuals 9
   D Develop methods for collecting performance data for performance standards 10
   E Transition period reporting 10
03 Base Services 10
   A Telecommunication Systems Program Management 11
   B Site Management 14
   C ACS Technical Support 16
   D ACS Systems Administration & Programming 18
   E NetPlus Systems Support Services 18
   F Administrative Support Services 21
04 Supplemental Services 23
   A Supplemental Parts Services 23
   B Supplemental Construction Services 23
   C Supplemental Consulting Services 24
05 Contract Administration and Reporting Requirements 24
   A Contract Administration 24
   B Reporting requirements 27

SECTION VI - KEY PERSONNEL 29

SECTION VII - SUMMARY OF CONTRACT DELIVERABLES 30
01 Transition Services Period 30
02 Base Services Period 30
SECTION VIII - APPENDICES

APPENDIX 1 - EXISTING TELECOMMUNICATIONS INFRASTRUCTURE
APPENDIX 2 - NETWORK DIAGRAMS
APPENDIX 3 - ACS SERVICES
APPENDIX 4 - HISTORICAL VOLUMES
APPENDIX 5 - HOURS OF OPERATION
APPENDIX 6 - RESPONSIBILITY FOR ASSIGNED PROPERTY
APPENDIX 7 - PERFORMANCE STANDARDS
APPENDIX 8 - SAMPLE POSITION DESCRIPTIONS
APPENDIX 9 - INFORMATION SECURITY STANDARDS
APPENDIX 10 - TELECOMMUNICATION DEPARTMENT ORGANIZATION
APPENDIX 11 - DCA VEHICLE AOA REQUIREMENTS
APPENDIX 12 - IAD VEHICLE AOA REQUIREMENTS
SECTION I - STATEMENT OF PURPOSE

The Metropolitan Washington Airports Authority (Authority) is requesting proposals from qualified firms to assist the Authority Telecommunication Systems Department (MA-620) with management, maintenance, and operation of the Authority Airport Communications System (ACS) and provision of other telecommunication related services. A functional organization chart of MA-620 is presented as Appendix 10. With broad guidance and directions from MA-620, the contractor will provide the day-to-day management, maintenance, operation and support of the Authority ACS and related systems. This will include managing and maintaining the existing telecommunication Infrastructure (see Appendix 1). The Authority intends to collaborate with the Contractor to accomplish the following objectives:

- Improve the identification and marketing of ACS services to tenants
- Improve the quality of technical support services to ACS customers and Authority staff
- Improve response times to service calls
- More closely coordinate ACS development activities
- Ensure Authority-wide ACS standards are developed, maintained and enforced
- Support a secure ACS network environment
- Support and enforce the security of ACS assets
- Sustain the Authority’s ACS environment at current/near current state of the art revision/release levels consistent with the delivery of secure, reliable, consistent service levels
- Identify and, with Authority approval, test and implement new technologies that improve ACS services, increase efficiencies, and reduce costs
- Maintain Industry Best Practices and follow recognized standards in the development, maintenance and delivery of technical support services within the Authority ACS environment
- Identify options to reduce ACS costs
- The length of this contract will be for fourteen (14) months from notice to proceed with four (1) one-year renewal options at the Authority’s sole discretion. The initial fourteen (14) month period of service will be divided into a two (2) month transition services period and a twelve (12) month base service period.

Transition period costs must be reflected in the initial year Base Services rates.
SECTION II - BACKGROUND

The Authority is a regional agency created in 1986 by an interstate agreement between the District of Columbia and the Commonwealth of Virginia. The Authority manages and operates Ronald Reagan Washington National Airport (DCA) and Washington Dulles International Airport (IAD) pursuant to a lease, currently set to expire in 2067, from the Federal Government. The Authority is independent of both the District and the Commonwealth, and issues revenue bonds to make capital improvements to DCA and IAD. The Authority is self-supporting, using aircraft landing fees and revenues from concessions to fund operating expenses. The Authority is not taxpayer-funded. Bonds issued by the Authority, Federal and State Airport Improvement Funds and Passenger Facility Charges fund the Capital Construction Program. For additional background information, offerors are encouraged to visit the Authority’s web site at http://www.mwaa.com.

The Authority’s mission is to operate, develop, and promote the Airports in a manner that is sensitive to the needs of the Metropolitan Washington area traveling public. The Authority is committed to safety and excellence and strives to improve efficiency, responsiveness, and customer orientation.

The Authority employs approximately 1,400 people in a structure that includes central administration, airport operations and management, and public safety (police and fire departments). The Authority's administrative headquarters are located at DCA in its Corporate Office Building (COB). The Office for Information Systems and Telecommunications (OIST) provides information technology, telecommunications and radio/wireless support for the Authority and is responsible for the ACS. The Airports Authority has also assumed responsibility for the Dulles Toll Road operations (DTR) as well as the Dulles Rail Project (DRP).
SECTION III - ACS OVERVIEW

01 AIRPORTS COMMUNICATIONS SYSTEM (ACS) HISTORY

The Authority employs a shared tenant services (STS) business model for the ACS, offering Airport tenants services and equipment for their voice, data and video needs. Tenants are charged for these services based upon a schedule of fees established by the Authority. The revenue collected by the Authority from these tenants for ACS services provided to them is used to offset the Authority’s expense of managing, maintaining and operating the ACS.

ACS End Users are comprised of internal Authority Departments; Authority staff and contractors; and Authority tenants, such as airlines, retail concessions, government organizations (e.g. TSA, FAA) and others. The ACS encompasses:

- **End User Services** - The equipment, management, operations, maintenance and processes that enable local and long distance, land-line dial tone and accompanying features
- **Infrastructure Services** – The facilities, management, operations and processes that provide intra/inter-facility optical fiber and copper connectivity, access to Local Exchange Carrier SONET services, and connectivity between customer premise and third party provider facilities
- **Project Oversight Services** - The management oversight and quality assurance on all Capital Construction and other projects that have a communications plant component.

For the past fourteen years, the Authority has outsourced the management, maintenance and operations of the ACS. Under this new contract, the Authority intends to enhance the close working relationship with the contractor. The Authority expects the contractor’s operations, services, marketing, staffing levels, and adherence to performance standards under the ACS contract to be fully transparent to the Authority during the term of this contract. The Authority further expects the Contractor to engage in a robust effort to market ACS full service offerings to tenants, with the goal of maximizing ACS revenue while minimizing ACS expenses.

02 ACS INFRASTRUCTURE

The ACS copper and optical fiber cable plant infrastructure includes numerous telecommunication rooms (TRs) and network equipment which are deployed at multiple locations throughout DCA, IAD, the Dulles Toll Road Center and the Dulles Metro Rail Offices. The cable plant is owned, upgraded, secured and maintained by one entity (the Authority) to optimize utilization and reduce abandoned plant and dead-ends. Collectively the cable plant infrastructure is used to facilitate ACS voice, video, data, and wiring service offerings. The ACS voice service offering is primarily supported by a network of Avaya PBX’s interconnected by an OC-12 SONET ring on each airport (see Appendix 2). The wiring service offering is primarily supported by an expansive footprint of both single and multi-mode optical fiber cable plant that terminates in multiple telecommunication rooms at both airports and is complemented by a ubiquitous copper distribution network.

The ACS Wiring Infrastructure is comprised of:

- Numerous (16,500+ cable feet) copper point to point deployments entrenched in an Authority controlled conduit and cable system.
- Numerous (12,300+ cable feet) optical fiber point to point deployment entrenched in an Authority controlled conduit and cable system
- Both the optical fiber and copper facilities are terminated in TRs located in numerous locations throughout the airport buildings at DCA and IAD.
- Inside Plant (ISP) distribution facilities (horizontal and vertical risers) to end user locations
Details on the ACS infrastructure, components, quantities and physical locations can be found in Appendices One and Two.

**All offerors must be Authorized Avaya Partners.**

### 03 ACS SERVICE OFFERING

The ACS service offering is comprised of basic local and long distance services, optical fiber connectivity, and associated equipment, features and labor to support such offerings. The service offering and rate structure for the ACS are determined by the Authority and are designed to be competitive in terms of both price and customer service with other telecommunication providers. Appendix 3 summarizes the various ACS services offered, grouped by service type.

### 04 VOLUME STATISTICS

Historical ACS service and other volume statistics can be found in Appendix 4.
**SECTION IV - ONGOING CHANGES TO THE AIRPORTS AUTHORITY ENVIRONMENT**

At the time this document was developed, the following projects were currently underway that may impact the ACS technical environment.

- Enhancements to the Public Safety Communications Center (PSCC) that serves both DCA and IAD Police and Fire Departments
  - Including Public Safety Access Point (PSAP) service at the PSCC which includes a secondary E911 Operations Center or PSAP and server/network redundancy
- Initial planning and pilot testing of transition to Voice over IP Telephony (VOIP)
- Research and identification of more economical options than the current OC-12 circuit to connect the two airports

These projects are listed to provide contractors with a sense of the *dynamic nature* of the Authority environment.
SECTION V - SCOPE OF SERVICES

01 INTRODUCTION

The Contractor shall provide the services necessary to accomplish this Statement of Work and its stated objectives. The services requested are structured into three distinct areas:

- Transition Services
- Base Services
- Supplemental Services

02 TRANSITION SERVICES

The Authority has specified a two-month (60 calendar days) transition period for the Contractor to collect information, coordinate space requirements, implement the staffing plan, prepare the required reports described below, and develop recommendations for improving performance and reporting standards to ensure a successful transition. The Transition Services period of performance will begin on the contract award date and end two months from the date of contract award. The start of the Base Services period will be at the conclusion of the Transition Services period. Transition period costs must be reflected in the initial year Base Services rates.

A Develop and submit transition plan

Within two (2) weeks after contract award, the Contractor shall develop and submit for review by the Contracting Officer’s Technical Representative (COTR) an update of the transition plan included in the Contractor’s proposal. This updated transition plan shall address, at a minimum, the transition activities specified in this Statement of Work. The plan shall include a detailed description of transition activities, including, but not be limited to:

- Evaluating and documenting the Authority’s ACS infrastructure (cable plant, switches, and points of presence)
- Evaluating and documenting the Authority’s ACS administrative, equipment and supplies space allocation
- Reviewing existing Standard Operational Procedures (SOPs)
- Developing recommended modifications to SOPs and additional SOPs
- Developing the methods to collect performance data for each performance standard
- Transition period reporting
- Schedule of activities for each operational or service area
- Approach to ensuring continued system stability during the transition period
- Requirements for Authority-furnished equipment, software, space, telecommunications and services, including staff time
- Precise definition of the support activities to be undertaken

For each Base Services area, the plan should at a minimum identify:

- Timing for the on-site appearance of each Contract position
• Approach to be used for Contractor personnel to learn and understand the Authority’s infrastructure, application systems, procedures, clients (including Authority clients) and practices.
• Length of overlap with existing Contractor personnel in each Base Services area
• Process for a turnover of responsibilities
• Proposed timing of the turnover of responsibilities

B Evaluate and document technical infrastructure

The Contractor shall undertake a comprehensive review and evaluation of the Authority’s telecommunication environment. The purpose of this task is to permit the Contractor to become familiar with the Authority’s environment and collect the information and documentation necessary to ensure successful management, operation, and maintenance of the telecommunication infrastructure and applications. This review shall include an evaluation of:

• Existing system architecture and technical infrastructure including telecommunication equipment and billing/invoicing systems
• Existing business and support processes
• Standards, SOPs and current Authority practices, including the Authority Design Manual
• Equipment and software warranty status
• Orientation and training requirements
• Hardware and software inventories within the Telecommunications Department
• Other property assigned to the Contractor
• Property assigned to individual Contractor personnel

The Contractor shall develop and maintain a record of all Authority property assigned to individual Contractor personnel (see Appendix 6).

The Contractor shall review and confirm the existing Authority telecommunications property inventory. This will establish the telecommunications property baseline.

The Contractor shall comply with all Authority property control procedures and, at the end of the transition period, the Contractor will be held responsible for the property identified in the baseline inventory and for keeping the property records accurate and current.

The Contractor shall provide a deliverable to the COTR that addresses its findings during this task and, identify suggested improvements to systems, procedures and/or documentation accompanied by a plan for implementing the suggested changes and an estimate of the time and resources necessary to implement them.

C Review/Update/Develop procedures manuals

The Contractor shall review current Authority procedures and develop and submit to the COTR a recommended procedures manual for COTR review. The Contractor is expected to draw upon the existing Authority procedures and its own existing documentation to tailor a manual for Authority use that contains SOPs for each Base Services area described in this Statement of Work.

The procedures manuals shall be updated periodically and submitted for Authority approval by the MA-620 Manager.
D Develop methods for collecting performance data for performance standards

Performance standards are stated in Appendix 7. The Contractor may submit recommendations for modifications or additions to the stated performance standards in the Contractor's proposal. The Authority Contracting Officer (CO) and COTR use the performance standards to ensure the quality of the services delivered. During the transition period the Contractor shall submit proposed data collection methods to efficiently and accurately collect performance data for each performance measure. The Contractor shall propose a format for submitting, on an on-going basis, a monthly performance report including performance scores to the COTR and the Vice President, Information and Telecommunications Systems for review.

E Transition period reporting

The Contractor shall submit weekly status reports to the CO and COTR during the transition period specifying progress to date in accomplishing the transition plan, findings, problems encountered and resolutions, planned activities for the upcoming week, and summarizing hours expended by labor category.

03 BASE SERVICES

Base Services are the entire range of technical and administrative support services required on an on-going basis to support the Authority’s telecommunication systems. The Base Services period shall be the twelve months immediately following the two month Transition Services period. The transition period and base services period will constitute the fourteen (14) total months of the initial contract term.

The Authority’s telecommunication systems shall be secure, reliable, responsive, transparent and easily accessible to authorized users at all times. When components fail, trained personnel using consistent procedures should preserve the integrity of data, restore the services and minimize the impact on its users. This shall include escalation procedures and periodic updates to management and executive teams, as appropriate.

All Authority networks shall be operated and maintained in a manner that meets or exceeds the Authority Information Security Standards (see Appendix 9).

The required technical and administrative services that comprise Base Services are described in the following sections. Each section describes the required routine operational functions and functions to be performed as well as the schedule for performance. Performance standards are listed in Appendix 7. At a minimum, the Contractor is required to meet the “Acceptable” performance standards listed.

Base Services are further divided into the following groups:

A. Telecommunication Systems Program Management
B. ACS Site Management
C. ACS Technical Support
D. ACS System Administration & Programming
E. NetPlus Systems Support Services
F. Administrative Support Services

For purposes of Base Services reporting and performance standards, ACS alarms will be categorized as:

- Critical Alarms
- Loss of 10% or more station to station call capability, or
- Loss of greater than 10% of trunking, or
- A DDM-2000 SONET or Avaya CS-1000 failure, or
- Avaya Call Pilot failure, or
- Failure of service on a critical line (see paragraph below)

- Major Alarms
  - CS-1000 Loop failure, or
  - Multiple (3 or more) Trunk card failures, or
  - A DDM-2000 DS-1 card failure, or
  - Inoperative Call Pilot Voice Mail service

- Minor Alarms
  - Indications of degrading system performance that does not interrupt subscriber service

The Authority has defined a number of telephone lines that are critical for Airport Operations and Public Safety. The number of lines at each airport so designated is approximately 15, but this number can vary according to needs at a given time. A failure of any such line or equipment attached to it, including telephone sets, as determined by ACS alarm monitoring or by a call to the ACS Help Desk shall be classified as “Critical.”

A  Telecommunication Systems Program Management

Program Management provides overall program control and reporting services. The Program Manager is the primary point of coordination between all Program activities and the COTR.

The Program Manager is responsible for:

- Overseeing the management of the telecommunication systems for the Authority.
- The contract management structure, and the experience and expertise of the resources allocated to perform the contract services.
- Defining and implementing a complete set of operating methods and procedures that will govern the day to day operations and maintenance of the telecommunication system networks, customer support, alarm priority and response times, external interactions, and related systems. It is expected that these methods and procedures will follow industry standards and best practices and result in the delivery of services at a level consistent with or exceeding the Performance Standards (see Appendix 7) in order to provide the highest quality service to ACS customers and the Authority.
- Describing the methodology by which the Airports Authority’s telecommunication equipment, software, and services will be maintained, inventoried, and improved; the industry standards that apply to that methodology; and how the proposed methodology best aligns with the Airports Authority’s current telecommunication environment.
- Periodically reviewing all technical advances in surveillance, provisioning, and troubleshooting of telecommunication systems and networks.
- Assessing the effectiveness of the current methods and procedures and revise them as necessary, with Authority concurrence.
  - Design and Engineering Guidelines
    - PBX Engineering
    - SONET Engineering
    - VoIP Engineering
    - Fiber Optic Engineering
    - Environmental Controls
    - Cable Plant Engineering
    - Power and Battery Plant Engineering
    - Facility Planning/Optimization
Trouble Response Procedures
- Trouble Ticket Tracking
- Escalation Procedures
- Service Performance Metrics

Service Request Response Procedures
- Service Request Tracking
- Customer Relations Guidelines
- Service Performance Metrics

Billing and Reconciliation Procedures
- Produce monthly charges and invoices
- Respond to requests for invoice explanations
- Process invoice adjustments as approved by the Authority

Third Party Provider Negotiation and Management
- Contractors
- Local Exchange Carriers (LECs)/Inter Exchange Carriers (IXCs)
- Equipment Vendors

Network Performance Reporting
- Definition of Performance Metrics
- Report Format and Intervals

Staff Training

Contract Performance Metrics
- Overseeing the monitoring and maintenance of the telecommunication infrastructure and performance.
  - Network Monitoring
    - 24x7x365 Monitoring
    - Proactive and Reactive Alarms
    - System-Wide and Network Element Views
  - Preventative Maintenance
    - Remote Maintenance Reviews
    - Event Logs
    - Performance Statistics
    - Configuration Settings/Updates
- Providing, scheduling, and installing software and firmware updates and patches to Authority telecommunication switches (see Appendix 1)
- Providing manufacturer defined level 1 and level 2 support to Authority telecommunication switches (see Appendix 1)
- Accessing manufacturer’s level 3 support for Authority telecommunication switches (see Appendix 1), as needed
- Performance of traffic studies on all high capacity circuits to ascertain utilization and recommend changes to effect performance improvements and/or reductions in capacity requirements no less frequently than annually
- Delivering appropriate contract management structure, experience and expertise of the resources allocated to perform the contract services.
- Management of third party service provider relationships (e.g. Public Switched Telephone Network)
- Contributing to plans for future services and improved profitability.
  - Providing recommendations to improve various planning aspects of the ACS including strategic planning, sales and marketing planning, network capacity planning/evolution.
    - Strategic Planning
    - Sales and Marketing (quarterly updates)
      - Revenue Generation Plans
      - Marketing Plans
- Network Capacity Planning (semi-annual updates)
  - PBX/Voicemail
  - SONET (Leased and Owned)
  - LEC/IXC/Transport
  - VoIP
  - Providing recommendations for improvements in Inventory Control and Asset Tracking
- Adherence to Authority Policies for Procurement requisitioning when responding to supplemental construction services task orders. *(See Metropolitan Washington Airport Authority Contracting Manual, APPENDIX C, C.4 COMPETITION GUIDELINES at http://www.mwaa.com/352.htm)*
- Contributing to budget call requests and post budget management.
  - Assists the Manager, MA-620 in the development of the annual budget submission.
  - Assists the Manager, MA-620 adhere to the approved operating budget.
  - Budgeting and planning activities will follow industry best practices and/or documented Authority guidelines where applicable.
- ACS Operating Budget recommendations will include:
  - Pricing Models
  - Revenue Forecasts
  - Suggested areas for possible expense reduction
- Project Management.
  - Management of all Supplemental Services
  - Oversight of subordinate contract staff.
  - Oversight of other contractor staff supporting the ACS and related systems.
  - Performance testing of all contract work.
- Involvement in day to day telecommunications and ACS activities

The Program Manager may reside at either DCA or IAD and shall participate in the day to day operation and delivery of telecommunications services through the ACS and related systems. These activities will generally be supervisory in nature but may involve hands-on engineering or repair activities. Contractor staff shall possess appropriate technical expertise and certifications to successfully execute the proposed Management functions including but not limited to:

- 24x7x365 On-call Rotation for Responding to Network Issues
- Final Recommendations For:
  - Major technical design changes
  - Engineering decisions
  - Contractor Scope of Work and Specifications development for Supplemental Services
  - Bid proposal reviews and recommendations
- Review and Recommendation for:
  - Communications ductbank and conduit placement
  - Optical fiber installation and termination
  - Telecommunication room build outs
  - Other construction/deployment projects
- Participation in Design Meetings
- Supervision of All Contract Staff Personnel Functions
  - Communicate Roles and Responsibilities
  - Performance Reviews
  - Salary and Overtime Tracking
  - Status Reporting
- Liaison to Authority and Tenants
- Identification and Development of New Services to market to existing ACS customers
• Maintain communication with ACS Customer Management and Potential ACS Customer Management.
• Recommendation of statement of work and cost proposals for supplemental services

B Site Management

Site Management provides detailed supervision and control over services delivered at their respective site (DCA, IAD, and the Public Safety Communications Center [PSCC]). Due to proximity, the IAD Site Manager shall also be responsible for Dulles Toll Road and Dulles Rail Partner support.

