NORFOLK AIRPORT AUTHORITY

REQUEST FOR PROPOSALS

FOR

IDENTITY MANAGEMENT SYSTEMS

RFP ISSUE DATE:	**January 17, 2024**
Questions Due By:	**January 31, 2024 (by 2:00 PM EST)**
Proposal Due Date:	**February 20, 2024 (by 2:00 PM EST)**
Vendor Demonstrations (if required):	**March 5 and 6, 2024.**
Contract Award Date:	**May 1, 2024**

Contents

SECTION 1.0

1.1 INTRODUCTION

Norfolk International Airport (ORF) is soliciting responses to this Request for Proposal (RFP) from qualified firms for a comprehensive and automated Identity Management System (IDMS) at the Norfolk International Airport ("Airport" or "ORF").

The received proposals will be utilized to select and award the contract to One (1) Contractor who is experienced in the deployment of an Identity Management System (IDMS) at US Airports. All submissions received prior to the submission deadline which meet the minimum requirements will be evaluated by the evaluation committee at Norfolk International Airport (ORF). At the Airport's discretion, a select group of shortlisted Contractors will be asked to provide a demonstration of their product. Those submissions not selected will be eliminated from further consideration.

1.2 OBJECTIVE

Norfolk International Airport (ORF) primary objectives for seeking an automated Identity Management System (IDMS) are:

- reduce manual, time consuming, error prone, and duplicate data entry in multiple standalone systems and excel sheets.
- improve customer service; and achieve paperless process.
- enforce business rules for badge issuance.
- comply with the Transportation Security Administration (TSA) regulations and Security Directives (SD).
- provide data integrity and security for the airport employee's information.

1.3 BACKGROUND

There are approximately 2,500 active badged airport employees and approximately 180 Authorized Signatories (AS). The Airport employees and AS represent airport employees, airline, tenants, contractors, vendors, concessionaires, and government (local, state, and federal) agencies at ORF. The Airport Badging Office handles approximately 10-12 transactions per day. These transactions include processing new and renewal applicants, fingerprinting, and issuing replacement badges.

The current process entails paper application forms (filled by the employee / badge applicant, reviewed, and signed by the AS) to be then entered by the badging office staff in multiple systems that provide specific functions for background checks, training, financial (Point of Sale and receipt printer) and access control.

1.4 SCOPE

The scope of this project includes the procurement, configuration, installation, support & maintenance of a new IDMS for ORF. The proposed solution will be configured and installed on the ORF environment provisioned for use by ORF.

Significant coordination with IT, Security and other Airport departments will be required to further define current software versions, configuration limitations, project phasing and training. This solution will be configured in a test environment and then rolled into the production environment. Environments are defined later in this document.

Existing Business Process: The Contractor will refer to the existing business processes for standard systems and specialized system interfaces, badging office setup, badge types and privileges in **Attachment A** of this document.

Future (Proposed) Business Process: The Contractor will refer to the future (proposed) business processes, system architecture and badging office setup in **Attachment B** of this document.

Functional and Technical Requirements: The Contractor will respond to all the functional and technical requirements identified in **Attachment C & D** of this document. Requirements left blank or with no responses will be considered a non-compliant response.

1.4.1 ENVIRONMENTS

ORF will provide the server, server operating system, SQL server, workstations, network infrastructure and badge stock. The Contractor will provide the software and hardware required for successful IDMS implementation. The Contractor will provide detailed server and network requirements based on the minimum specifications and quantities.

Environment Name	Description
Testing and Training (Pre-production)	1) Development environment will host a "working out-of-the-box" IDMS with sample database installed by the IDMS Contractor. 2) ORF will provide a database server for where source data repositories will be made available. The Contractor will use this setup for data analysis, reconciliation reports generation, and data migration activities. The Contractor will run as many iterations as possible of data analysis, reconciliation and data migration required to provide ORF with confidence in migrated data. 3) This environment will be used for system acceptance testing, system performance evaluation, and training. 4) This environment will be a complete replica of the Production system. 5) All hot fixes, patches, upgrades will be applied to this environment to keep in sync with the Production environment.
Production	1) This environment will be the production setup. Changes will be implemented in the Testing and Training Environment first and only after approvals from ORF will the changes be installed in the Production Environment.