The Site Managers shall be responsible for:

• Continually striving to improve efficiency of telecommunication services and related operations that translate into lower Authority costs.
• Documenting and reviewing the allocation of contract staff at each site to identify ways to improve staff allocation and performance
• Performance of required functions in a manner that is in the meets or exceeds the performance standards listed in Appendix 7.
• Development of draft scopes of work (SOWs) and draft cost proposals for supplemental services.
• Participating on projects and committees, as assigned, providing technical support and knowledge of ACS systems and locations.
• Ensuring preventive maintenance is performed each month on all appropriate equipment and plant.
• Providing, planning, and installation of patches and upgrades to all ACS components in a manner that does not invalidate manufacturer provided warranties and maintenance support.
• Coordinating access control responsibilities for physical access to communication closets containing MA-620 equipment with other Airports Authority Departments, as required.
• Managing and documenting administrator access to all Airports Authority telecommunication devices.
• Monitoring and maintenance of the ACS infrastructure and performance.
  o On Site Maintenance Reviews
    ▪ Event Logs
    ▪ Performance Statistics
    ▪ Configuration Settings
  o On Site Maintenance Verification and Adjustments
    ▪ Environmental Controls
    ▪ Card Seating
    ▪ Power System Levels
    ▪ Uninterruptable Power Supplies (UPS)
    ▪ Cable Security
    ▪ Site Cleanliness
  o Reporting and Escalation
    ▪ Log and Report Maintenance Findings
    ▪ Initiate Remedial Maintenance Procedures
• Remedial Maintenance
  o Response Triggers
    ▪ Preventative Maintenance Procedures
    ▪ Monitors and Alarms
    ▪ End User Trouble Reports
  o Response Intervals per Performance Standards (see Appendix 7)
    ▪ Minor
- Major
- Critical
  - Repair Time and Escalation
    - Conform to Specified MTTR (Mean Time To Repair)
    - Follow Tier 3/Vendor Escalation Procedures
  - Monitor MTBF (Mean Time Between Failure) experience vs. Manufacturer published figures to identify underperforming equipment.
- Engineering and design of copper voice and data wiring infrastructure and the optical fiber infrastructure
  - The specific network elements and engineering responsibilities of the Contract Staff include, but are not limited to:
    - CS-1000 Release 7.0 Software and Optical Fiber PBX Remote Sites
      - Port, Trunk and Network Capacity Planning
      - P.01 Grade of Service Engineering
      - Network Expansions (peripheral and super-loops)
      - Moves/Adds/Changes
      - PRI (Primary Rate Interface) and Trunk Routing
      - Handset Configuration
    - Call Pilot and United Airlines Centigram Voicemail
      - Mailbox Capacity Planning and Expansion
      - PBX Interconnect Engineering
    - Lucent SONET ADM (Add/Drop Multiplexor)
      - Aggregate and Circuit Capacity Planning
      - Circuit Adds/Changes
      - Protection and Diversity Engineering
    - LEC/IXC Facilities
      - PRI and Circuit Provisioning
      - Customer Capacity Planning
    - Fiber Optic Cable
      - OTDR (Optical Time Domain Reflectometer) Measurements
      - Attenuation and Distance Planning
      - Splice Engineering
      - Route Diversity
      - Fiber Terminations Splice Case Integrity
      - Splice Diversity (Mechanical vs. Fusion)
    - Power and Battery
      - Rectifier Sizing
      - Battery Plant Sizing (UPS)
      - BDFB (Battery Distribution Fuse Board) Sizing and Placement
      - Busy Hour Reserve Limits
- End User training (level 3)
- Contract Staff Training
- Test and turn up of intra and inter airport circuits
- Records maintenance for as-built drawings, OSP/ISP (Outside Plant/Inside Plant), and network configurations
- Supply chain management for telecommunications equipment to ensure optimized inventory levels and availability of critical spares
- Identification and tracking of assets as required by this contract and Authority inventory policies
- Site Budgeting and Planning
- Defining and maintaining operational methods and procedures
• Tactical involvement in day to day telecommunications activities at DCA and IAD
• Maintain communication with telecommunications Customer Management
• Responsible for the actual hands-on operation and maintenance of the ACS network and support of the ACS user community. This includes:
  o Development of customer orders to expand ACS usage
  o Engineering of orders (e.g. Customer orders, maintenance orders, end-of-life replacement orders)
  o Installation and repair
  o Troubleshooting
  o Help Desk third tier support,
  o Tenant billing, and work order management.
• Responses to Service Requests, including:
  o New Service Requests
  o Add/Move/Change Requests
  o Installation of Analog/Digital Handsets
  o Repairs/Replacements for defective equipment
  o Outside Plant (OSP)
    ▪ Pull Cable through Authority controlled ductbank and conduits
    ▪ Pull and Splice Cable at Building Entrance Facilities
    ▪ Pull Cable Intra-Building and Intra-Room (Authority cable tray)
    ▪ Labeling and Documentation
  o Splicing, Termination and Cross Connects
    ▪ Manhole/Handhole
    ▪ Optical Fiber Distribution Panels (LIUs)
    ▪ Copper Distribution Frames
  o Inside Plant (ISP)
    ▪ Deployment and Maintenance of In-Building Wiring
    ▪ Termination and Jack Installation
    ▪ Labeling and Documentation
• Maintain “As-Built” documentation of the ACS for all work performed
• Customer relations
  o Professional Interaction with Customers
  o Perform Trouble Diagnoses
  o Communicate Repair Expectations
  o Engage in Preventative Training
  o Requirements Gathering
  o Trouble Diagnoses
  o Status Updates
  o Training
• Coordination with other service providers
  o LEC/IXC Service Orders
  o Tier 1 LEC/IXC Troubleshooting
  o Inspects and evaluates performance of other contractors whose work impacts the ACS
    ▪ Provides a report to the Authority if such performance is problematic

C **ACS Technical Support**

Technical Support provides for the ongoing plant management and maintenance and delivery of services to ACS customers. These contract personnel support the Site Managers in the execution of their duties as assigned. Specific tasks include, but are not limited to:

- User station installations, upgrades and repairs of the copper wiring infrastructure
- Preventive and remedial maintenance, system monitoring and trouble resolution
- End User training (level 2)
- P.01 Grade of Service assurance
- Maintenance of industry standards and best practices for equipment and processes
- Inventory and asset tracking of ACS equipment, cable and facilities
- On-Call and emergency repairs to ACS equipment, facilities and outside plant that does not invalidate manufacturer provided warranties and maintenance support.
- Responsible for the actual hands-on operation and maintenance of the ACS network and support of the ACS user community. This includes:
  - Respectful interaction with ACS customers
  - Engineering of orders (e.g. Customer orders, maintenance orders, end-of-life replacement orders)
  - Installation and repair
  - Troubleshooting
  - Help Desk second tier support,
- Responding to Service Requests, including:
  - New Service Requests
  - Add/Move/Change Requests
  - Installation of Analog/Digital Handsets
  - Outside Plant (OSP)
    - Pull Cable Through Conduit
    - Pull and Split Cable at Building Entrance Facilities
    - Pull Cable Intra-Building and Intra-Room
    - Labeling and Documentation
  - Splicing, Termination and Cross Connects
    - Manhole/Handhole
    - Optical Fiber Distribution Panels
    - Copper Distribution Frames
  - Inside Plant (ISP)
    - Deployment and Maintenance of In-Building Wiring
    - Termination and Jack Installation
    - Labeling and Documentation
- Responding to Trouble Resolution tasks such as:
  - Response Triggers
  - Preventative Maintenance Procedures
  - Monitors and Alarms
  - End User Trouble Reports
  - Remote Support
    - Gain Remote Access
    - Utilize Equipment Specific Command Line Interface
    - Utilize Equipment Specific Diagnostic Methods
  - On Site Support
    - Gain Craft/Management Access to various areas of the airport
    - Utilize Equipment Specific LED Readings
    - Utilize Equipment Specified Diagnostic Methods
    - Employ Test Equipment and Methodologies
      - T-BERD
      - OTDR
      - Loopback Tests
      - Battery Tester
      - Server/Network Surveillance Systems
• Maintain “As-Built” documentation of the ACS for all work performed
• Customer relations
  o Professional Interaction with Customers
  o Perform Trouble Diagnoses
  o Communicate Repair Expectations
  o Engage in Preventative Training
  o End User Training (level 2)
  o Status Updates

D ACS Systems Administration & Programming

The ACS Systems Administrator is responsible for all ACS Systems Administration & Programming support tasks focused on ACS operations including but not limited to:

• CS-1000 PBX and Voicemail Systems
  o Move/Add/Change Programming
  o Mailbox Creation and Software Maintenance
  o Coordinated Dialing Plans
  o Trunk Routes/Translations
• Records Maintenance
  o Direct In Dial Telephone Number and Port Utilization Tracking
  o Optical Fiber Cable Plant
  o Copper Cable Plant
  o Other technical records
  o Traffic Studies
• ACS software upgrade/patch testing and installation
• Coordination with other contract service providers and Authority staff as needed

E NetPlus Systems Support Services

The Authority maintains a contract with Ventraq, Inc., the manufacturers of NetPlus, which covers basic computer network (see Appendix 2) maintenance. This includes both hardware and software maintenance services.

The contractor shall be responsible for NetPlus Systems Support Services including the operation and data maintenance of the NetPlus program, execution of backups (and when necessary restorations), and maintenance of virus protection updates. This system supports both an ACS help desk/work order function as well as the billing function for the ACS program.

1 Help Desk/Work Order Operation

The ACS Help Desk/Work Order Desk provides a single point of contact for all ACS customers who wish to communication with ACS staff. They will document all incoming communications, triage, resolve or assign to other ACS staff for resolution. The responsibilities of this group include but are not limited to:

• ACS Help Desk management for work orders, service requests, and trouble tickets
  • ACS Work Order generation, updating, monitoring, reporting, and close out
    ▪ Help Desk Interface
    ▪ Tier-1 Support and Information Gathering
    ▪ Dispatch to Technical Staff
    ▪ Tracking and Reporting
- Resource Allocation and Usage Tracking
- Work Order Status Documentation
  - Entering hours, materials consumed, and notes from completed work orders into the NetPlus System
- Resolution Documentation
- Work Order Usage and Performance Reports
  - Man Hours/Trouble Resolution
  - Time in Queue
  - Time to Close
- Service Request generation, updating, monitoring, reporting, and close out
  - Interface with System Design Specialists
  - Track Progress and Update Customer
  - Report on Service Request Activity
  - Service Request Usage and Performance Reports
    - Man Hours
    - Time in Queue
    - Time to Close
- Trouble Tickets generation, updating, monitoring, reporting, and close out
  - Interface with System Design Specialists and/or Technical Staff
  - Track Progress and Update Customer
  - Initiate Escalations per Documented Procedures
  - Trouble Ticket Usage and Performance Reports
    - Man Hours
    - Time in Queue
    - Time to Close
- End User training (level 1)
- Customer relations
  - Professional Interaction with Customers
  - Perform Trouble Diagnoses
  - Communicate Repair Expectations
  - Engage in Preventative Training with Customers over the phone
- Call Center Functionality including:
  - Performance Reporting
    - Report on Help Desk Activity
    - Report on Help Desk Performance
    - Report on remote Call Center Activity
    - Report on remote Call Center Performance

2 Remote Call Center Operations

Outside normal business hours (see Appendix 5) calls to the ACS Help Desk are forwarded to the Contractor’s Remote Call Center Operations, where details of the call shall be:

- Recorded
- Relayed to the appropriate on-call technician
- Faxed to the Help Desk for entry into NetPlus on the next business day

3 Invoicing and Collection Operations

The Billing/Account Specialist is responsible for all invoicing and collection operations for the ACS. The Authority utilizes the NetPlus system network (see Appendix 2) to prepare invoices.
Invoices include ACS usage data as well as charges for Work Orders, as appropriate. Each month, invoices are prepared and printed, sorted, stuffed in envelopes, and mailed.

Invoice data is downloaded and converted into an electronic spreadsheet format for transfer to the Authority Accounting Department. The invoice data is then uploaded for entry into the Authority Financial Systems. All incoming remittances are the responsibility of the Authority Accounting Department and are posted into the Authority Financial Systems.

Each month, the Billing/Account Specialist runs a report from the Authority’s Propworks system that lists payments and credits for telecommunication accounts. This report is reviewed manually and payments and credits identified are entered into the NetPlus system by the Billing/Account Specialist. The Billing/Account Specialist is responsible for all collection activities for delinquent telecommunication accounts.

Activities performed in this area include:

- ACS Network polling, data mediation and invoice generation
- Invoice preparation and mailing
- Response to Customer and/or Authority Billing Inquiries
- Transferring billing records to the Authority Oracle EBS Accounting System
- Billing function that includes:
  - Customer Record Maintenance
    - Contact Details
    - Services and Rates
    - Billing History
  - Polling and Mediation
    - Gather Usage Based Data
    - Perform Raw Data Translations
  - Invoice Generation and Distribution
    - Operate Invoicing Software Platform
    - Create and Distribute Invoices at Regular Intervals
- Collection function that includes:
  - Preparation of aging reports
  - Follow up calls and letters

4 NetPlus Technical Support

The Authority maintains a contract with Ventraq, Inc., the manufacturers of NetPlus, which covers basic computer network (see Appendix 2) maintenance. This includes both hardware and software maintenance services. However, the Contractor shall perform the following tasks:

- Performance of daily and weekly server backup operations
- Performance of server restorations, as needed
- Maintenance of off-site backup storage
- Correction of erroneous entries into the system, as needed
  Note: This requires basic SQL+ programming capabilities.
F  **Administrative Support Services**

1  **General Administrative Support**

The Contractor shall provide qualified staff to perform all ongoing administrative tasks in support of the Authority Telecommunication Systems Department and the Telecommunication Systems Support Services contract. The Contractor is expected to make day-to-day decisions concerning administrative tasks within guidelines provided by the Manager of MA-620. The Authority’s environment is dynamic, and all guidelines will not be predetermined. The support will include, but not be limited to:

- **Departmental Records Maintenance**
  - Maintain all Authority Telecommunication Systems Department records in a manner directed or approved by the COTR
  - Establish and maintain a system to archive or destroy records as directed by the COTR
  - Maintain library of SOPs using the latest industry standards, Directives, Polices and other direction or guidance either established by Authority Telecommunication Systems Department management or by other authorized areas within the Airports Authority
  - Maintain statistics on Departmental and Contract activity including the preparation of regular reports documenting such activity for management review. This will include but is not limited to Monthly Revenue Reports and Circuit Increase/Decrease Activity Reports.
  - Maintain a file of Non-Disclosure Agreements signed by each contract employee assigned to work with MA-620.

- **Documentation Support**
  - Document Authority Telecommunication Systems Department activities as directed by the COTR
  - Draft material to be used for training and/or orientation (both internal and customer).
  - Assist in documenting changes in the Authority’s ACS environment as they occur.
  - Technical Library Support - Organize and maintain a library of technical references and instruction having to do with the Airports ACS
  - Draft a monthly Telecommunication Systems Support Services Project Update e-mail for COTR approval and distribution. This will include a “Hot Spot” report with Cable Plant Topology highlighting where capacity is in jeopardy of exhaustion.
  - Maintain archive files of publications, available on the Authority’s intranet for reference
  - Develop and maintain SOPs for all areas of ACS activity
    - Gather information on a given process or activity and consolidate it in an easily understandable and executable form
    - Format and generate draft of an SOP for executing the process or activity and provide to Telecommunication Systems Department management (or designated representative) for review and recommended revision
• Implement recommended revisions and provide Final Draft of the SOP for or Telecommunication Systems Department management (or designated representative) approval and release

• Maintain telecommunication standards documentation
  • Document all established Authority telecommunication standards as designated and required
  • Make those Standards available to all applicable personnel and ensure the Standards are kept current and documented on the Authority Intranet
  • Circulate Standards as necessary on a periodic basis for review and revision
  • Have the MA-620 Manager (or designated representative) review the Standards as required to ensure their appropriateness

• Maintain a list of relevant Authority Standards
  • Develop a list of relevant Authority Standards as designated and required
  • Make the list available to all applicable personnel and ensure the list is kept current and documented on the Authority Intranet
  • Circulate the list as necessary on a periodic basis for review and revision
  • Have the MA-620 Manager (or designated representative) review the list as required to ensure its appropriateness and completeness

• Develop User Manuals and User Guides as required

• Requisition processing
  • Assist the Manager, MA-620 in the acquisition of materials and services.
  • Research and recommend products
  • Advise of product availability
  • Prepare the appropriate requisitions
  • Log and track requisitions
  • Assist the Authority’s various Procurement offices as required,
  • Take receipt of material ordered
  • Ensure property is properly registered and tracked, as required.

• Inventory Tracking
  • Assist the MA-620 Manager and Authority Telecommunication Systems Department personnel and their Property Sub-Custodian(s) in tracking the location and disposition of all accountable property assigned to the Authority Telecommunication Systems Department
  • Ensure procured items are recorded, as required, on inventory
  • Report on excess property no longer useful or required, at the COTR/Property Custodian’s discretion, to the appropriate office and coordinate its removal
  • Assist the various Authority Property Offices with questions or issues concerning Authority Telecommunication Systems Department property
  • Maintain inventory records of Authority property assigned to Contractor personnel

• Software License Maintenance
  • Ensure software in use by the ACS is properly licensed, supported and renewed as required and directed by the COTR
  • Maintain records on the number and types of licenses owned by the Authority Telecommunication Systems Department and it’s support status and requirements
• Other Administrative Processes
  • Coordinate annual ID badge renewal.
  • Coordinate annual parking permit renewal process
  • Coordinate other security clearance requirements, as needed
  • Coordinate Departmental meetings
  • Executive Support
  • Provide clerical and administrative support for the Authority Telecommunication Systems Department

• Related duties as assigned.

04 SUPPLEMENTAL SERVICES

The Airports Authority’s telecommunications workload is variable and unexpected demands sometimes arise. The Contractor may be assigned, through contract modification, supplemental support tasks that are necessary to fulfill the mission of the Airports Authority. Supplemental services will be administered through a set of task orders.

Supplemental Services include:

A. Supplemental Parts Services
B. Supplemental Construction Services, which include Supervision and Quality Assurance
C. Supplemental Consulting Services

The Contractor can add or delete subcontractors only with advance prior approval of the Authority CO. The Authority reserves the right to use vendors other than the Contractor for supplemental telecommunication related services.

A Supplemental Parts Services

The Authority ACS is comprised of a large number of diverse components. While the Authority strives to maintain an adequate inventory of spare parts, there are times when there is a need for an emergency acquisition of a part or parts.

In such occurs, the contractor may be directed to acquire the needed part(s) on a cost plus Contractor markup basis. Products provided must be obtained through processes that comply with the Authority’s Procurement Policies. (See Metropolitan Washington Airport Authority Contracting Manual, APPENDIX C, C.4 COMPETITION GUIDELINES at http://www.mwaa.com/352.htm)

B Supplemental Construction Services

The Contractor may be required to provide services in connection with construction affecting the ACS. The work to be performed will be of a temporary nature, and may require a diversity of skills suitable to a variety of telecommunications functions, including but not limited to:

• Large installations or equipment moves
• Construction projects including the laying of conduit and cable

The work required throughout the duration of any task will vary with each requirement depending upon the scope of the work to be performed. Specific work to be performed will be included in a statement of work for the individual requirement.
The Contractor will be required to submit a specific technical and price proposal for all Airports Authority requests for Supplemental Construction Support Services. The proposals will include:

- Proposed prices with sufficient breakdown to allow a thorough analysis, including indirect and direct rates
- Technical approach to performance of services
- Personnel qualifications
- Subcontractor mark-ups

The Contractor will be responsible for providing supervision and Quality Assurance (i.e. testing) on all supplemental construction activities.

Products and services provided must be obtained through processes that comply with the Authority’s Procurement Policies on competition. (See Metropolitan Washington Airport Authority Contracting Manual, APPENDIX C, C.4 COMPETITION GUIDELINES at http://www.mwaa.com/352.htm)

### C Supplemental Consulting Services

The Contractor may be requested to provide supplemental consulting services of a temporary nature, relating to a variety of telecommunication functions, including but not limited to:

- Investigation of new technologies
- Integration of new technologies
- ACS marketing and/or promotional projects

The work required throughout the duration of any task will vary with each requirement depending upon the scope of the work to be performed. Specific work to be performed will be included in a statement of work for the individual requirement.

The Contractor will be required to submit a specific technical and price proposal for all Airports Authority requests for Supplemental Consulting Support Services. The proposals will include:

- Proposed Work Program including labor categories and hours for each activity
- Proposed Prices by Labor Category
- Technical approach to performance of services
- Personnel qualifications

### 05 CONTRACT ADMINISTRATION AND REPORTING REQUIREMENTS

#### A Contract Administration

1 **Contractor- provided resources**

The Contractor is expected to provide personnel resources for this contract including cellular phones and pagers for Contractor personnel who spend significant time away from their assigned base location (e.g. Site Managers and Technicians) or who may reasonably be expected to support emergency situations after hours or on weekends and holidays. The Contractor will also provide normal tools of the trade for contract staff assigned to the Authority including:
• All hand tools, test equipment and associated equipment needed to support the copper, optical fiber and other systems that the ACS supports. This can include radio, media panel and CATV equipment.
• Manhole lifter and confined space equipment
• Cell phones for both staff and technicians

The Contractor will also provide services of a 24x7x365 ACS After-Hours Monitoring Center.

The contractor shall provide vehicles necessary for the transport of personnel while at work. Appendices Eleven and Twelve provide information on the procedures followed to certify a vehicle for access to the Air Operations Area (AOA) at DCA and IAD respectively.

The Contractor is not expected to provide the Authority with any equipment, tools, furniture, office supplies, or software under this contract, except through supplemental support services.

2 Required hours of operation

Normal hours of operation currently required are documented in Appendix 5. Holidays will be treated in the same manner as Sundays.

ACS users are directed to call the ACS Help Desk with all service issues. During hours that the ACS Help Desk is not staffed, the Contractor shall provide appropriate telephone and/or beeper numbers to the Remote Call Center for notification purposes. The Contractor shall return telephone messages or pages within one hour during off-hours. The Contractor shall be required to arrive on-site within four hours notice, although the Contractor may propose a shorter period.

3 Other support contracts

The Contractor shall coordinate support and maintenance activities with other Authority telecommunication contractors providing onsite support and maintenance that can affect the delivery of telecommunication services. This includes but is not limited to:

• Verizon
• Ventraq, Inc.

At the completion of other support contractor’s work, the Contractor shall attempt to confirm the return to normal service levels and notify the Manager, MA-620 of such findings. This contract shall involve coordination but not supervision of other support contractors.

The Contractor shall review applicable existing Airports Authority support contracts as they come up for renewal. The Contractor shall evaluate requirements and existing support activities and make recommendations, where appropriate, to achieve optimum system performance and minimum cost through the support contract.

The Contractor shall retain full responsibility for its subcontractors’ performance (both base services subcontractors and supplemental support services subcontractors).

4 Location of performance

The Contractor shall provide the services identified in this SOW to all Airports Authority locations. Current locations are Washington Dulles International Airport, Ronald Reagan
Washington National Airport, the Dulles Toll Road offices at the Spring Hill Road exit and the Dulles Rail Project offices at 1593 Spring Hill Road, Suite 300, Vienna, VA 22182. While locations may be added or removed during the term of the contract, there are no known plans to do so in the immediate future.

5 **Airports Authority provided resources**

The Airports Authority shall provide all network and workstation hardware and software required by the ACS and NetPlus networks. All procurements shall be made by the Authority’s CO, with recommendation and technical assistance from the COTR. The Airports Authority intends to retain ownership and leases of all hardware, software, and data. The following resources will be provided by the Airports Authority:

- Adequate work space including furniture
- Telephone service with voice mail
- Access to the ACS and NetPlus networks
- Access to NetPlus software, network management software and other support software as described in this SOW
- Internet access (required for software patches and related items)
- Workstations for on-site Contractor personnel working in the Telecommunications Department office area and Contractor personnel working on the NetPlus network
- Day-to-day operating supplies for on-site Contractor personnel working in the Telecommunications Department office area only
- Parking for employees will be provided as indicated below:
  - **Ronald Reagan Washington National Airport.** Parking available in employee parking lot for $95.00/year.
  - **Washington Dulles International Airport.** Parking available in employee parking lot for $350.00/year.
  - Note: Parking fees are adjusted each year in October. The parking fees cover the period October 1 through September 30. The fees specified above will remain in effect until September 30, 2012.
- Identification badges will be provided as indicated below:
  - **Ronald Reagan Washington National Airport.** ID Badges are issued for $0/year.
  - **Washington Dulles International Airport.** ID Badges are issued for $0/year.
  - There is an escalating fee to replace a lost badge. The first time fee is $50.
  - Note: All identification badge fees may be adjusted from time to time by the Authority. ID Badges expire on the last day of the birth month of the holder (or the contract termination month). In addition to the annual badge fee, there is a one-time fee of $27 for a Fingerprint based Criminal History Records Check (includes fingerprinting) and $11 for a one time only Security Threat Assessment.
In order to receive an Airport issued airport operations area or a sterile area identification Badge, each person must be fingerprinted at their respective airport (National or Dulles Airport Pass & ID Office); successfully complete an FBI criminal history records check (CHRC) and; pass a TSA Security Threat Assessment (STA). Additional fingerprinting (no more than one year old) is required and conducted by Customs and Border Control (CBP) for those who need access to customs areas and to obtain a U.S. Customs seal on the identification badge.

The Contractor will be responsible for all Airports Authority property issued during the contract term. A property inventory of all issued assets shall be conducted on the first and last day of the contract term to determine Contractor accountability of Airports Authority property.

The Contractor will be responsible for conducting an inventory of Airports Authority issued property each quarter including reconciliation to the prior inventory.

The Airports Authority will conduct unscheduled property inventories during the Contract term.

B Reporting requirements

1 Monthly status reports

After the Transition Services period is completed, the Contractor will submit a monthly report to the Authority CO and COTR that describes the overall status of the contract and the Airports Authority ACS related systems. This report will follow a format agreed to by the Airports Authority and the Contractor. The format of the report is expected to change from time to time.

Initially, the report is expected to contain the following sections:

- Overview
  - Accomplishments, Planned Activities, Summary of Performance Metrics vs. Performance Standards, and Issues
  - LDBE (Local Disadvantaged Business Program) tracking
  - Detailed tracking of performance metrics and other Airports Authority identified metrics
- Personnel
  - A list of all contract Base Services positions and assigned personnel
- Usage Statistics/Measures
  - Traffic studies, including fiber remotes
- Base Services
  - Cost summary
    - Base Servicers Cost Summary
      - Delivered Cost (sum of the actual hours for the month multiplied by rate for each position)
      - Invoiced Cost
      - Cumulative Difference
- Telecommunication Systems Program Management Performance
- Site Management Performance
- ACS Technical Support Performance
- ACS Systems Support Performance
- ACS Systems Administration & Programming Performance
- NetPlus Systems Support Services Performance
  - Help Desk/Work Order Support Services Performance
  - Billing System Support Performance
  - NetPlus Network & System Administration Performance
- Administrative Support Services Performance
- Supplemental Services
- Project Summaries

Other periodic reporting (e.g. daily, weekly, monthly) shall be provided as requested.

2 Program management reviews and planning meetings

The Contractor shall coordinate monthly Program Management Reviews with the COTR and the Vice President, Information and Telecommunication Systems. The purpose of these reviews will be to review the monthly status report and discuss high-level management issues and plans with Contractor management personnel. The Contractor's Program Manager and appropriate management team personnel will be present at these reviews. The Contractor shall maintain and publish minutes of these meetings.
SECTION VI - KEY PERSONNEL

Certain personnel proposed by the Contractor will be considered for the purposes of award and contract administration as “key personnel.” The Contractor shall use its best efforts to notify the Authority CO and COTR 30 days prior to reassigning any key personnel during the life of the contract. The Authority CO reserves the right to approve replacement of key personnel.
## SECTION VII - SUMMARY OF CONTRACT DELIVERABLES

### 01 TRANSITION SERVICES PERIOD

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Transition Services</td>
<td>Date of Award + 2 months</td>
</tr>
<tr>
<td>Updated Transition Plan with Gantt Chart</td>
<td>Two weeks after contract award</td>
</tr>
<tr>
<td>Evaluation of technical infrastructure</td>
<td>As per transition plan</td>
</tr>
<tr>
<td>Update to property inventory</td>
<td>As per transition plan</td>
</tr>
<tr>
<td>Standard Operational Procedures Manual</td>
<td>As per transition plan</td>
</tr>
<tr>
<td>Performance standards data collection methods</td>
<td>As per transition plan</td>
</tr>
<tr>
<td>Weekly transition status reports</td>
<td>Weekly during transition period</td>
</tr>
</tbody>
</table>

### 02 BASE SERVICES PERIOD

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Base Services and Performance</td>
<td>12 months, starting 2 months + 1 day after award</td>
</tr>
<tr>
<td>User Satisfaction Survey - 10% of trouble calls</td>
<td>Weekly</td>
</tr>
<tr>
<td>Provide support services identified in the RFP</td>
<td>12 months, starting 2 months + 1 day after award</td>
</tr>
<tr>
<td>Inventory of Airports Authority issued property</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Status report</td>
<td>Monthly</td>
</tr>
<tr>
<td>Program Management Reviews</td>
<td>Monthly</td>
</tr>
<tr>
<td>Minutes of Program Management Reviews</td>
<td>Monthly</td>
</tr>
</tbody>
</table>
APPENDIX 1

EXISTING TELECOMMUNICATIONS INFRASTRUCTURE
### Active Components

<table>
<thead>
<tr>
<th>DCA</th>
<th>IAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>• One (1) Avaya CS-1000E Private Branch Exchange (PBX) deployed at DCA</td>
<td>• One (1) Avaya CS-1000E Private Branch Exchange (PBX) deployed at IAD</td>
</tr>
<tr>
<td>• One (1) Avaya CS-1000M Private Branch Exchange (PBX) deployed at DCA</td>
<td>• Three (3) Avaya CS-1000M Private Branch Exchange (PBX) deployed at IAD</td>
</tr>
<tr>
<td>• Two (2) Site Event Buffers (SEB or smart modems) for remote access to PBX switches</td>
<td>• Seven (7) Avaya Fiber Remote switches deployed at strategic IAD locations</td>
</tr>
<tr>
<td>• Two (2) Station Message Detail Recording (SMDR) Buffer Servers to collect raw call data from SMDR port of PBX switches</td>
<td>• One (1) Avaya Voice Mail System</td>
</tr>
<tr>
<td>• One (1) Avaya Voice Mail System</td>
<td>• Four (4) SEBs for remote access to PBX switches</td>
</tr>
<tr>
<td>• Four (4) Lucent Synchronous Optical Network (SONET) Add Drop Multiplexers (ADMs)</td>
<td>• Four (4) SMDR Buffer Servers</td>
</tr>
<tr>
<td>• Four (4) Newbridge T-Carrier Level 1 (T1) Channel Banks</td>
<td>• One (1) Centigram Voice Mail System</td>
</tr>
<tr>
<td>• One (1) CrashNet Alert System</td>
<td>• Five (5) Lucent SONET ADMs</td>
</tr>
<tr>
<td>• One (1) CrashNet Alert System</td>
<td>• Five (5) Newbridge T1 Channel Banks</td>
</tr>
<tr>
<td>• One (1) E911 Call Center PSCC Option 61 switch, server and reader board</td>
<td>• One (1) FFET Phone System</td>
</tr>
</tbody>
</table>

### ACS Passive and Support Components

<table>
<thead>
<tr>
<th>Passive Components</th>
<th>Support Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Seicor Fiber Distribution Panels (FDP)</td>
<td>• Absolyte Gel Cell Battery Units</td>
</tr>
<tr>
<td>• Copper Distribution Frames</td>
<td>• Avaya Rectifiers</td>
</tr>
<tr>
<td>• ADC Patch Panels</td>
<td>• Conduit and Cable Management Systems</td>
</tr>
<tr>
<td>• Avaya Digital and Analog Handsets</td>
<td>• ACE*Comm NetPlus Management System</td>
</tr>
</tbody>
</table>
APPENDIX 2

NETWORK DIAGRAMS
PollCat dials into NetPlus to report telephone usage for billing.
NetPlus automatically FTP Automatic Location Information (ALI) to PCSS's Vesta
APPENDIX 3