1.4.2 IMPLEMENTATION APPROACH

The IDMS implementation is to be performed in a single phase. However, the Contractor may recommend an alternate implementation strategy that will reduce implementation timeframes without compromising the functionality and performance of the expected IDMS, as per the requirements.

Below is a list of Contractor responsibilities, tasks, and deliverables to be included in the project implementation.

1. The Contractor will within thirty (30) days of the Notice to Proceed (NTP) submit for ORF to review the Project Charter to include the following:

    a) Project schedule
    b) Communications Plan should address at a minimum the following topics:
        i. Weekly and monthly project status meetings followed by minutes.
        ii. Monthly executive summary reporting including financial statuses, tasks completed, 30-60 look ahead reporting, project risks and schedule impacts / changes.
        iii. Forms and templates to track ongoing open items, issues, actions, decisions, and statuses.
    c) Change Management Plan should include at a minimum:
        i. Request for Information (RFI) process, form templates, and method to document resolutions.
        ii. Change control process for raising change requests, review and approval methods, form templates, and cost analysis impacts.
    d) Business process workflows, system design and technical documentation
        i. Business process workflows (swim lanes) for handling:
            1. Company onboarding, de-activation, exception scenarios such as name change and mergers.
            2. AS onboarding, off boarding, pre-enrollment, renewals, audits, etc.
            3. Applicant portal functions.
            4. Badge holder pre-enrollment, badge issuance including exceptions such as background checks fails, re-fingerprinting, adjudications, Rapback, etc.
            5. All business rules that are necessary for the functioning of the IDMS.
        ii. System Architecture: Physical and logical design indicating all internal and external systems connectivity for Testing and Training Environment and Production Environment.
        iii. System Software & Hardware Requirements: Server, OS, Database, Network, Firewalls, Workstations, service accounts (server, databases, 3rd party systems), badging equipment including quantities for servers, workstations, and badging peripherals.
        iv. External Systems Interface Control Documents

    e) Data Migration Plan should include:

        i. impact analysis of certain data fields that are mandatory for the normal performance of the IDMS.

        ii. The contractor will submit reports of preliminary analyses from the data repositories identifying missing or incorrect data elements.

        iii. The contractor will recommend the priorities for critical and mandatory data elements that need to be cleaned up by ORF including implications and associated timeline(s) per the project plan. Additionally, the Contractor is to

provide suggestions for clean-up priority for non-critical/ non-mandatory data elements.

iv. The Contractor will perform data migration into the test environment such that the system is test ready.

2. The Contractor will first install and configure the system in the Testing and Training Environment (pre-production) and perform the system acceptance testing and training in this environment.
3. The Contractor will perform readiness testing and submit testing results to:
   a) ensure that the system components meet business and process requirements as established in this RFP,
   b) ensure system software has been configured such that it meets the functional and technical requirements and future business processes as established in this RFP,
   c) ensure system acceptance can commence by the ORF users.
4. The Contractor will provide for the system acceptance testing the following:
   a) Test Plan to include test timeline, staff and equipment resources required.
   b) Test scripts / Test cases: Scenario based and mapped to the Functional Specifications Requirements established.
   c) Online Issue Tracking System: Method to log, identify issues (bug/missing functionality/ not in scope/ other) and track testing results for actions.
5. The Contractor will receive System Acceptance Approval in the Testing and Training Environment from the ORF after all requirements are demonstrated and tested, there are no open items, and ORF has provided explicit acceptance of the system.
6. The Contractor will be required to conduct training for the system users – Trusted Agents, Authorized Signatories, and other Airport users.
7. The Contractor will provide User Manuals – electronic copies (pdfs) and hard copy, bound user manuals for all training sessions. The user manuals and “Help” will be made available within the IDMS application such as Authorized Signatory portal or application portals.
8. The Contractor will be required to perform the implementation and roll out of the system into the Production Environment. The installation in the Production Environment must take place after ORF has approved the System Acceptance Testing.
9. The Contractor will provide an Implementation Plan or Run Book for ORF’s review and approval which will include – step-by-step guide for installation, configuration, database migration, 3rd party integration sequence and production sanity testing details. Each step will include the resource responsible, and time taken for each step. The Contractor will provide details of all the resources required on-site from the Contractor, ORF Security, IT and any 3rd party systems.
10. The Contractor will provide two (2) full time engineering resources familiar with ORF’s implementation and will be on-site for two (2) weeks post go-live for support and system stabilization.
11. The Contractor will provide details, before the IDMS go-live, for ORF’s review and approval, of the maintenance and support system. The details should include the ticketing

system information. The Contractor will train key ORF staff to use the ticketing system that will allow ORF to report and track production issues.