ACS SERVICES
<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Plans</td>
<td>Local Calls</td>
<td>Per call, regardless of duration</td>
</tr>
<tr>
<td></td>
<td>Local Extended Calls</td>
<td>Cost varies depending on the calling range</td>
</tr>
<tr>
<td></td>
<td>Basic Long Distance</td>
<td>Flat charge for first minute, each tenth of a minute thereafter</td>
</tr>
<tr>
<td></td>
<td>International Long Distance</td>
<td>Cost varies by country</td>
</tr>
<tr>
<td>Fiber</td>
<td>Fiber Optic Cable Segment</td>
<td>Fiber Optic Charges per Segment per Strand</td>
</tr>
<tr>
<td></td>
<td>IAD Fiber Ckt - B con. To D con.</td>
<td>Intra Building Fiber Circuit - B concourse to D concourse</td>
</tr>
<tr>
<td></td>
<td>Land Side Fiber Ckt</td>
<td>Land Side Fiber Circuit - per 100 ft.</td>
</tr>
<tr>
<td></td>
<td>IAD Fiber Ckt - Main to B con.</td>
<td>Intra Building Fiber Circuit - Main to B Concourse</td>
</tr>
<tr>
<td></td>
<td>IAD Fiber Ckt - Main to D con.</td>
<td>Intra Building Fiber Circuit - Main to D Concourse</td>
</tr>
<tr>
<td>Handsets</td>
<td>Digital Data Set (M2008)</td>
<td>Digital/data set, type m2008 w/data</td>
</tr>
<tr>
<td></td>
<td>Sngl Line Set, No Dial, Red</td>
<td>Telephone Set, Single Line, No Dial, Red</td>
</tr>
<tr>
<td></td>
<td>Outdoor Telephone Set</td>
<td>Outdoor Telephone Set (Gai-tronics - 256 CSK)</td>
</tr>
<tr>
<td></td>
<td>Single Line Set, 2500</td>
<td>Telephone Set Single Line 2500</td>
</tr>
<tr>
<td></td>
<td>Sngl Line DTMF Wall Set, 2554</td>
<td>Telephone Set Single Line DTMF Wall</td>
</tr>
<tr>
<td></td>
<td>TP Sngl Line Elevator</td>
<td>Telephone Single Line Elevator</td>
</tr>
<tr>
<td></td>
<td>TTY Analog Phone Set</td>
<td>Analog Telephone Set w/ TTY Capabilities</td>
</tr>
<tr>
<td></td>
<td>Digital 6 BTN (M2006 Basic)</td>
<td>Telephone Digital 6 Button M2006 Basic</td>
</tr>
<tr>
<td></td>
<td>Digital 8 BTN (M2008 Basic)</td>
<td>Telephone Digital 8 Button M2008 Basic</td>
</tr>
<tr>
<td></td>
<td>Digital 8 BTN w/ DSP (M2008)</td>
<td>Telephone Digital 8 Button w/ Display (M2008)</td>
</tr>
<tr>
<td></td>
<td>Digital 8 BTN w/ HF &amp; DSP (M2008)</td>
<td>Telephone Digital 8 Button w/ Handsfree &amp; Display (M2008)</td>
</tr>
<tr>
<td></td>
<td>Digital 16 BTN (M2616)</td>
<td>Telephone Digital 16 Button M2616</td>
</tr>
<tr>
<td></td>
<td>Dig 16 BTN w/ HF &amp; DSP (M2616)</td>
<td>Telephone Digital 16 Button w/ Speaker (M2616)</td>
</tr>
<tr>
<td></td>
<td>Digital NORSTAR (M7310)</td>
<td>NORSTAR Digital Set M7310</td>
</tr>
<tr>
<td></td>
<td>Digital NORSTAR (M7324)</td>
<td>NORSTAR Digital Set M7324</td>
</tr>
<tr>
<td></td>
<td>Digital 22 BTN Add-On Module</td>
<td>Telephone Digital 22 Button Add-On Module</td>
</tr>
<tr>
<td></td>
<td>Analog Feature Set (M8009)</td>
<td>Telephone Analog Feature Set M8009</td>
</tr>
<tr>
<td></td>
<td>Analog Feature Set (M8314)</td>
<td>Telephone Analog Feature Set M8314</td>
</tr>
<tr>
<td></td>
<td>Courtesy Set/TT Dial (Viking)</td>
<td>Ring-Down Telephone Set w/ Touch Tone Dial (Viking K1900-8)</td>
</tr>
<tr>
<td></td>
<td>Analog Set (AT&amp;T 210)</td>
<td>Analog Set (AT&amp;T 210)</td>
</tr>
<tr>
<td>Labor</td>
<td>Install &amp; Svc Ord Labor, 1/4 Hour</td>
<td>Installation and Service Order Labor, 1/4 Hour</td>
</tr>
<tr>
<td></td>
<td>Install &amp; Svc Ord Labor, Overtime</td>
<td>Installation and Service Order Labor, Overtime</td>
</tr>
<tr>
<td>Lines</td>
<td>ACS Digital Port</td>
<td>Digital Port, ACS Digital Phones</td>
</tr>
<tr>
<td></td>
<td>ACS Analog Port w/ ACS Set</td>
<td>Analog Port, ACS Analog Sets</td>
</tr>
<tr>
<td></td>
<td>ACS Analog Port w/o Equipment</td>
<td>Analog Port, Without Equipment</td>
</tr>
<tr>
<td></td>
<td>FAX or Modem Line</td>
<td>FAX or Modem Line</td>
</tr>
<tr>
<td>Materials</td>
<td>Dry Pair (monthly rental fee)</td>
<td>ACS Dry Cable Pairs</td>
</tr>
<tr>
<td>Misc. Service</td>
<td>Indoor Loud Bell</td>
<td>Indoor Loud Bell (Wheellock UTA-WH-VPS)</td>
</tr>
<tr>
<td></td>
<td>Telephone Jack (all types)</td>
<td>All types of telephone jacks (single/dual/quad)</td>
</tr>
<tr>
<td></td>
<td>Data Jack (8 Pin)</td>
<td>Jack, Keyed 8 Pin</td>
</tr>
<tr>
<td></td>
<td>Handset/Line Cords (Any Size)</td>
<td>Handset/Line Cords (Any Size)</td>
</tr>
<tr>
<td></td>
<td>Outdoor Signal Horn (15w Bogen)</td>
<td>Outdoor Signal Horn (15w Bogen)</td>
</tr>
<tr>
<td></td>
<td>Outdoor Signal Horn (Claxton)</td>
<td>Outdoor Signal Horn (Claxton)</td>
</tr>
<tr>
<td></td>
<td>Analog Terminal Adapter</td>
<td>NORSTAR - Analog Terminal Adapter</td>
</tr>
<tr>
<td></td>
<td>Run Cross Connects (MDF/IDF)</td>
<td>MDF of IDF Run Cross-Connects</td>
</tr>
<tr>
<td></td>
<td>Run CAT6 Cable (per ft.)</td>
<td>Station Wire 4 Pair</td>
</tr>
<tr>
<td></td>
<td>Voice Mailbox</td>
<td>Voice Mailbox</td>
</tr>
<tr>
<td>Trunk Access</td>
<td>Pager Notification via Voice Mail</td>
<td>Pager Notification via Voice Mail</td>
</tr>
<tr>
<td></td>
<td>Restore Voice Mail Password</td>
<td>Restore Voice Mail due to Password Lockout</td>
</tr>
<tr>
<td></td>
<td>Equipment Service Charge</td>
<td>Equipment Service Charge</td>
</tr>
<tr>
<td></td>
<td>TRK ACC CHGE-National Airport</td>
<td>Trunk Access Charge - National Airport</td>
</tr>
<tr>
<td></td>
<td>TRK ACC CHGE-Dulles Airport</td>
<td>Trunk Access Charge - Dulles Airport</td>
</tr>
</tbody>
</table>
APPENDIX 4

HISTORICAL VOLUMES
## CY2011 Trouble Ticket Counts

<table>
<thead>
<tr>
<th>Month</th>
<th>DCA Troubles</th>
<th>IAD Troubles</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>73</td>
<td>123</td>
</tr>
<tr>
<td>February</td>
<td>55</td>
<td>107</td>
</tr>
<tr>
<td>March</td>
<td>130</td>
<td>134</td>
</tr>
<tr>
<td>April</td>
<td>62</td>
<td>135</td>
</tr>
<tr>
<td>May</td>
<td>90</td>
<td>127</td>
</tr>
<tr>
<td>June</td>
<td>81</td>
<td>136</td>
</tr>
<tr>
<td>July</td>
<td>83</td>
<td>118</td>
</tr>
<tr>
<td>August</td>
<td>69</td>
<td>116</td>
</tr>
<tr>
<td>September</td>
<td>81</td>
<td>129</td>
</tr>
<tr>
<td>October</td>
<td>120</td>
<td>151</td>
</tr>
<tr>
<td>November</td>
<td>60</td>
<td>140</td>
</tr>
<tr>
<td>December</td>
<td>94</td>
<td>144</td>
</tr>
<tr>
<td><strong>CY2011 TT Totals</strong></td>
<td><strong>998</strong></td>
<td><strong>1,560</strong></td>
</tr>
</tbody>
</table>

## CY2011 Work Order Counts

<table>
<thead>
<tr>
<th>Month</th>
<th>DCA Work Orders</th>
<th>IAD Work Orders</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>129</td>
<td>188</td>
</tr>
<tr>
<td>February</td>
<td>109</td>
<td>138</td>
</tr>
<tr>
<td>March</td>
<td>111</td>
<td>174</td>
</tr>
<tr>
<td>April</td>
<td>133</td>
<td>206</td>
</tr>
<tr>
<td>May</td>
<td>106</td>
<td>194</td>
</tr>
<tr>
<td>June</td>
<td>140</td>
<td>169</td>
</tr>
<tr>
<td>July</td>
<td>89</td>
<td>152</td>
</tr>
<tr>
<td>August</td>
<td>118</td>
<td>173</td>
</tr>
<tr>
<td>September</td>
<td>108</td>
<td>190</td>
</tr>
<tr>
<td>October</td>
<td>98</td>
<td>332</td>
</tr>
<tr>
<td>November</td>
<td>81</td>
<td>182</td>
</tr>
<tr>
<td>December</td>
<td>134</td>
<td>144</td>
</tr>
<tr>
<td><strong>CY2011 WO Totals</strong></td>
<td><strong>1,356</strong></td>
<td><strong>2,242</strong></td>
</tr>
</tbody>
</table>
## CY2010 Trouble Ticket Counts

<table>
<thead>
<tr>
<th>Month</th>
<th>DCA Troubles</th>
<th>IAD Troubles</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>77</td>
<td>170</td>
</tr>
<tr>
<td>February</td>
<td>44</td>
<td>142</td>
</tr>
<tr>
<td>March</td>
<td>77</td>
<td>129</td>
</tr>
<tr>
<td>April</td>
<td>68</td>
<td>172</td>
</tr>
<tr>
<td>May</td>
<td>82</td>
<td>160</td>
</tr>
<tr>
<td>June</td>
<td>96</td>
<td>196</td>
</tr>
<tr>
<td>July</td>
<td>80</td>
<td>201</td>
</tr>
<tr>
<td>August</td>
<td>84</td>
<td>186</td>
</tr>
<tr>
<td>September</td>
<td>81</td>
<td>221</td>
</tr>
<tr>
<td>October</td>
<td>100</td>
<td>156</td>
</tr>
<tr>
<td>November</td>
<td>95</td>
<td>171</td>
</tr>
<tr>
<td>December</td>
<td>86</td>
<td>133</td>
</tr>
<tr>
<td>CY2010 TT Totals</td>
<td>970</td>
<td>2,037</td>
</tr>
</tbody>
</table>

## CY2010 Work Order Counts

<table>
<thead>
<tr>
<th>Month</th>
<th>DCA Work Orders</th>
<th>IAD Work Orders</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>94</td>
<td>269</td>
</tr>
<tr>
<td>February</td>
<td>153</td>
<td>318</td>
</tr>
<tr>
<td>March</td>
<td>166</td>
<td>347</td>
</tr>
<tr>
<td>April</td>
<td>135</td>
<td>360</td>
</tr>
<tr>
<td>May</td>
<td>100</td>
<td>262</td>
</tr>
<tr>
<td>June</td>
<td>144</td>
<td>278</td>
</tr>
<tr>
<td>July</td>
<td>131</td>
<td>334</td>
</tr>
<tr>
<td>August</td>
<td>129</td>
<td>190</td>
</tr>
<tr>
<td>September</td>
<td>113</td>
<td>283</td>
</tr>
<tr>
<td>October</td>
<td>133</td>
<td>309</td>
</tr>
<tr>
<td>November</td>
<td>116</td>
<td>213</td>
</tr>
<tr>
<td>December</td>
<td>77</td>
<td>163</td>
</tr>
<tr>
<td>CY2010 WO Totals</td>
<td>1,491</td>
<td>3,326</td>
</tr>
</tbody>
</table>
**ACS System:**

<table>
<thead>
<tr>
<th>Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Woking Trunk Lines</td>
<td>1,787</td>
</tr>
<tr>
<td>Working Lines</td>
<td>8,967</td>
</tr>
<tr>
<td>Total Ports</td>
<td>10,754</td>
</tr>
</tbody>
</table>

**Recent Invoice Count:**

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenants Printed and Mailed</td>
<td>282</td>
</tr>
<tr>
<td>MWAA Printed</td>
<td>62</td>
</tr>
<tr>
<td>MWAA Electronic (E-mail)</td>
<td>57</td>
</tr>
<tr>
<td>Tenants Electronic (E-Mail)</td>
<td>4</td>
</tr>
<tr>
<td>Total</td>
<td>405</td>
</tr>
</tbody>
</table>

**Supplemental Services Work:**

<table>
<thead>
<tr>
<th>Year</th>
<th>Count</th>
<th>Dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>192</td>
<td>Over $6,000,000</td>
</tr>
<tr>
<td>2011</td>
<td>177</td>
<td>Over $6,000,000</td>
</tr>
</tbody>
</table>
APPENDIX 5

HOURS OF OPERATION
<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Hours of Operation</th>
<th>Hours Staffed (M-F)</th>
<th>Hours Staffed (Saturday)</th>
<th>Hours Staffed (Sunday)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ACS Program Management</td>
<td>24 hours per day</td>
<td>8:30 AM - 5:30 PM</td>
<td>On Call</td>
<td>On Call</td>
</tr>
<tr>
<td>2 ACS Site Management</td>
<td>24 hours per day</td>
<td>8:30 AM - 5:30 PM</td>
<td>On Call</td>
<td>On Call</td>
</tr>
<tr>
<td>3 ACS Technical Support</td>
<td>24 hours per day</td>
<td>8:30 AM - 12:00 AM</td>
<td>8:00 AM - 12:00 PM</td>
<td>On Call</td>
</tr>
<tr>
<td>4 System Support – ACS System Support</td>
<td>24 hours per day</td>
<td>8:30 AM - 5:30 PM</td>
<td>8:00 AM - 12:00 PM</td>
<td>On Call</td>
</tr>
<tr>
<td>5 System Support – Help Desk/Work Order Support</td>
<td>12 hours per day</td>
<td>6:00 AM - 6:00 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 System Support – Billing System Support</td>
<td>8 hours per day</td>
<td>8:30 AM - 5:30 PM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Holidays will be considered as a Sunday.
APPENDIX 6

RESPONSIBILITY FOR ASSIGNED PROPERTY
The Contractor shall have custodial responsibility for all Airports Authority physical property issued to its control with an acquisition cost of $500.00 or more, during the contract term. Authority personal property, which includes computer equipment, furniture, fax and copier machines, etc., will be tracked by: (i) Airports Authority-issued bar codes; (ii) if no Airports Authority issued bar code, then by serial number assigned by the manufacturer; or (iii) if no bar code or a serial number, such as furniture, a unique identification number issued by Contractor personnel for tracking purposes. This number will be of a type and range approved by the COTR. A property inventory of all issued assets shall be conducted on the first and last day of the contract term to determine Contractor responsibility of Airports Authority property. The inventory listing shall include the description of the property, bar-code number (if assigned), serial number (or ID number), acquisition cost, acquisition date, manufacturer, location and user. If the acquisition cost and date for an issued asset cannot be provided to the Contractor by the Airports Authority, then the Contractor shall provide an estimated acquisition cost and date for the inventory listing, subject to the COTR's approval. The Airports Authority will provide all equipment and supplies necessary to provide and track property by bar-code. Unscheduled property inventories will be conducted by the Airports Authority during the contract term. The Contractor accepts the issued property in "as is condition." The property will be returned to the Airports Authority in the same condition as issued, reasonable wear and tear expected. The Contractor is not liable for the loss or damage of Airports Authority property, except when such loss or damage results from negligence by the Contractor. The Contractor's responsibility stated herein is solely for the purpose of tracking Airports Authority physical property that is issued to the Contractor and that is used exclusively by the Contractor in the performance of its contract scope.
APPENDIX 7

PERFORMANCE STANDARDS
<table>
<thead>
<tr>
<th>Objective</th>
<th>Metric</th>
<th>Target Performance Standard</th>
<th>Acceptable Performance Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Service</td>
<td>P.01 Grade of Service</td>
<td>100%/mo</td>
<td>100%/mo</td>
</tr>
<tr>
<td>Reliable Service</td>
<td>Network Uptime</td>
<td>100%/mo</td>
<td>99.95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>Normal Equipment Installs in 10 calendar days or less</td>
<td>100%/mo</td>
<td>98%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>Expedited Equipment installs in 7 calendar days or less</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>Answer phone call within 15 seconds – Within Business Hours</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>Answer phone call within 30 seconds – Outside Business Hours</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>Answer phone call within 45 seconds – Weekend Hours</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>Answer phone call within 60 seconds – Holiday Hours</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>On-Site Response – Major Alarm 7AM to 9PM – One Hour</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>On-Site Response – Major Alarm 9PM to 7AM – Two Hour</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>On-Site Response – Minor Alarm 7AM to 9PM – Same Day</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>On-Site Response – Major Alarm 9PM to 12PM – Next Day</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>On-Site Response – Major Alarm 12PM to 7AM – Same Day</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>Repair Logical Configuration Troubles Within Business Hours in less than 1 Hour</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Timely Service</td>
<td>Repair Logical Configuration Troubles Outside Business Hours in less than 2 Hour</td>
<td>100%/mo</td>
<td>95%/mo</td>
</tr>
<tr>
<td>Customer Service</td>
<td>Recommend new service offerings to the Authority for consideration</td>
<td>4/yr</td>
<td>2/yr</td>
</tr>
<tr>
<td>Reliable Service</td>
<td>Number of Trouble Tickets per 100 Working Ports</td>
<td>&lt; 2</td>
<td>&lt; 3</td>
</tr>
</tbody>
</table>
APPENDIX 8

SAMPLE POSITION DESCRIPTIONS
<table>
<thead>
<tr>
<th>TITLE:</th>
<th>Program Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>YEARS OF RELEVANT EXPERIENCE:</td>
<td>3</td>
</tr>
</tbody>
</table>
| EDUCATION: | College Bachelors Degree or higher  
Major in Marketing, Business, or Engineering desirable |
| CERTIFICATIONS/TRAINING: | |
| DESCRIPTION OF RELEVANT EXPERIENCE: | Experience serving as a Program Manager over a telecommunications operation contract involving a minimum of 3,000 handsets, 4 central switches, providing services to over 100 separate companies over 2 or more campuses. |

*Note: Entries that are in italics are recommended minimums for the example CLIN*
<table>
<thead>
<tr>
<th>TITLE:</th>
<th>Airport Site Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>YEARS OF RELEVANT EXPERIENCE:</td>
<td>3</td>
</tr>
<tr>
<td>EDUCATION:</td>
<td>College Associates Degree or higher desirable</td>
</tr>
<tr>
<td>CERTIFICATIONS/TRAINING:</td>
<td></td>
</tr>
</tbody>
</table>

**DESCRIPTION OF RELEVANT EXPERIENCE:**

*Experience serving as a Site Manager over a telecommunications operation contract involving a minimum of 1,000 handsets, 2 central switches, and providing services to over 50 separate companies.*

<table>
<thead>
<tr>
<th>TITLE:</th>
<th>PSCC Site Manager</th>
</tr>
</thead>
</table>

*Note: Entries that are in italics are recommended minimums for the example CLIN*
YEARS OF RELEVANT EXPERIENCE: 3

EDUCATION: Bachelor’s Degree desirable

CERTIFICATIONS/TRAINING:
- Avaya or Nortel Communication Server 1000 Linux Platform Architecture
- Avaya or Nortel Communication Server 1000 to Rls. 6.0 Upgrades for Technicians
- Avaya or Nortel Communication Server 1000 Rls. 6.0 Upgrades for Engineers
- Avaya or Nortel Call Pilot Rls. 5.0 Engineering
- Avaya or Nortel Communication Server 1000 Rls. 5.0 & IP Networking Design
- Avaya or Nortel Communication Server 1000 Rls. 5.0 Upgrades for Engineers
- Avaya or Nortel Call Pilot Rls. 5.0 Installation & Configuration
- Avaya or Nortel Communication Server 1000 Rls. 5.0 Upgrades for Technicians
- Avaya or Nortel Technology Standards and Protocol for IP Telephony Solutions
- Avaya or Nortel Call Pilot Rls. 4.0 Unified Messaging
- Avaya or Nortel NCSS-Communication Server 1000/4.0 Software Installation and Maintenance
- Avaya or Nortel Communication Server (CS) 1000 Rls. 4.0 Hardware I&M
- Avaya or Nortel Call Pilot 4.0 Installation and Maintenance Exam
- Avaya NNCSS Call Pilot 2.0 Certification Exam
- Avaya NNCSS Meridian 1 Database Exam
- BRI/PRI/ISDN Installation and Maintenance

DESCRIPTION OF RELEVANT EXPERIENCE:
Experience serving as a Site Manager over a Public Safety Communications Center operation contract involving a minimum of 100 handsets, E911 Call Center Plant Vesta equipment.

Note: Entries that are in italics are recommended minimums for the example CLIN
**TITLE:** Senior System Design Specialist  

**YEARS OF RELEVANT EXPERIENCE:** 3  

**EDUCATION:**  
*College Associates Degree or higher desirable and Relevant Training Certificates to support this position*

**CERTIFICATIONS/TRAINING:**
- Attended and passed the Avaya or Nortel X11 Database Administration course  
- Attended and passed the Avaya or Nortel Call-Pilot Database Administration course.  
- Must have a minimum of four (4) year experience with Avaya or Nortel Call-Pilot product.  
- Must have working knowledge of Centigram Voice Mail programming and features (within first 3 months of employment).  
- Must have working knowledge of Avaya or Nortel NARS/BARS.  
- Must have working knowledge of Avaya or Nortel ACD  
- Working knowledge and/or training in Voice Over IP desired

**DESCRIPTION OF RELEVANT EXPERIENCE:**
This individual will be responsible for the software programming and managing of the Avaya PBX voice systems as well as the Call Pilot data base. The duties also include audits of both phone, voice mail and cable records, both ACS copper, Verizon DM-7 pairs and optical fiber records. The SDS will also be responsible for the monthly pass word changes on all critical ACS systems.
EDUCATION: College Associates Degree or higher desirable and Relevant Training to support this position

CERTIFICATIONS/TRAINING:

DESCRIPTION OF RELEVANT EXPERIENCE:

This person is responsible for being the point of contact for all MWAA and tenant billing issues as it relates to MWAA Telecommunications services. Additional duties include any NetPlus reports or historical data needed to support any billing issues that might arise from the various tenants or MWAA departments and the managing of the ACS copper and optical fiber cable records which are needed for billing the various tenants.

Demonstrated skills in the areas of:

- Billing & Invoicing
- Bookkeeping / Account Specialist
- Database Management / Support
- Administrative Support
- Workflow & Organization Management
APPENDIX 9

INFORMATION SECURITY STANDARDS
INFORMATION SECURITY STANDARDS

FOREWORD

These Information Security Standards (ISS) define the Metropolitan Washington Airports Authority (the Authority) standards governing the set up and operation of all Authority owned data processing systems and associated networks. It is issued under the authority of the Authority Electronic Communications Systems Policy (GA-005), section 4.b.

George R. Ellis
Vice President for Information and Telecommunication Systems

Date 2/7/2011
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Purpose</td>
<td>1</td>
</tr>
<tr>
<td>2.0</td>
<td>Definitions</td>
<td>1</td>
</tr>
<tr>
<td>3.0</td>
<td>Firewall Standard</td>
<td>2</td>
</tr>
<tr>
<td>4.0</td>
<td>Installation Standard for New Systems</td>
<td>3</td>
</tr>
<tr>
<td>5.0</td>
<td>Data Classification Standard</td>
<td>3</td>
</tr>
<tr>
<td>6.0</td>
<td>Data Retention Standard</td>
<td>4</td>
</tr>
<tr>
<td>7.0</td>
<td>Encryption Standard</td>
<td>4</td>
</tr>
<tr>
<td>8.0</td>
<td>Vulnerability Management Standard</td>
<td>5</td>
</tr>
<tr>
<td>9.0</td>
<td>Patch Management Standard</td>
<td>5</td>
</tr>
<tr>
<td>10.0</td>
<td>Access Control Standard</td>
<td>5</td>
</tr>
<tr>
<td>11.0</td>
<td>Password Standard</td>
<td>6</td>
</tr>
<tr>
<td>12.0</td>
<td>Physical Security Standard</td>
<td>7</td>
</tr>
<tr>
<td>13.0</td>
<td>Security Monitoring Standard</td>
<td>8</td>
</tr>
<tr>
<td>14.0</td>
<td>Security Testing Standard</td>
<td>9</td>
</tr>
<tr>
<td>15.0</td>
<td>Incident Response Standard</td>
<td>10</td>
</tr>
<tr>
<td>16.0</td>
<td>Security Awareness Standard</td>
<td>11</td>
</tr>
<tr>
<td>17.0</td>
<td>Vendor Management Standard</td>
<td>11</td>
</tr>
<tr>
<td>18.0</td>
<td>Configuration Management Standard</td>
<td>12</td>
</tr>
<tr>
<td>19.0</td>
<td>Availability Management Standard</td>
<td>12</td>
</tr>
</tbody>
</table>
Information Security Standard

1.0 Purpose

The Metropolitan Washington Airports Authority provides electronic communication equipment and systems to enable Users to accomplish the Authority's mission and to promote the efficient conduct of Authority business. It is consistent with the Authority’s commitment to Safety, Security and Risk Reduction that standards be identified for the establishment, maintenance and usage of such systems in a manner that promotes Information Security.

This document is subordinate to, and is to be interpreted consistent with, the Authority Electronic Communications Systems Policy (GA-005). It is issued under the authority of the Authority Electronic Communications Systems Policy, section 4.b and will be periodically reviewed, maintained and updated by the Office of Information and Telecommunications Systems.

2.0 Definitions

2.1 Authorized Personnel: See the Authority Electronic Communications Systems Policy (GA-005).

2.2 Confidential Information: See the Authority Electronic Communications Systems Policy (GA-005).

2.3 Information Security Group: A group within the Office of Information and Telecommunications Systems designated to monitor and improve the Authority’s Information Security posture.

2.4 Network Architect: The person within the Office of Information and Telecommunications Systems designated as responsible for the design of the Authority Data Network.

2.5 Owner: See the Authority Electronic Communications Systems Policy (GA-005).

2.6 Private Information: See the Authority Electronic Communications Systems Policy (GA-005).

2.7 Policy: See the Authority Electronic Communications Systems Policy (GA-005).

2.8 System Custodian: See the Authority Electronic Communications Systems Policy (GA-005).

2.8.1 Database Custodian: A System Custodian who is tasked with the technical support of one or more databases.

2.8.2 Network Custodian: A System Custodian who is tasked with the technical support of network equipment and connections.

2.8.3 Server Custodian: A System Custodian who is tasked with the technical support of one or more servers.
2.8.4 **Workstation Custodian:** A System Custodian who is tasked with the technical support of one or more workstations and related peripheral devices.

2.9 **User:** See the Authority Electronic Communications Systems Policy (GA-005).

### 3.0 Firewall Standard

#### 3.1 Firewall configuration standard

3.1.1 All firewall configurations will be tested and approved by the assigned Network Custodian.

3.1.2 The Network Custodian will update and maintain a network diagram with all connections into their assigned network represented and provide an updated copy to the Network Architect and to the Information Security Group within MA-600.

3.1.3 An enterprise firewall must be maintained at each Internet connection, between any demilitarized zone (DMZ) and the internal network zone and between network zones as determined by the Information Security Group.

3.1.4 The following individuals and/or groups have responsibilities for logical management of the listed network components:

- Firewalls: Network Custodian
- Routers: Network Custodian
- Switches: Network Custodian
- Wireless Access Points: Network Custodian
- VPN Devices: Network Custodian
- IP Range Assignments: MA-640 (Network Architect)

Documentation of the approved settings of each firewall must be maintained by the Network Custodian.

3.1.5 Each protocol other than hypertext transfer protocol (HTTP), secure sockets layer (SSL), secure shell (SSH), hypertext transfer protocol over secure socket layer (HTTPS), transport layer security (TLS) and virtual private network (VPN) will be justified and documented by the Network Custodian.

3.1.6 Each protocol allowed, such as file transfer protocol (FTP), will be justified and documented by the Network Custodian with appropriate compensating controls.

3.1.7 Each Authority router will be configured according to the base rule set approved by the Network Custodian.

3.1.8 The Information Security Group will perform a quarterly review of firewall and router configuration files and compare to approved settings.
4.0 Installation Standard for New Systems

4.1 All vendor-supplied default passwords and accounts must be changed by the System Custodian as part of the system installation

4.1.1 For wireless environments, change wireless vendor defaults, including, but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable protected access technology for encryption and authentication according to current industry best practices.

4.2 New systems will be installed by the System Custodian according to industry best practices.

4.2.1 All unnecessary services and protocols will be disabled

4.2.2 System security parameters will be configured to prevent misuse

4.2.3 All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and web servers will be removed

4.2.4 Each server will have only one primary function (for example, web server, database server, DNS, etc.)

4.3 Administrative access to systems across network boundaries will only be allowed by encrypted non-console services such as SSH, VPN or SSL

4.4 Warning banners will be displayed as specified in the Authority IT Policy – Banners as published on the Authority’s Livelink site.

4.5 Screensavers that require re-verification will be enabled with no more than a 15 minute wait period.

5.0 Data Classification Standard

5.1 Any data containing information such as credit card data, social security numbers, performance issues or medical files is classified as private information

5.1.1 Private information must be protected by the information owner with the appropriate technical, administrative and physical safeguards

5.1.2 Private information may only be shared with authorized personnel, as determined by the information owner

5.1.3 Unauthorized disclosure or access to private information must be reported immediately to the immediate supervisor and/or information owner.

5.1.4 Private information may not be copied, moved, or stored onto local hard drives or removable electronic media without specific authorization by the information owner.

5.2 Any data containing information that is intended for Authority business purposes only, such as system information, pending procurement matters, Authority credit card data or prospective bond issues is classified as confidential
5.2.1 Confidential information must be protected by the information owner with the appropriate technical, administrative and physical safeguards

5.2.2 Confidential information may only be shared with Authority employees and/or contractors on a business need-to-know basis, as determined by the information owner.

5.2.3 Unauthorized disclosure or access to confidential information must be reported immediately to the immediate supervisor and/or information owner.

6.0 Data Retention Standard

6.1 The System Owner will develop and assure implementation of data retention standards for information contained within their systems.

6.2 Data retention standards will be developed with full consideration to legal, regulatory and business requirements for retention of subject data.

6.3 Data retention standards will include provisions for disposal of data when no longer needed for legal, regulatory or business requirements.

6.4 Where legal, regulatory or business requirements dictate; a manual or automated process to remove data exceeding the applicable data retention standard will be developed.

7.0 Encryption Standard

7.1 Strong cryptography (as defined in FIPS 140-2) and security protocols will be used when transmitting private or confidential data such as passwords, pending procurement matters or credit card data

7.1.1 When entering or transmitting private or confidential data such as passwords, pending procurement matters or credit card data via an Internet browser, you must ensure that the address begins with https:// and that the secure lock symbol is visible in your browser window.

7.1.2 Users must never transmit private or confidential data such as passwords, pending procurement matters or credit card data over an open, public network without encryption through security protocols such as secure sockets layer (SSLv3/TLS) and Internet protocol security (IPSEC)

7.1.3 Users must never send private or confidential data such as passwords, pending procurement matters or credit card data via unencrypted email or other unsecured methods

7.1.4 Users must assure that the destination URL and/or IP number used in transmission of encrypted data is legitimate.
8.0 Vulnerability Management Standard

8.1 Anti-malware software will be deployed and maintained by the System Custodian on all systems commonly affected by viruses and other forms of malware

8.1.1 The software must be capable of detecting, removing and protecting against viruses and other forms of malicious software, including spyware and adware

8.2 The System Custodian will ensure, no less frequently than weekly, that all anti-malware mechanisms are current, actively running and capable of generating audit logs

9.0 Patch Management Standard

9.1 The System Custodian will ensure, no less frequently than monthly, that all system components and software have the latest vendor-supplied security patches installed

9.2 The System Custodian will maintain a method to identify newly discovered security vulnerabilities for Authority system components and software

9.3 All software development will follow a formal software development life cycle, implementing information security throughout the process

9.4 Separate development, test, and production environments will be maintained

9.5 There will be a separation of duties between production environments and others

9.6 There must be a documented change control process for all production hardware and software changes maintained by the System Custodian

9.7 The web application development teams will follow the Open Web Application Security Project guidelines during custom application development

9.8 All web-facing applications must be protected against known attacks by one of the following methods: (1) independent validation of all custom application code or (2) installing an application layer firewall in front of the web-facing application

10.0 Access Control Standard

10.1 Access to system components must be restricted on a business need-to-know basis

10.2 For usage of critical user-facing technologies, each user must abide by the standard/policy governing proper use, including:

10.2.1 Explicit management approval (See Electronic Communications Systems Policy, Sec. 5.b.)

10.2.2 Authentication/authorization for use of the technology as established by the System Custodian
10.2.3 Acceptable uses of the technologies (See Electronic Communications Systems Policy, Sec 9.a.)
10.2.4 Use only products from the company-approved list maintained by the System Custodian.
10.2.5 Automatic disconnect of sessions after a specific period of inactivity set by the System Custodian
10.2.6 Activation of access for vendors only when needed, with immediate deactivation after use

11.0 Password Standard
11.1 Username and password will be unique to an individual and not shared unless authorized by the System Custodian/Information Owner and the Information Security Group
11.2 Where passwords are used, each System Custodian will maintain and enforce a password standard that meets or exceeds industry best practices and the Authority IT Policy – Passwords as published on the Authority’s Livelink site.
11.3 To access The Authority network remotely, each user must have two forms of authentication (such as a password and a VPN certificate)
11.4 Passwords must be encrypted during transmission and storage on all system components
11.5 The System Custodian and/or Owner will ensure proper user authentication and password management on all system components as follows:
   11.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
   11.5.2 Verify user identity before performing password resets
   11.5.3 Set network first-time passwords to a unique value for each user and change immediately after the first use
   11.5.4 Immediately revoke access for any terminated users
   11.5.5 Remove inactive user accounts at least every 90 days
   11.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed
   11.5.7 Communicate password procedures and policies to all users
   11.5.8 Do not use group, shared, or generic accounts and passwords, unless authorized by the System Custodian/Information Owner and the Information Security Group
   11.5.9 Change user passwords at least every 90 days
   11.5.10 Change administrative passwords at least every 60 days
   11.5.11 Require a minimum password length of at least eight characters
   11.5.12 Use passwords containing both numeric and alphabetic characters
   11.5.13 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
11.5.14 Limit repeated access attempts by locking out the user ID after not more than six attempts
11.5.15 Set the lockout duration to no less than thirty minutes or until an administrator enables the user ID
11.5.16 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal
11.5.17 Authenticate all access to any database containing private or confidential data. This includes access by applications, administrators, and all other users

12.0 Physical Security Standard

12.1 Facility entry controls will be implemented to limit and monitor physical access to areas containing private or confidential information
12.1.1 Cameras may be implemented to monitor such areas. Collected data may be monitored and must be stored for a minimum of seven days
12.1.2 Publicly accessible network jacks (other than those intended for guest usage) must require additional authentication before permitting any access
12.1.3 Access to wireless access points and wireless gateways must be restricted
12.1.4 Access to wireless handheld devices with access to private or confidential data must be restricted

12.2 Access to areas where private or confidential information is stored or transmitted must be restricted

12.3 Visitors entering areas where private or confidential data is processed or maintained:
12.3.1 Must be authorized by the system custodian
12.3.2 Must be escorted or given a temporary physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees
12.3.2.1 If a temporary physical token is given, it must be surrendered before leaving the facility or at the date of expiration

12.4 A visitors log that maintains a physical audit trail of visitor activity must be maintained. Collected data must be retained for a minimum of three months

12.5 Media back-ups must be stored in a secure location, preferably off-site

12.6 All paper and electronic media that contains private or confidential data must be physically secured

12.7 The internal and external distribution of any kind of media that contains private or confidential data must be strictly controlled

12.7.1 Mark the media as private or confidential
12.7.2 Transfer the media by secured courier or other delivery method that can be accurately tracked

12.8 Management must approve any and all media that is moved from a secured area, especially when media is distributed to individuals

12.9 The storage and accessibility of media that contains private or confidential data must be strictly controlled

12.9.1 All such media must be properly inventoried and securely stored

12.10 Once the decision to destroy media containing private or confidential data has been made, destruction must proceed as follows:

12.10.1 Cross-cut shred, incinerate or pulp hardcopy materials

12.10.2 Purge, degauss, shred or otherwise destroy electronic media so that private or confidential data cannot be reconstructed

### 13.0 Security Monitoring Standard

13.1 The System Custodian will ensure that all access to system components are linked to each individual user for logging purposes.

13.2 The System Custodian will ensure that automated audit trails for all system components are implemented to reconstruct the following events:

- **13.2.1** All individual user accesses to private or confidential data (through the application or otherwise)
- **13.2.2** All actions taken by any individual with root or administrative privileges
- **13.2.3** Access to audit trails of financial systems or other systems primarily used to process and store private or confidential data
- **13.2.4** Invalid logical access attempts
- **13.2.5** Use of application level identification and authentication mechanisms

13.3 The System Custodian will ensure that all audit trail entries record at least the following parameters for each event:

- **13.3.1** User identification
- **13.3.2** Type of event
- **13.3.3** Date and time
- **13.3.4** Success or failure indication
- **13.3.5** Origination of event
- **13.3.6** Identity or name of affected data, system component, or resource.

13.4 The System Custodian will ensure that all critical system clocks and times are synchronized

13.5 The System Custodian will ensure that all audit trails are secured so that they cannot be altered, and:

- **13.5.1** Limit viewing of audit trails to those with a job-related need
- **13.5.2** Protect audit trail files from unauthorized modifications
- **13.5.3** Promptly back-up audit trail files to a centralized log server or media that is difficult to alter
13.5.4 Copy logs for wireless networks onto a log server on the internal LAN.
13.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert) if a centralized log server is not being used.

13.6 The System Custodian will review logs for all system components at least daily or implement an automated log reviewing function that will generate alerts for unusual events. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol servers (for example, RADIUS).

13.7 Audit trail history must be retained for at least two years, with a minimum of three months online availability.

13.8 The System Custodian will monitor and analyze security alerts and information and distribute to appropriate personnel (including the Information Security Group).

14.0 Security Testing Standard

14.1 The System Custodian (or Information Security Group if designated by the System Custodian) will test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.

14.2 The System Custodian (or Information Security Group if designated by the System Custodian) will test wireless access security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.

14.3 The System Custodian (or Information Security Group if designated by the System Custodian) will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). At a minimum, quarterly external vulnerability scans must be performed by an approved scanning vendor certified by the PCI Security Standards Council.

14.4 The System Custodian (or Information Security Group if designated by the System Custodian) will perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:
14.4.1 Network-layer penetration tests
14.4.2 Application-layer penetration tests.

14.5 The System Custodian (or Information Security Group if designated by the System Custodian) will use network intrusion detection systems and/or
host-based intrusion detection systems and/or intrusion prevention systems
to monitor network traffic and alert personnel to suspected compromises.
The System Custodian or Information Security Group will ensure that all
intrusion detection and prevention engines are up-to-date.