12. There will be a system stabilization period of a minimum of thirty (30) calendar days after the IDMS is working in the Production Environment. During this period, the Contractor will monitor and report system health checks to include - performance metrics, integration or network issues, database growth, or other system (functionality) related issues that impact the badging operations. The Contractor will work with ORF for corrective actions on any of the items identified during this period. The exact start and end date of the stabilization period or if the stabilization period will be reset due to critical issues (as defined in section 1.7 of this document) encountered will be agreed upon with ORF.
13. ORF will provide final system acceptance in Production Environment once all phases are complete. ORF is experiencing beneficial use of the system, and there are no critical open issues. The Warranty period will begin only after ORF has accepted the system in the Production environment.

1.4.3 WARRANTY, SUPPORT AND MAINTENANCE

The Contractor will be responsible for maintaining the software components procured as part of the IDMS contract. The maintenance period is defined in the length of contract section of this document.

For the purposes of this section the “IDMS” represents all components of the software including functionality modules, 3rd party or external integrations, badging equipment hardware and firmware, and any add-on modules installed by the Contractor.

The one (1) year warranty period and subsequent maintenance years for all components (software and hardware) will commence after the Final System Acceptance in Production Environment by ORF.

1. The Contractor will provide a one (1) year manufacturer-based warranty on all components (software and hardware) provided by the Contractor. The Contractor warrants that the IDMS will be free of defects in workmanship and materials for a period consistent with industry standards and the nature of the (“Warranty Period”). The Contractor includes an explanation of the system’s warranty coverage and includes optional extended maintenance agreement\warranty options.
2. The Contractor will develop and submit a maintenance plan required under the IDMS contract. The Contractor will document service levels including, but not limited to, coverage time, maintenance request response time and acceptable system downtime. All software upgrades during the warranty period and subsequent maintenance years will be performed at no additional cost to ORF and will be as part of a maintenance agreement. All system maintenance will be completed in coordination with ORF.
3. After ORF has initiated the warranty and maintenance phase, the Contractor will provide updates, enhancements, and/or bug fixes to all systems at no additional charge during the term of any maintenance/service agreements. All system changes will be conducted in coordination with ORF.
4. The Contractor will provide all (software and hardware) upgrades in the first-year warranty and included in subsequent years as part of maintenance agreements. The Contractor will

provide methods for version and periodic upgrades to support changes in platform operating systems, support applications and security requirements. The Contractor will provide during the warranty period, and any period thereafter, where the IDMS is covered by an annual maintenance agreement, no-charge updates to maintain compliance with CCURE and TSC upgrades.

5. During the warranty period, if the IDMS does not perform in accordance with the Contract, then the Contractor will take such steps as necessary to repair or replace the defective portion at no additional cost to ORF for material and labor. Such warranty service will be provided at the Contractor's expense.
6. If any defect in the IDMS is not rectified by the Contractor before the end of the Warranty Period, the Warranty Period will be extended until, in the opinion of ORF, the defect has been corrected; and the IDMS functions in accordance with the Contract are operational for a reasonable period. Once the defect has been rectified, it is at the sole discretion and option of ORF to request that the acceptance testing for the IDMS be reperformed.
7. Despite any other provision, ORF may return a defective IDMS to the Contractor within thirty (30) days of delivery of the IDMS and the Contractor will immediately provide full exchange or refund.
    - For this section, "defective Solution" includes, but is not limited to: (1) IDMS has not met contractual obligations during acceptance testing or during the valid "Warranty Period". (2) IDMS causes significant impact and disruption to ORF operations and requires excessive downtime and interaction of ORF staff. Excessive downtime is defined when IDMS is non-operational for more than sixteen (16) business hours or two (2) full business days.
8. The ORF staff reporting the issue will describe and categorize the support issues as follows:

1.4.3.1 Service Level Agreement (SLA)

Critical Issues & Response Times:
Critical issues are defined as catastrophic failures which affect the overall operations at ORF. For example, the failure of a server, or the loss of integration or errors in the integration between the IDMS and external systems. Critical issues require the Contractor to respond per the response times indicated below.