15.0 Incident Response Standard

15.1 Members of the Computer Incident Response Team are as follows:
15.1.1 The Information Security Group
15.1.2 MA-610 Managers
15.1.3 All System Custodians
15.1.4 Others, as needed.

15.2 Authority system users shall notify the Computer Incident Response Team
of all potential security incidents, including but not limited to:
15.2.1 Unauthorized use; (sending SPAM, chain e-mails or threatening e-
           mails, planting viruses, conducting network-level probes/scans,
           exceeding authorization level, etc.)
15.2.2 Theft of data
15.2.3 Unauthorized alteration or deletion of data
15.2.4 Denial of service and/or system failure
15.2.5 Unsuccessful access attempts repeated in excess of defined
       thresholds
15.2.6 Unauthorized access that is manifested:
       15.2.6.1 Internally (by an employee, customer, vendor or other on
              company property)
       15.2.6.2 Externally (by an employee, customer, vendor and all
              others outside company property)

15.3 The Computer Incident Response Team shall establish procedures to:
15.3.1 Recover systems or services as quickly as possible
15.3.2 Analyze and identify the cause of the incident
       15.3.2.1 Allowing only clearly identified and authorized staff to
              access live data and systems
       15.3.2.2 Document in detail all emergency actions
       15.3.2.3 Report to management all emergency actions
       15.3.2.4 Confirm the integrity of business systems and security
              controls with minimal delay
15.3.3 Plan and implement remedies to prevent recurrence
15.3.4 Collect audit trails and/or evidence
       15.3.4.1 To provide evidence for investigation, prosecution, and
              disciplinary actions, certain information should be captured
              whenever it is suspected that computer or network related
              crime or abuse has taken place
15.3.4.2 The relevant information should be securely stored off-line until such time as it is determined that The Authority will not pursue legal action or otherwise use the information.

15.3.4.3 The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, as well as copies of all potentially involved files.

15.3.5 Communicate with business users and others affected by or involved with the recovery from the incident.

16.0 Security Awareness Standard
16.1 All Authority users will attend at least one hour of Information Security training each year.
16.2 Security related articles/inserts will appear in each monthly issue of IT’s NEWS.

17.0 Vendor Management Standard
17.1 Contracting Officers and Contracting Officers’ Technical Representatives will exercise due diligence in selecting IT outsourcing service providers.
17.2 Contracting Officers and Contracting Officers’ Technical Representatives will require IT outsourcing service providers by contract to implement appropriate measures designed to meet the objectives below:
17.2.1 Ensure the security and confidentiality of private and confidential information.
17.2.2 Protect against any anticipated threats or hazards to the security or integrity of such information.
17.2.3 Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any entity.
17.2.4 Dispose of private and confidential information in a secure manner.
17.2.5 Immediately inform The Authority in the event of a security breach involving private or confidential information.
17.3 Contracting Officers’ Technical Representatives will monitor IT outsourcing service providers to confirm that they have satisfied the obligations described above. As part of this monitoring, Contracting Officers and Contracting Officers’ Technical Representatives will review documents that may include, but are not limited to, contracts, audits, and summaries of test results or other documents. In addition, Contracting Officers and Contracting Officers’ Technical Representatives will request a SAS 70 Part II or equivalent third-party assessment of significant IT outsourcing service providers. These reviews will take place on at least an
annual basis for existing vendors. For new vendors, these documents will be reviewed prior to signing any contract.

18.0 Configuration Management Standard
18.1 System Custodian will maintain an inventory of information system components (hardware and software) under their control that:
18.1.1 Ensures the security and confidentiality of private and confidential information
18.1.2 Accurately reflects the current information system(s);
18.1.3 Is consistent with the authorized boundary of the information system(s);
18.1.4 Is at a level of granularity necessary for tracking and reporting.

19.0 Availability Management Standard
19.1 System Custodian will take all reasonable steps to assure system availability during required hours of operation. Steps shall include:
19.1.1 Providing adequate HVAC for equipment;
19.1.2 Providing adequate power supply and power conditioning for equipment;
19.1.3 Performing periodic backups of all central production servers;
19.1.4 Performing periodic restoration testing of central production servers;
19.2 Review, no less frequently than annually, the system architecture (redundant hardware, data paths, and power) for appropriateness.
APPENDIX 10

TELECOMMUNICATION DEPARTMENT ORGANIZATION
APPENDIX 11

DCA VEHICLE AOA REQUIREMENTS
SUBJECT: VEHICLE CONTROL PROGRAM FOR
RONALD REAGAN WASHINGTON NATIONAL AIRPORT

1. PURPOSE

This Orders & Instructions (O&I) establishes the Vehicle Control Program for the Secured Area and Air Operations Area for Ronald Reagan Washington National Airport, as required by Federal Aviation Regulation Part 139, Transportation Security Administration Regulations Part 1542 and the Metropolitan Washington Airports Regulations.

2. DISTRIBUTION

This O&I is distributed to Metropolitan Washington Airports Authority (Airports Authority) Section levels and above, Airport Operations Duty Managers, Police Officers, air carriers, tenants, concessionaires, governmental agencies and contractors at Ronald Reagan Washington National Airport (National).

3. CANCELLATION


4. DEFINITIONS

A. Accident – A collision between one aircraft or vehicle and another aircraft, vehicle, person or object that results in property damage, personal injury or death.

B. Air Operations Area (AOA) – That portion of the airport, as specified in the Airport Security Program, in which security measures mandated by TSAR Part 1542 are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps and safety areas which are used by aircraft regulated under TSAR Part 1544 or 1546, and any adjacent areas, such as general aviation areas, that are not separated by adequate security systems, measures or procedures. This area does not include the Secured Area.

C. Airport Operator – An entity that operates an airport. The airport operator for Ronald Reagan Washington National Airport (National) is the Metropolitan Washington Airports Authority (Airports Authority).
D. **Aircraft Support Vehicles** – Those service vehicles routinely used on the Secured Area or AOA to support aircraft operations, including aircraft tugs, baggage carts, belt loaders, deicers and catering trucks.

E. **Airport Tenant** – Any person or organization, other than an air carrier, that has an agreement with MWAA to conduct business on airport property.

F. **Air Traffic Control (ATCT)** – A service operated by the appropriate authority, normally the Federal Aviation Administration (FAA), to promote the safe, orderly and expeditious flow of air traffic.

G. **AOA Motor Vehicle Operator Permit** – A driving authorization issued by the Airport Manager that allows an individual to operate a motor vehicle on the Secured Area/AOA at National. The individual must first have a valid state driver’s license, participate in a Secured Area/AOA drivers training session and pass the Secured Area/AOA Motor Vehicle Operator Permit test before an AOA Motor Vehicle Operator Permit will be issued. To obtain a Movement Area endorsement, the applicant must have a need determined by the airport and complete the Movement Area training. (see item “S” of this section).

H. **Automated Access Control System (AACS)** – A computer-based access control system.

I. **Contractor** – Any individual(s) who represent a non-tenant service company with a contractual agreement to work at the airport.

J. **Emergency Vehicles** – Trucks, automobiles and equipment used for primary emergency response, such as Airports Authority Police cars, Fire apparatus and Airport Operations vehicles.

K. **Escort** – To continually accompany and monitor the activities of an individual who does not have unescorted access authority into or within the Secured Area, Security Identification Display Area (SIDA) or AOA.

L. **Foreign Object Debris (FOD)** – Debris found on runways, taxiways and aprons that can cause damage to aircraft components.

M. **Identification (ID) Badge** – Access media that meets the requirements of TSAR Part 1542 and the DCA Airport Security Program.

N. **Instrument Landing System (ILS) Critical Area** – An area provided to protect the signals of a localizer and glide slope.

O. **Incursion** – Any occurrence at an airport involving an aircraft, vehicle, person or object on the ground which creates a collision hazard or results in a loss of separation with an aircraft taking off, intending to take off, landing or intending to land.
P. **Jet Blast** – Turbine engine exhaust or propeller wash.

Q. **Levee Road** – The airport perimeter road that follows the shoreline of the Potomac River along the eastern boundary of National (see Enclosure 1). Levee Road begins on the south end of the airport at Vehicle Gate A and runs eastward across the approach paths of Runways 4 and 1. It then turns north along the riverbank, crossing the approach paths of Runways 33 and 22. It turns west at the north boathouse, crossing the approach paths of Runways 19 and 15, ending as it connects to the designated vehicle lane at the edge of the commuter aircraft parking ramp.

R. **Light Gun** – A hand-held light signaling device that emits a bright narrow beam of white, green or red light, as selected by the air traffic controller, and is used to signal approval or disapproval of anticipated pilot or vehicle actions when radio communication is not available.

S. **Movement Area** – The runways, taxiways and other areas of an airport that are used for the taxiing, take off and landing of aircraft, exclusive of loading ramps and aircraft parking aprons.

T. **Movement Area Service Road** – The driving lane that ground vehicles may use to cross an active taxiway without clearance from the ATCT. The Movement Area Service Road extends from the Terminal A “Banjo” area across Taxiway P to the vehicle lane adjacent to the airport fire station.

U. **Non-movement Area** – Ramps and airport service roads wherein clearance from the ATCT is not required to operate a motor vehicle.

V. **Operator** – Any person who is in actual physical control of an aircraft or motor vehicle, regardless of the ownership of the vehicle.

W. **Owner** – Any person who holds the legal title of an aircraft or motor vehicle.

X. **Ramps (Aprons)** – Paved areas used for the parking or servicing of aircraft.

Y. **Restricted Areas** – Those areas of the airport not intended for public access unless authorization has been granted. These areas are clearly identified with warning signs.

Z. **Runway** – A defined rectangular area on a land airport constructed for the landing and takeoff runs of aircraft along its length.

AA. **Runway Safety Area** – A defined space surrounding the runway prepared or suitable for reducing the risk of damage to airplanes in the event of an undershoot, overshoot or excursion from the runway.
BB. **Secured Area** – That portion of the airport specified in the Airport Security Program in which certain security measures mandated by TSAR Part 1542 are carried out. This area includes locations where air carriers enplane and deplane passengers, sort and load baggage, and any adjacent areas that are not separated by adequate security measures.

CC. **Security-controlled Areas** – Areas of the airport where access is controlled for security purposes. The Secured Area, AOA, SIDA and Restricted Areas are all considered security-controlled areas.

DD. **Security Identification Display Area (SIDA)** – That portion of the airport, specified in the Airport Security Program, wherein security measures mandated by TSAR Part 1542 are carried out. The SIDA at National includes the Secured Area and may include other areas of the airport.

EE. **Taxiway** – A defined path designated for the surface maneuvering of aircraft to and from the runways and aircraft parking areas.

FF. **Vehicle Lane** – The roadway that motor vehicle operators use to move between destination points on the Secured Area/AOA of National.

5. **POLICY**

CFR Part 139 requires an airport operator to ensure that each employee, tenant or contractor who operates a ground vehicle on any portion of the airport’s secured areas or the movement area is familiar with the airport’s procedures for the safe operation of ground vehicles and the consequences of non-compliance. In order to comply with this regulation, National has established this O&I to provide rules governing the operation of a motor vehicle within the Secured Area and AOA.

6. **GENERAL**

The only motor vehicle operations permitted on the Secured Area or AOA are those vehicles operated by the Airports Authority, the airlines and airport tenants who provide regular and consistent service in the Secured Area and AOA. All vehicles must successfully complete a vehicle safety inspection before they may be operated on any part of the Secured Area or AOA. Vehicle safety inspections are conducted by either the Airport Operations Duty Managers or Airport Operations Safety and Security Personnel.

A Secured Area/AOA motor vehicle operator permit and a valid state driver’s license are required for all individuals who operate a motor vehicle on the Secured Area or AOA. Vehicle operators are responsible for the actions of all passengers associated with the vehicle they are operating while in the Secured Area/AOA.
7. **MOVEMENT AND NON-MOVEMENT AREAS**

A. **MOVEMENT AREA**

The ATCT controls all vehicle movement within the movement area. Vehicles operating on the movement area must be capable of two-way radio communication with the ATCT on the Ground Control frequency of 121.7 MHz or must be escorted by a vehicle that has that capability. Only authorized individuals may drive on the movement area of the airport, and then only after receiving clearance to proceed from the ATCT. Vehicles operating on service roadways or Levee Road need not communicate with the ATCT but they must have that capability while on these roadways unless specifically authorized by Airport Operations to operate without two-way radio communications capability.

(1) **LOSS OF COMMUNICATION PROCEDURES**

(a) Because radio equipment could fail at any time, it is imperative that vehicle operators look in all directions and for light gun signals from the ATCT before proceeding onto any runway, taxiway or other aircraft movement area, even though they have received an ATCT clearance to proceed.

(b) If a vehicle that has established radio contact with the ATCT should lose radio contact, the operator should immediately clear the area and return to the closest non-controlled area on the airport if he can do so without crossing a usable runway or taxiway. Otherwise, the operator should clear the active runway or taxiway and attempt to signal the ATCT of the situation by flashing the vehicle headlights on and off. The driver shall await assistance from either Airport Operations or a light gun signal from the ATCT to clear the area.

(c) Any vehicle that is reasonably expected to operate on usable runways or taxiways will have a placard with a description of the light gun signals used by the ATCT as shown below. These placards may be obtained from Airport Operations. Vehicle operators are responsible for understanding the meaning of these signals and for complying with them. The light gun signals and their meanings are as follows:
## Runway Markings, Lights and Signs

Runways are areas where aircraft land and take off. Runways are always designated by a number such as 15 or 33. The numbers indicates the compass heading of the runway. An aircraft taking off on runway 15 is headed 150 degrees. All runway markings are white except for the yellow lead-in/lead-off lines that extend from the runway centerline.

(a) **Runway lights are lighted with a variety of colored lights:**

1. **Runway Edge-Lights** are white. If the runway has an instrument approach, the last 2,000 feet of the runway will be yellow in color.
2. **Runway Centerline Lights** are white except for the last 3,000 feet of the runway, where they begin to alternate red and white. For the last 1,000 feet of runway the centerline lights are all red.
3. **Runway Touchdown Zone Lights** are white
4. **Runway End/Threshold Lights** are split lenses that are red/green.

(b) Runway Distance Remaining Signs:

<table>
<thead>
<tr>
<th>Light Description</th>
<th>Sign Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steady Green</td>
<td>Cleared to cross or proceed</td>
</tr>
<tr>
<td>Steady Red</td>
<td>Stop</td>
</tr>
<tr>
<td>Flashing Red</td>
<td>Clear the runway or taxiway</td>
</tr>
<tr>
<td>Flashing White</td>
<td>Return to starting point</td>
</tr>
<tr>
<td>Alternating Red &amp; Green</td>
<td>Exercise extreme caution</td>
</tr>
</tbody>
</table>

3 Runway distance remaining signs provide distance remaining information to pilots during takeoff and landing operations. They have white numbering on a black background. The number on the sign provides the remaining runway length in 1,000 foot increments.

## Taxiway Markings, Lights and Signs

Taxiways have yellow paint markings and blue edge lights or reflectors. Taxiways are designated by a letter or a letter-number combination.
(a) **Location Signs**

Location signs indicate that the vehicle operator is located on the designated taxiway or runway. Location signs have yellow lettering in the center of a black panel with a yellow border around it.

(b) **Taxiway Direction and Designation Signs**

Taxiway direction and designation signs have black lettering and a directional arrow or arrows on a yellow background. The arrow indicates the direction to that taxiway, runway, or destination.

(4) **RUNWAY HOLDING POSITION MARKINGS**

Runway holding position markings (“hold bars”) are located across each taxiway which intersects a runway. The hold bars consist of two sets of parallel yellow lines, one pair solid and one pair dashed, which may be outlined in black on light-colored pavement. The solid pair of lines is on the taxiway side of the marking and the dashed pair of lines is on the runway side. Vehicle operators may only cross the hold bars if they are authorized to do so and only if they have received clearance from the ATCT.

(5) **Enhanced Taxiway Centerline Markings**

Enhanced Taxiway Centerline Markings appear before a runway hold line as illustrated. These markings are intended to serve as an additional warning to flight crews that they are approaching the runway.

The runway holding position markings are always located next to a Runway Hold Position Sign, which has white lettering and numbering on a red panel.
(6) Operations on Usable Runways and Taxiways

Airport Operations (703-417-8050) must be notified before beginning ground vehicle operations on any runway or taxiway at National. Once permission has been granted by Airport Operations to conduct operations on a runway or taxiway, the vehicle operator shall remain in the vehicle lane and establish radio contact with the ATCT on Ground Control frequency (121.7 MHz).

The vehicle operator must listen for other traffic on the frequency, wait for a break in the traffic and then call Ground Control and state his/her intentions for the work to be performed. The driver may proceed to the work area only after receiving clearance from Ground Control and acknowledging all instructions with the ATCT. The vehicle operator must still look in all directions for other vehicle or aircraft traffic before proceeding onto any runway or taxiway.

Once the work on the runway or taxiway is completed, the vehicle operator must contact Ground Control again for the ATCT clearance back to the vehicle lane. When back in the vehicle lane, the driver shall advise the ATCT that he/she has returned to the vehicle lane.

(7) Operations on Levee Road

Unless specifically authorized by Airport Operations to operate on Levee Road without two-way radio communications capability with the ATCT, each operator shall ensure that his/her vehicle or the escort vehicle has the capability to communicate with the ATCT on 121.7 MHz. This capability is required in the event it should become necessary for the ATCT to clear or deny use of Levee Road or clear a vehicle to cross the ends of Runways 1 or 19 in low visibility weather.

Use of Levee Road is limited to Airports Authority employees, FAA Airways Facilities Maintenance personnel and others as may be approved on a case-by-case basis by Airport Operations.

B. NON-MOVEMENT AREAS

Non-movement areas include ramps, aprons and other areas not under control of the ATCT. Authorized drivers may operate vehicles and equipment in the non-movement areas without being in positive radio contact with the ATCT.

(1) Vehicle Lane Markings

Vehicle lane markings consist of solid white edge markings and a dashed white line in the center to separate directional lanes of traffic. All ground vehicles must operate within the painted vehicle lanes except when servicing an aircraft.
(2) **Fire Lane Markings**

The fire lanes are designated for emergency vehicle traffic only and are identified by solid red edge lines.

(3) **Non-Movement Area Service Road Markings**

The non-movement area service road is a vehicle lane that may be used to cross an active taxiway without the ATCT clearance. At National the non-movement area service road extends from the vehicle lane at the Terminal A “Banjo” area, across Taxiway P to the vehicle lane adjacent the blast fence. This service road is marked with white zipper line edge markings. Drivers operating vehicles on this roadway must first look in all directions and yield the right of way to all aircraft and emergency vehicles prior to continuing across Taxiway P.

(4) **Non-Movement Area Boundary Marking**

Non-movement area boundary markings are used to delineate the movement area from the non-movement area. These markings consist of two yellow lines, one solid on the non-movement area side and one solid on the movement area side. A driver is not to cross from the solid-lined side without first notifying Airport Operations and obtaining clearance from the ATCT on the Ground Control frequency (121.7 MHz).

8. **SECURED AREA/AOA MOTOR VEHICLE OPERATOR PERMIT CRITERIA**

Anyone desiring to operate a motor vehicle on the AOA must first obtain a Secured Area/AOA Motor Vehicle Operator Permit. The following criteria must be met before a Secured Area/AOA Motor Vehicle Operator Permit will be issued:
A. NATIONAL AIRPORT ID BADGE

All applicants seeking a Secured Area/AOA Motor Vehicle Operator Permit must first have, or have applied for, a National Airport (ID) badge.

B. STATE DRIVER’S LICENSE

All applicants seeking a Secured Area/AOA Motor Vehicle Operator Permit must have a valid state-issued driver’s license. If a permit holder’s state driver’s license should become suspended or revoked, the permit holder must report this information to the Pass & ID Office immediately. All Secured Area/AOA driving privileges shall be revoked until the permit holder provides the Pass & ID Office with proof that his/her state driver’s has been reinstated by the issuing authority.

C. SECURED AREA/AOA DRIVER TRAINING

(1) Secured Area/AOA Driver Training Class/Interactive Video Examination

All applicants to include renewals for a Secured Area/AOA Motor Vehicle Operator Permit must attend the Secured Area/AOA driver training class or successfully pass the computer based interactive video exam with a passing score of 100 percent. The Pass & ID Office trainer must complete the appropriate section of the ID badge application confirming that the driver training was completed.

(2) Movement Area Endorsement Training

All applicants to include renewals requiring a Movement Area endorsement to their AOA Motor Vehicle Operator Permit must complete the Movement Area video in addition to sup-paragraph (1) of this section. The Airport Manager or designee determines the need for the endorsement. The Pass & ID Office administers the Movement Area endorsement. The Airport may require “DM” drivers to complete Movement Area training every six-months.

9. SECURED AREA/AOA MOTOR VEHICLE OPERATOR PERMIT APPLICATION, DESCRIPTION & DISPLAY

A. APPLICATION

To obtain an ID badge and Secured Area/AOA Motor Vehicle Operator Permit at the same time, an individual must complete an MWAA ID Badge/Secured Area/AOA Motor Vehicle Operator Permit Application (Enclosure 2). In addition, the applicant’s employer must complete the appropriate section of the form indicating the need for a Secured Area/AOA Motor Vehicle Operator Permit.
Current ID badge holders who need to obtain a Secured Area/AOA Motor Vehicle Operator Permit only need provide a letter from their company certification official requesting the permit authorization. The badge holder will also need to complete the driver training class and successfully pass the interactive video examination before the driving authorization will be added to his/her ID badge.

B. DESCRIPTION

(1) Permit Designator

The Secured Area/AOA Motor Vehicle Operator Permit is designated on the ID badge by a white “D” (“DM” for Movement Area endorsement) on a red background in a square on the lower right corner of the front face of the ID badge (Enclosure 3).

(2) Expiration Date

The expiration date for the Secured Area/AOA Motor Vehicle Operator Permit coincides with the expiration date of the individual’s ID badge. The permit is renewed at the same time the ID badge is renewed. The permit holder must present a valid state-issued driver’s license to renew his/her permit. If any Secured Area/AOA violation points have accumulated on the permit holder’s record in the previous year, the permit holder must attend the Secured Area/AOA Driver Training Class prior to the issuance of a renewed permit. If the permit expires, the permit holder must reapply for the permit in accordance with the initial issuance requirements stated above.

C. DISPLAY

Airport security regulations require that each individual must display his/her ID badge with the picture right side up, readily visible between the neck and waist, on the outermost garment at all times while in the security-controlled areas. Because the Secured Area/AOA Motor Vehicle Operator Permit appears on the ID badge, drivers always have the permit on display while driving on the Secured Area/AOA.

10. SECURED AREA/AOA MOTOR VEHICLE IDENTIFICATION & REQUIREMENTS

A. AIRFIELD REGISTRATION

All unescorted vehicles operating in the security-controlled areas of the airport must be registered, as indicated by a decal affixed to the driver’s side front bumper of the vehicle (Enclosure 4). Prior to the initial registration all vehicles must pass a safety inspection, which shall be performed by an Airport Operations Duty Manager. All vehicles operated on the Secured Area/AOA must be covered by the insurance requirements listed below (at minimum). Vehicle owners must be able to provide proof of such insurance if requested by Airport Operations.
Airfield vehicle registrations are valid for two years, with the exception of fuel trucks whose registration is valid for only one year, or until the tenant leaves the airport, whichever is sooner. If an airfield registration expires, the tenant may request a renewal following a re-inspection of the vehicle.

(1) Vehicle Insurance

Prior to the initial vehicle inspection, the company representative must provide proof of motor vehicle insurance. The insurance must be maintained for the duration of the vehicle’s use in the security-controlled areas of the airport with the Airports Authority listed as an additional insured. The following are the minimum insurance coverage amounts required:

- **Personal Injury**: $500,000 each person
  $1,000,000 each occurrence
- **Property Damage**: $5,000,000 each occurrence

All tenant managers with AOA-registered vehicles are responsible for notifying Airport Operations if any vehicle is permanently removed from service or if a decal is unreadable due to damage.

(2) Vehicle Inspection

To receive permanent airfield registration, a vehicle must first pass a comprehensive safety inspection based on the Vehicle Inspection Checklist (Enclosure 5). Vehicles are inspected on the Terminal A ramp near the Airport Operations office unless other arrangements are approved in advance. Vehicles that successfully pass the inspection shall be registered by Airport Operations and have a numbered decal affixed to the driver’s side front bumper.

All vehicles authorized to operate in the Secured Area/AOA are subject to random inspections by Airport Operations Duty Managers and the Airport Police. Operators of vehicles found to be deficient may be issued a citation (Notice of Violation) and the vehicle will have its Secured Area/AOA decal removed. The vehicle must be successfully re-inspected by an Airport Operations Duty Manager before a new decal will be issued.

B. VEHICLE MARKINGS

Vehicles authorized to operate in the security-controlled areas of the airport are required to display a unique number comprised of the company’s identifying initials and a sequential non-repeating number. The number must appear on the sides and roof of the vehicle. The markings may be painted, a stenciled decal or a magnetic sign. The side markings must be a minimum of 8 inches high. The roof markings must be a minimum of 12 inches high and should be applied so as to be read when looking at the front of the vehicle from the outside. The color of the markings should be in sharp color contrast to the rest of the vehicle.
Unmarked Airport Management, Airport Operations and Public Safety vehicles are exempt from the requirements of this section.

C. VEHICLE COLORS

(1) Aircraft Rescue and Firefighting (ARFF) Vehicles
   (a) ARFF response vehicles and equipment are lime green.
   (b) ARFF command vehicles are white.

(2) Airport Maintenance Vehicles
   Airport maintenance vehicles are chrome yellow.

(3) Other Vehicles
   Aircraft support, Airport Operations, Airport Police and other vehicles may be any color or combination of colors other than lime green or chrome yellow.

D. VEHICLE LIGHTING

(1) ARFF Vehicles
   ARFF vehicles must have red, or combination red and white, flashing beacons or light bars.

(2) Airport Management and Airport Operations Vehicles
   Airport Management and Airport Operations vehicles must have a yellow flashing beacon, used during normal operations and a red, or combination red and white, flashing beacons or light bar to be used during emergency situations.

(3) Airports Authority Police Vehicles
   (a) Marked Airports Authority Police vehicles must have blue, or combination blue and red, flashing beacons or light bars.
   (b) Unmarked Airports Authority Police vehicles may have yellow beacons that may be magnetically mounted to the roof of the vehicle when needed.

(4) Airport Maintenance Vehicles
   Airport maintenance vehicles must have yellow flashing beacons.
(5) **Aircraft Support and Other Vehicles**

Aircraft support and other vehicles with a height of five feet or more and all sedans and station wagons must be equipped with one of the following types of lights:

(a) U.S. Department of Transportation, Federal Highway Administration (DOT-FHA) motor carrier safety regulation clearance lights mounted in accordance with DOT-FHA requirements, or

(b) A single non-flashing 360-degree yellow light that is a minimum of 4 inches high and 2 ½ inches in diameter. The yellow light should be removed, covered or turned off if the vehicle is operated outside of the Secured Area/AOA.

(6) **Exceptions**

Certain U.S. Government and Airports Authority official vehicles are exempt from the vehicle lighting requirements.

11. **SECURED AREA/AOA MOTOR VEHICLE EQUIPMENT AND PROCEDURES**

A. **VEHICLE SAFETY EQUIPMENT AND PROCEDURES**

(1) **Safety Equipment**

Each vehicle operating in the Secured Area/AOA must have the following equipment on board at all times unless the equipment is specified only for a specific class of vehicle:

(a) All vehicles must be equipped with at least one 5-pound carbon dioxide or dry chemical fire extinguisher. Carbon Tetrachloride, Chlorobromomethene or other vaporizing liquid extinguishers are not permitted. Vehicles used for fueling operations must meet specific requirements for fire safety regulations.

(b) Vehicle tires must be in good condition. Grooved tires must have a minimum depth of 1/8 inch. Tires with fabric or steel in direct contact with the road surface or with sidewall cracks are not acceptable.

(c) Mufflers and exhaust lines must be of rigid construction with either screw flange or sleeve and clamp type joints, and must be free of holes. The exhaust end of the tailpipe must extend parallel to and be at least 18 inches from the ground on all fuelers and defuelers.
(d) All towing vehicles must be equipped with positive locking couplings.

(e) Sediment bowls, fuel pump bowls and carburetor float chambers must be made of metal.

(f) All lubricating oil-, fuel- or alcohol-dispensing nozzles must be of the “dead man” type to prevent the flow of product unless they are manually operated. Devices that permit the automatic flow of fuel are prohibited.

(g) Vehicles that are not equipped with dimmer switches for headlights must have the headlights focused to strike the ground 50 feet or less ahead of the vehicle.

(h) All vehicles with a chassis that would require licensing to operate on Virginia highways will have two operating taillights, brake lights and turn signals.

(i) Truck cab floors and steps must be covered with a non-skid mat or coated with non-skid paint.

(j) Emergency brakes must be capable of holding the vehicle when the transmission is placed in “drive” with the motor running.

(k) All windows and windshields of the vehicle must be free of cracks, blisters, discoloration or any other defects that cause distortion. In addition, the windows must be free of obstructions that block the vision of the operator.

(l) Vehicles, if so equipped, must have windshield wipers, horns and speedometers in working condition.

(m) All baggage tugs, forklifts and other small ramp vehicles must have at least one operating taillight.

(n) Baggage carts must be equipped with reflectors and have at least one 3-inch strip of reflective tape, a reflective company insignia or reflective paint across the front and rear panels.

(2) Safety Procedures

(a) Each driver is required to perform a safety check of his/her vehicle before commencing any operation on the Secured Area/AOA.

(b) All push-back vehicles must have the headlights illuminated prior to moving any aircraft.
(c) Persons operating motor vehicles on the Secured Area/AOA will keep the beacon, headlights and taillights fully illuminated between the hours of sunset and sunrise and during inclement weather.

(d) If a motor vehicle becomes stalled on the AOA between the hours of sunset and sunrise, or during inclement weather, the parking lights must be illuminated or warning lights must be placed on the ground around the vehicle. Airport Operations must be notified immediately and the vehicle must be removed as soon as possible.

(e) Smoking is prohibited inside any vehicle on the Secured Area/AOA.

(f) Smoking is prohibited at all times in fuel trucks and hydrant fueling equipment. A “No Smoking” sign must be prominently posted in the cab or every aircraft fuel-servicing vehicle. Smoking equipment, such as cigarette lighters and ashtrays, must be removed from all such equipment.

(g) Pictures, stickers, signs or other objects on the windows of a motor vehicle operating on the Secured Area/AOA, other than those required by state law or airport regulation, are prohibited.

(h) Motor vehicles shall not be operated when the front, side or rear vision is obstructed by baggage, boxes or other items being transported.

(i) If the vision of a driver is restricted in any way, operation of the vehicle is prohibited unless a guide is positioned outside the vehicle to assist the operator.

(j) During aircraft arrival and departure operations, all airline ground handlers are required to have wing walkers wearing a reflecting jacket and carrying illuminated or reflective batons.

(k) All motor vehicles operating on the Secured Area/AOA shall be equipped with at least one mirror adjusted so that the driver has a clear view of at least 200 feet to the rear. Special service vehicles, not licensed for general highway use, with a cab that provides the driver with unobstructed 360-degree visibility are exempt from this requirement.

(l) Any vehicle leaking lubricating oil, fuel, alcohol, antifreeze, lavatory water or any other fluid is not allowed to operate on the Secured Area/AOA.
(m) All vehicle operators in the Secured Area/AOA, who handle, store, dispense or use hazardous materials must be familiar with their organization’s “Spill Control Plan” and all federal, state and Airports Authority hazardous materials requirements and practices.

(n) If a spill of fuel or other hazardous material occurs, the vehicle operator shall immediately attempt to control or stop the release of the fuel or hazardous material from the vehicle.

(o) Any hazardous materials release or fuel spill, regardless of quantity, must be immediately reported to the Airports Authority Fire Department and to Airport Operations. The owner of the vehicle involved shall complete the MWAA Spill Notification Checklist (Enclosure 6) and forward it to the National Environmental Staff within 24 hours of a spill.

(p) The following actions are prohibited by drivers and passengers of vehicles operating on the Secured Area/AOA: to stand up in or on the vehicle while it is in motion; to ride on any part of the vehicle not equipped with a proper seat for passengers; or, to ride with any arms or legs protruding from the moving vehicle.

(q) Cargo containers shall be placed on dollies lengthwise so that the width of the container does not extend beyond the width of the dolly or tug.

(r) The operation of any 2-wheeled vehicle on the Secured Area/AOA is prohibited unless the Airport Manager has granted special written permission.

(s) With the exception of persons authorized by the Airport Manager, the carriage of firearms in any vehicle on the Secured Area/AOA is prohibited.

(t) Equipment that is used to tow, push or lift should not be used beyond its design limits.

(u) Each vehicle must be placed in “park” with the parking brake set and the engine turned off whenever the driver of the vehicle is not in the driver’s seat to immediately control the vehicle.

(v) Vehicles or equipment with expired inspection decals, or in an otherwise inoperable condition, must be removed from the Secured Area/AOA as soon as possible. Such vehicles must be repaired and re-inspected prior to being operated on the Secured Area/AOA again.
B. VEHICLE OPERATING PROCEDURES

(1) General

(a) Each driver must ensure that his/her vehicle is in good operating condition, free from excessive damage or rust that could produce FOD, and not producing excessive smoke prior to driving the vehicle on the Secured Area/AOA.

(b) Each driver must follow all instructions, rules and regulations pertaining to the operation of motor vehicles on the Secured Area/AOA.

(c) Vehicle operations must be conducted in a safe manner. Drivers are responsible for reducing driving speed when the pavement is icy or wet or during hours of darkness.

(d) Unless otherwise posted, vehicles approaching one another will pass left side to left side.

(e) Headlight beams must be lowered in vehicles equipped with dimming devices when approaching vehicles or aircraft during hours of darkness or inclement weather.

(f) No personal music devices (ipod, etc.) will be used while operating a vehicle on the Secured Area/AOA.

(g) No texting allowed while operating a vehicle on the Secured Area/AOA.

(h) Each driver on the Secured Area/AOA must remain in compliance with all restrictions identified on his/her state driver’s license, such as wearing of eyeglasses or hearing aids.

(i) Motor Vehicle Operator Permits issued by airports other than Ronald Reagan Washington National Airport or Washington Dulles International Airport for purple badges, are not valid at National.

(2) Speed Limits

(a) The speed limit on Secured Area/AOA vehicle roadways is 15 miles per hour.

(b) The speed limit for any area outside of the vehicle lanes, to include the aircraft ramps and baggage tunnels, within the Secured Area/AOA is 6 miles per hour.
(c) Emergency vehicles (i.e., Airports Authority Police, Fire and Airport Operations) that are responding to an emergency with lights and sirens activated are exempt from the designated speed limits.

(3) Right of Way

(a) Drivers must yield the right of way to Fire, Police and Airport Operations vehicles that have lights and sirens activated.

(b) Drivers must yield the right of way to any aircraft with the engine(s) running, any aircraft under tow, or any pushback tug crossing the vehicle lane to return to the gate area from Taxiway K.

(c) In all areas of the Secured Area/AOA, the driver approaching an intersection from the right will have the right of way unless otherwise directed by posted signs.

(4) Gate Areas

(a) No vehicle operator shall drive across passenger loading lanes while an aircraft is in a gate position and passenger loading or unloading operations are under way.

(b) Any driver operating on ramp areas shall drive in the vehicle lane until they are abeam the intended destination. Once at the destination, the driver shall carefully turn at an angle close to 90 degrees to enter the desired area. Drivers shall not cut across gate areas rather than use the designated vehicle lane.

(c) Vehicles shall never be driven under the moveable portion of a passenger loading bridge.

(d) Operators of vehicles including airline’s contractors may drive under the fixed portion of a passenger loading bridge providing the airline’s policy allows this practice.

(5) Baggage Carts

(a) Riding on baggage carts, trailer hitches, fenders or on any portion of a vehicle not equipped with proper seats is prohibited.

(b) The length of a baggage cart and/or dolly train under tow shall not exceed 60 feet or 4 cart/dolly units.
(c) Baggage carts or vehicles must not be left standing in roadways or taxiways at any time.

(d) Tugs, trailers, baggage carts or cargo carts must be returned to an assigned storage area and parked with the parking brake set immediately following their use.

(e) The excessive use of horns in the baggage makeup area or baggage concourses is prohibited.

(f) Drivers of baggage carts shall shut down the engine of the vehicle whenever stopped in the baggage concourse for longer than 30 seconds.

(6) Aircraft Service Vehicles

(a) Aircraft service vehicles assigned to a specific aircraft at the gate is the only vehicles that may pass within 20 feet of that aircraft.

(b) No aircraft servicing may be conducted until the aircraft has come to a complete stop at its designated parking position.

(c) When approaching an aircraft for servicing, operators of service vehicles shall stop 20 feet from the aircraft, and then slowly approach aircraft.

(7) Traffic Signals and Signs

(a) Vehicle operators are required to obey all posted regulatory signs and traffic signals.

(b) Vehicles entering or exiting the baggage tunnel must come to a complete stop to allow the mega-door time to fully open before proceeding.

C. VEHICLE PARKING PROCEDURES

Vehicles may only be parked in designated vehicle parking areas that are outlined in white. Vehicles shall never be left unattended while the engine is running. Vehicles shall never be parked inside the aircraft footprint, which is designated by red and white lines painted on the pavement. Parking within 15 feet of a fire hydrant, fire bottle, fire extinguisher or in a designated fire lane is prohibited. Parking within 250 feet of the edge of a runway is prohibited. All parked vehicles must have the emergency brake set. Vehicles parked in violation of these rules may be towed without notice and at the owner’s expense.
D. ESCORT PROCEDURES

All unregistered vehicles must be escorted while on the Secured Area/AOA by a vehicle with a valid airfield registration/inspection decal. A maximum of 3 vehicles may be escorted by one registered, lead vehicle and one end vehicle. Escorting two vehicles can be done with one registered vehicle. The escorting vehicle(s) must remain with the unregistered vehicle(s) at all times and must escort the unregistered vehicle(s) from the Secured Area/AOA at the appropriate time. The operator of each unregistered vehicle must have a valid state driver’s license in his/her possession while on the Secured Area/AOA.