Critical Issues Response Times:

- Initial response and acknowledgement within 15 minutes (business or non-business working hours) of reported issue(s).
- Follow up contact with ORF representative within thirty (30) minutes (business or non-business working hours) to understand the issue and to start the trouble shooting process. The Contractor will establish a conference line and hourly status calls.
- Within two (2) hours (business working hours) of the issue being reported, the Contractor will provide the next steps to fix the issue or advise and initiate restoring system(s).
- Within eight (8) hours (business working hours) of the issue being reported, the Contractor will restore the system back to operational status.

Liquidated Damages:

- Failure to fix the Critical issue and restore the IDMS to a fully operational state within eight (8) hours from the issue being reported, ORF will result in the imposition of liquidated damage of $250 per hour, to be specified in the Authority's Professional Services Agreement to be entered into by the Contractor and the Authority. The Contractor will reduce the monthly invoice by the amount assessed by ORF.
- Failure to fix the Critical issue and restore the IDMS to fully operational state after two (2) business days will result in liquidated damages of up to 5% of the monthly invoice.
- The Contractor will not be charged with delay, or assessed Liquidated Damages for delay or failure, which occurs for reasons beyond the reasonable control of the Contractor or subcontractors, as determined by ORF.

Non-critical Issues and Response Times:

Non-critical issues are defined as failures or problems which do not affect the operations at ORF. For example, the failure of a non-critical redundant piece of server, or the issue with report generation would usually be considered non-critical.

Non-critical Issues Response Times (Service level agreement):

- Initial response and acknowledgement within 15 minutes (business working hours) of reported issue(s).
- Follow up contact with ORF representative within two (2) hours (business working hours) to understand the issue and start trouble shooting process.
- Within twenty-four (24) hours (business working hours) or two (2) business days of the issue having been reported, the Contractor will provide status and next steps to fix the issue. The Contractor will diagnose and remedy the problem during normal working hours of the next working day.

Liquidated Damages:

- Failure to fix the non-critical issue within twenty-four (24) hours (business working hours) or two (2) business days of the issue having been reported will result in liquidated damages of $100 per issue. The Contractor will reduce the monthly invoice by the amount assessed by ORF.
- The Contractor will not be charged with delay, or assessed Liquidated Damages for delay or failure, which occurs for reasons beyond the reasonable control of the Contractor or subcontractors, as determined by ORF.

Business working hours are defined as 7:00 AM to 5:00 PM Eastern Time, Monday through Friday.

9. The initial status of a given outage will be communicated to the Contractor during initial notification. Should a "non-critical" outage be escalated to "Critical" status, the response time or service level agreements defined above will begin from the notification of the escalation of status to "Critical", and not from the initial notification of the non-critical event. If the resolution to the reported incident is within the control and responsibility of the Contractor, these SLA liquidated damages will apply. If the outage or incident is caused by something outside the reasonable control of the Contractor, then liquidated damage for failure to meet SLAs will not be assessed. The determination of responsibility resides with ORF Security Manager and Authority management.

10. The Contractor will provide escalation procedures including contact name, direct phone number and email address.
11. The Contractor will provide a detailed process including toll-free telephone and support email to ORF representative(s) to report any production issues encountered.
12. The Contractor must provide an online portal for support ticket requests. While reporting the issues ORF must be able to select the currently installed configuration options for the software and services being supported. The online support portal must provide the customer details such as:

    - Software installed with versions.
    - Knowledge base of previous support cases.
    - Technician assigned to support request.
    - Status updates on support tickets – via e-mail.
    - Listing all support tickets and who initiated the tickets.
    - Support category: warranty, out of warranty, covered, not covered.
    - Designate issue criticality (Critical or Non-Critical) and designate priority: Low, Medium, High.
    - Ticket resolution with details.

1.5 PRICING AND PAYMENT SCHEDULE

Below is a proposed payment scheduled based on project milestone completion. The Contractor will be paid as per the breakdown below.