E. CONTRACTOR PROCEDURES

In addition to the requirements identified above, contractors must watch the Movement Area Video and adhere to the following additional procedures:

- Construction vehicles and equipment must use only designated entrances, exits and haul routes on the Secured Area/AOA.

- Construction vehicles and equipment may only enter and exit the Secured Area/AOA during contractually specified times.

- A maximum of 3 dump trucks (5 during snow operations) must be escorted onto the Secured Area/AOA by one lead escort vehicle and one end vehicle.

- An escort vehicle may escort only one tractor-trailer on the Secured Area/AOA at a time.

- Concrete mixer chutes must be retracted to a single chute while the truck is in motion on the Secured Area/AOA.

- Forklift forks must be raised no less than 6 inches and no more than 12 inches from the ground and covered or protected by an approved pallet when proceeding from one point on the Secured Area/AOA to another.

- When not in use, all construction vehicles and equipment must be removed from work sites in the Secured Area/AOA unless the Airport Manager grants written authorization otherwise. If written authorization is received, the vehicles and equipment must be marked, lighted and parked in a designated area.

- Construction vehicles and equipment operating in the movement area (runways and taxiways) must have capability for 2-way radio contact with the ATC Tower or must be escorted by a vehicle that has such ability.
• Contractors must have sweepers on hand to clean up any debris resulting from the movement of construction vehicles and equipment traversing the Secured Area/AOA.

12. VEHICLE REPAIRS

With the exception of emergency repairs necessary to immediately move vehicles or equipment to a repair facility, vehicle repairs to include cleaning, maintaining or overhauling are not allowed on the Secured Area/AOA. If it is not possible to repair and move a vehicle immediately, the driver must call Airport Operations for assistance in having the vehicle towed. Vehicles will be towed at the owner’s expense. When emergency repairs are being performed on a vehicle with the engine running, an additional person must be seated in the driver’s position.

13. SECURITY REQUIREMENTS FOR VEHICLES

Operators of all vehicles entering the Secured Area/AOA through mechanical access gates must stop after safely clearing the gate and remain stopped there until the security gate returns to a closed, locked position. If the gate does not close, the driver must notify Airport Operations and remain at the gate until maintenance personnel arrive at the gate.

14. DRIVING UNDER THE INFLUENCE

Driving under the influence (DUI) of alcohol or any other substance, legal or otherwise, that impairs vision, judgment or reflexes, is absolutely prohibited. A blood alcohol or breath test need not be administered to support a DUI charge. DUI charges may be proven based solely on observation of the enforcing official.

15. ENFORCEMENT

The Airport Manager, Airport Operations Manager, Airport Operations Duty Manager, and the Airport Police are all authorized to enforce the airport vehicle rules and regulations.

A. NOTICES OF VIOLATION

Upon issuance of a Notice of Violation (Enclosure 7), a copy will be provided to the individual charged with the violation, with duplicates sent to the Airport Operations Department and the employee’s tenant manager. The driver’s signature is required to acknowledge receipt of a notice of violation. The signature is not an admission of guilt. Refusal to sign the Notice of Violation may result in immediate suspension of Secured Area/AOA driving privileges.
B. POINT SYSTEM

There is a point system for violations of airport rules and regulations. Points are accumulated over a 12-month period from the date the ID badge and motor vehicle operator permit is issued or renewed. Although points accumulate over a 12-month period, the record of offenses committed by a driver will be maintained for a period of 2 years. The points assessed for violations relating to the operation of motor vehicles on the Secured Area/AOA are as follows:

- Loaning a Secured Area/AOA operator’s permit/ID Badge: 12 points
- Altering or forging a Secured Area/AOA operator’s permit/ID Badge: 12 points
- Leaving the scene of an accident with personal injury: 12 points
- Operating under suspension/revocation of a state driver’s license: 12 points
- Driving under the influence (DUI): 12 points
- Movement Area Driving Violation (Runway/Taxiway Incursion): 8 points
- Reckless driving: 8 points
- Leaving the scene of an accident with no personal injury: 8 points
- Finding of being at fault in an accident: 8 points
- Failure to report an accident to Airport Operations or Airport Police: 6 points
- Operating without the proper class of permit: 5 points
- Operating a vehicle on the Secured Area/AOA without an inspection decal: 3 points
- Failure to yield right of way: 3 points
- Speeding: 3 points
- Failure to obey a sign, signal or instruction: 3 points
- Operating a vehicle without a state driver’s license in driver’s possession: 3 points
- Operating a vehicle without Secured Area/AOA permit in driver’s possession: 3 points
- Improper vehicle markings: 3 points
- Illegal parking on the Secured Area/AOA: 1 point

Appropriate points will be assessed for miscellaneous violations not listed above. If multiple offenses have been committed at the same time, points shall be assessed on all charges.

C. ENFORCEMENT PROCEDURES

(1) Points Accumulation

(a) If a driver accumulates 3 points on his/her record, a notification letter will be sent from Airport Operations to the tenant manager.

(b) Any vehicle operator who accumulates 5-7 points shall be required to meet with the Airport Operations Manager (or designee) to review the individual’s driving record. The driver must attend the Secured Area/AOA driver training and successfully pass the interactive video exam with a passing score of 100 percent.
(c) A driver who accumulates 8-11 points shall have his/her Secured Area/AOA motor vehicle operator permit suspended. The driver must attend the Secured Area/AOA driver training and successfully pass the interactive video exam with a passing score of 100 percent.

(d) A vehicle operator who accumulates 12 or more points in one year shall have his/her Secured Area/AOA Motor Vehicle Operator Permit permanently revoked.

A driver may be directed to re-attend driver training and successfully re-take the examination regardless of the points accumulated should the committed offense warrant such action. Drivers who have accumulated any points during the 12-month period will be required to re-attend driver training and successfully retake the interactive video examination prior to the renewal of his/her Secured Area/AOA Motor Vehicle Operator Permit/ID badge.

(2) Suspension and Revocation

(a) Suspension

If a vehicle operator accumulates 8-11 points on his/her driving record, a Notice of Suspension will be hand delivered or sent by certified mail to the individual. A copy will be sent to the individual’s employer. The individual and his/her supervisor will be required to meet with the Airport Operations Manager (or designee) to discuss the suspension. The duration of an initial suspension is 1 to 30 days. Subsequent suspensions are 15 to 90 days.

If a vehicle operator or pedestrian causes a runway or taxiway incursion, this immediately generates an 8 point infraction. In addition to the paragraph above, a Letter of Reprimand will be administered with possible suspension of the employee’s Airport issued ID badge and/or employment of up to 5 days based on the severity of the actual incursion. The employee must retake and pass all elements of the Secured Area/AOA Motor Vehicle Operator Permit test. Also, a “hands on” practical test of AOA and Movement Area driving skills will be administered by Airport Operations and must be passed to restore airfield driving privileges.

If a vehicle operator or pedestrian causes a repeat runway/taxiway incursion the following will occur:

- A suspension or revocation of airfield driving privileges.
- Suspension of the employee’s ID badge and/or employment of up to 30 days based on the severity of the actual incursion.
The Airport Operations Manager or an Airport Operations Duty Manager may suspend an operator’s permit immediately and without prior notice if there is an imminent substantial threat to public safety or deliberate impeding of the operation of the airport.

(b) Revocation

If a vehicle operator accumulates 12 or more points in a given year, a Notice of Revocation will be hand delivered or sent by certified mail to the individual. A copy will also be sent to the individual’s employer. The individual and his/her supervisor will be required to meet with the Airport Operations Manager (or designee) to discuss the revocation and appeals process.

(3) Appeal Hearings

Notices of Violation, Suspension or Revocation may be appealed to the Airport Manager. The driver must submit a written request for a hearing to the Airport Manager within 72 hours of receipt of the notice. A copy of the request must also be sent to the Airport Operations Manager. The Airport Manager (or designee) will conduct a hearing within 10 calendar days of receipt of the request for a hearing. A decision will be issued within 10 calendar days of the date of the hearing. When the request for a hearing is received, the Airport Operations Manager will delay the suspension or revocation until after the hearing, unless it appears that substantial harm could result if the suspension or revocation was not made immediately.

16. ACCIDENTS ON THE SECURED AREA/AOA

If an accident occurs on the Secured Area/AOA, the operator(s) shall remain with the vehicle(s) at the location of the accident and call Airport Police and Airport Operations immediately. Neither the driver(s) nor the vehicle(s) involved shall leave the scene of the accident until released by the investigating Airport Police Officer.

If an accident occurs on the Secured Area/AOA, the owner of the vehicle, not the driver, must send a written report of the accident to the Airport Operations Manager. The report must include the following information:

- The names and addresses of the individuals involved
- A description of the property or vehicles involved
- The registration and license numbers of the vehicles involved
- A description of the property damage
- A description of any injuries
- The names of any witnesses
• A statement of how the accident could have been prevented
• An explanation of any mitigating circumstances

17. EMERGENCY SITUATIONS

During emergency situations, Airport Operations may limit access to the scene and adjacent areas. Only those individuals and vehicles that are directly involved in the response and recovery efforts will be allowed into the designated incident area.

If there are any questions regarding this O&I, please contact Airport Operations at (703) 417-8050. Additional copies of this O&I may be obtained from the “Tenant Info” section of the MWAA website www.mwaa.com.

J. Paul Malandrino, Jr.
Airport Manager
Ronald Reagan Washington National Airport

Enclosures

1. DCA Airfield Layout Plan
2. ID Badge/Secured Area/AOA Motor Vehicle Operator Permit Application Form
3. Illustration of DCA ID Badge
4. Illustration of DCA vehicle registration/inspection decals
5. Vehicle Inspection Checklist
6. MWAA Spill Notification Checklist
7. Notice of Violation
APPENDIX 12

IAD VEHICLE AOA REQUIREMENTS
1. VEHICLE REGISTRATION PROCEDURES

a. Permanent Airfield Registration

(1) Airport tenants may obtain temporary or permanent airfield registration through vehicle registration, inspection, and decal issuance. This process is conducted on a first come, first served basis at the vehicle inspection station on Monday through Friday from 7:30am – 2:30pm. You do not need an appointment.

(2) Prior to registration, each vehicle shall be required to pass a safety inspection and provide proof of insurance. The insurance must list the Metropolitan Washington Airports Authority as “additional insured” in respect to all policies except worker’s compensation and employer’s liability. The safety inspection is conducted at the Inspection Station using the checklist on page 3. Items that have failed inspection must be corrected before registration.

(3) In addition, proof of motor vehicle insurance in at least the following amounts is required:

(a) Personal Injury - $500,000 each person, $1,000,000 each occurrence
(b) Property Damage - $1,000,000 each occurrence

(4) Vehicles satisfactorily completing the inspection will be registered with the Safety and Security office and assigned a numbered decal to be affixed to the left front portion of the vehicle.

(5) All tenant managers with registered vehicles must notify the Safety and Security office of any vehicle: (a) permanently removed from service or (b) with a decal that is damaged beyond readability, so that the vehicle registration can be voided/updated.
2. **VEHICLE REQUIREMENTS**

b. Identification. For the purpose of rapid identification, each vehicle authorized to operate on the airfield shall display on each side and on the roof (or the hoods of vehicles without roofs) three letter identifying initials with an identifying number immediately adjacent. These markings shall be:

(1) Painted on the vehicle
(2) Be a stenciled decal, or
(3) A magnetic sign

The side markings shall be a minimum of eight inches (8") in height and installed in any easily visible location. The roof (or hood) markings shall be a minimum of twelve inches (12") in height and shall be installed to be read when looking from front to rear of the vehicle. All identifying markings shall be in sharp color contrast to the rest of the vehicle. **To ensure that a specific three-letter identifier is available, please contact the Safety and Security office at (703) 572-2740 prior to installing markings on your vehicle(s).**

c. Special Lighting.

(5) Aircraft Support Vehicles and other vehicles five feet (5’) in height or over, and all sedans and station wagons shall be equipped with Department of Transportation, Federal Highway Administration (DOT-FHWA), motor carrier safety regulation type clearance lights mounted in accordance with DOT-FHWA requirements. If the configuration of a vehicle is such that DOT-FHWA type clearance lights cannot be installed, a single non-flashing 360-degree amber light may be used. This light shall be a minimum of four inches (4") high, two and one half inches (2 ½") in diameter, and of at least 50 candlepower. If the vehicle involved is to be operated off the airfield, the amber light may be a removable type, which must be covered or removed when the vehicle is operating off the airfield.

(6) Flashing or blinking lights are prohibited unless specifically authorized by the Airport Manager.
IAD O&I 3-2-2A
Airfield Vehicle Control Program

3. **VEHICLE SAFETY EQUIPMENT**

c. Fire Extinguisher. Each airfield approved vehicle shall be equipped with at least one *five pound* carbon dioxide or dry chemical extinguisher.

d. Tires shall be in serviceable condition. Grooved tires must have a minimum depth of 1/16 of an inch as specified by Virginia Code and tires with fabric or steel in direct contact with the road surface and/or with sidewall breaks are prohibited.

e. Mufflers and exhaust lines shall be of rigid construction with all joints of either screw flange, or sleeve and clamp type, and free of holes. The exhaust end of the tailpipe shall extend parallel to and at least 18 inches (18”) from the ground on all fuelers and defuelers.

f. Sediment bowls, fuel pump bowls, and carburetor float chambers shall be made of metal

g. All lubricating oil, fuel, or alcohol dispensing nozzles shall be designed to prevent flow of product unless manually operated. Devices that permit the automatic flow of fuel are prohibited.

h. For all vehicles that are not equipped with dimmer switches for headlights, headlights must be focused to strike the ground no more than 50 feet (50’) ahead of the vehicle.

i. All vehicles with a type chassis that normally would be required to be licensed to operate of Virginia highways shall have two operating taillights, stoplights, and appropriate turn signals.

j. Cab floors and steps shall be covered with a non-skid mat or coated with non-skid paint.

k. Emergency brakes must be capable of holding the vehicle when placed in drive with the motor running and only the emergency brake engaged.

l. Windshields, rear glass, and side glass must be clear and unbroken.

m. Vehicles so equipped shall have windshield wipers, horns, and speedometers in operating condition.

n. All Baggage tugs and small, specialized ramp vehicles must have at least one operating taillight

o. Baggage carts must be equipped with reflectors and have at least on three-inch strip of reflective tape or paint across the front and rear panels. A reflective company insignia will be acceptable.
Washington Dulles International Airport
Vehicle Maintenance Facility East
**Vehicle Inspection Station**
Hours of operation: M-F, 7:30 AM - 2:30 PM
**ACORD™ CERTIFICATE OF LIABILITY INSURANCE**

**PRODUCER**
Your Insurer

**INSURED**
Your Company Name & Address

**INSURERS AFFORDING COVERAGE**

**NAIC #**

**COVERAGES**

The policies of insurance listed below have been issued to the insured named above for the policy period indicated. Notwithstanding any requirement, term or condition of any contract or other document with respect to which this certificate may be issued or may pertain, the insurance afforded by the policies described herein is subject to all the terms, exclusions and conditions of such policies. Aggregate limits shown may have been reduced by paid claims.

<table>
<thead>
<tr>
<th>INSURER</th>
<th>A (e.g., Premiums)</th>
<th>B (e.g., General Aggregate)</th>
<th>C (e.g., Products - Comp/Op Agg)</th>
<th>D (e.g., Personal &amp; Adv Injury)</th>
<th>E (e.g., General Aggregate)</th>
<th>F (e.g., Bodily Injury)</th>
<th>G (e.g., Premises &amp; Torts)</th>
<th>H (e.g., Med Exp)</th>
<th>I (e.g., Occurrence)</th>
<th>J (e.g., Aggregate)</th>
<th>K (e.g., Each Person)</th>
<th>L (e.g., Premises &amp; Torts)</th>
<th>M (e.g., Each Incident)</th>
<th>N (e.g., Premises &amp; Torts)</th>
<th>O (e.g., Premises &amp; Torts)</th>
<th>P (e.g., Premises &amp; Torts)</th>
<th>Q (e.g., Premises &amp; Torts)</th>
<th>R (e.g., Premises &amp; Torts)</th>
<th>S (e.g., Premises &amp; Torts)</th>
<th>T (e.g., Premises &amp; Torts)</th>
<th>U (e.g., Premises &amp; Torts)</th>
<th>V (e.g., Premises &amp; Torts)</th>
<th>W (e.g., Premises &amp; Torts)</th>
<th>X (e.g., Premises &amp; Torts)</th>
<th>Y (e.g., Premises &amp; Torts)</th>
<th>Z (e.g., Premises &amp; Torts)</th>
</tr>
</thead>
</table>

**GENERAL LIABILITY**

- Commercial General Liability
  - Claims Made: 
  - Occur: 

**AUTOMOBILE LIABILITY**

- Any Auto
- All Owned Autos
- Scheduled Autos
- Hired Autos
- Non-Owned Autos

**GARAGE LIABILITY**

- Any Auto

**EXCESS/UMBRELLA LIABILITY**

- Occur: 
- Claims Made: 

**WORKERS COMPENSATION AND EMPLOYERS’ LIABILITY**

- Any Proprietor/Partner/Executive Officer/Member Excluded?
  - Yes: 
  - No: 

**OTHER**

- Special Provisions

**DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES / EXCLUSIONS ADDED BY ENDORSEMENT / SPECIAL PROVISIONS**

Additional Insured - Metropolitan Washington Airports Authority

**CERTIFICATE HOLDER**

**CANCELLATION**

Should any of the above described policies be cancelled before the expiration date thereof, the issuing insurer will endeavor to mail _______ days written notice to the certificate holder named to the left, but failure to do so shall impose no obligation or liability of any kind upon the insurer, its agents or representatives.

Authorized Representative

© ACORD CORPORATION 1988
Understanding the Acord Certificate of Insurance

Certificates of insurance are provided to verify the existence of coverage and determine whether the existing coverage limits are adequate and meet contract requirements. When obtaining a certificate of insurance, the recipient of the form should verify the insurance with a well-established, legal entity with a permanent address, telephone number and business license where required.

The certificate is issued as a matter of information only and confers no rights upon the certificate holder. The certificate does not amend, extend or alter the coverage afforded by the policy(ies) listed. If the recipient of the form has a verifiable interest in the policy, such as an additional insured, the policy must be amended by endorsement to provide the appropriate coverage.

| QUESTIONS: |
| OCWIP Participants: (703) 572-6792 |
| All Others: (703) 572-2740 |