#	Milestone Name	Software Licenses %	Professional Services %	Hardware
1	(1) Project Initiation (Kick-off and Workshop); (2) Install IDMS COTS in Airport Test and Training environment	25%	15%	Test Quantity costs
2	(1) Data Analysis and Data Migration Configure IDMS (2) Contractor performs System Acceptance Readiness Testing		15%	
3	System Acceptance Testing in Test Environment	25%	25%	Production Quantity costs
4	Completion of Training		10%	
5	Go-Live	25%	15%	
6	Final System Acceptance in Production Environment & Project Close Out	25%	20%	

SECTION 2.0

2.1 LENGTH OF CONTRACT

This contract will run for the base project implementation period of no more than twelve (12) months upon Notice to Proceed (NTP) with a 1-year warranty commencing upon final IDMS acceptance. The Contractor's response must provide a baseline schedule as part of the proposal containing sufficient detail to complete the installation within the specified timeframe with their proposal. The Contractor is encouraged to make recommendations regarding improvement to the anticipated project schedule.

- IDMS Implementation and Go-live.
- Year 1: Warranty, Support & Maintenance (No cost to ORF)
- Years 2, 3, 4 & 5: Maintenance and Support
- Years 6 & 7: Maintenance and Support (Option Periods extended by the Authority)

2.2 MINIMUM QUALIFICATIONS REQUIREMENTS

The minimum requirements for the Contractor to be eligible for proposal evaluation consideration is as follows:

- The Contractor should have qualified and experienced IDMS personnel on staff and be assigned to this project.
- The IDMS product version, proposed in the Contractor's proposal, must have been installed and operational in three (3) or more airports in the United States of similar size as ORF.
- The IDMS must have established and operational software interfaces with Physical Access Control System (Software House C•CURE 9000) AND Designated Aviation Channeling (DAC) service provider (TSC) in three (3) or more airports in the United States of similar size as ORF.

2.3 EVALUATION CRITERIA

The Team will use the criteria noted below for the final selection of the Contractor for contract award. The Team, after scoring the proposals, may decide to short list specific Contractors for IDMS product demonstrations. The product demonstrations will be scored separately from the evaluation criteria defined below. The Airport will send communications to the shortlisted Contractors with details for the product demonstration and requirements.

Based on the results of the proposals and if required product demonstrations, **one (1)** IDMS Contractor will be selected for further action, such as contract negotiations and contract award.

If, however, it is decided that no response is sufficiently advantageous, the Airport proposal evaluation team may take whatever further action is deemed necessary to fulfill its needs. If, for any reason, a proposal is selected, and it is not possible to finalize a subcontract with the Contractor, the Airport may begin contract negotiations and discussions with the next qualified Contractor or determine that no such alternate proposal exists.

Criteria	Points
Project Approach	15
Experience, Qualifications and References	20
Functional and Technical Requirements Specifications Response	25
Execution Plan including Project Schedule	10
Pricing Proposal (implementation costs, software licenses, hardware and maintenance)	30
TOTAL POINTS	**100**

2.4 EVALUATION CRITERIA DEFINITIONS AND EXPECTATIONS

2.4.1 PROJECT APPROACH

The Project Approach must be divided into sections as described below. Every point made in each section should be addressed in the order given with the question first stated followed by the Contractor's response. The same outline numbers should be used in the response. RFP language may be referenced but should not be repeated within the response.

2.4.1.1 Overview of Proposed Method

This overview must consist of a concise summary of the requested services proposed by the Contractor in response to this RFP. By reading the overview, the Team must be able to gain a comfortable grasp at a general level of the services to be provided and the methods proposed by the Contractor to provide them.

2.4.1.2 Approach Description

The description must indicate the methodology the Contractor will follow to fulfill the requirements of the scope. A detailed explanation should be included to understand how the proposed services comply with the technical components of this RFP. The Team intends that each Contractor provide a detailed and comprehensive description of all services that the Contractor will provide if it enters into a contract with the Authority pursuant to the RFP.

The Project Approach should detail how the Contractor will work with the Team and the Airport to ensure there are no operational impacts to the Airport's badging office during the implementation. It will detail how the existing security systems will be maintained and transitioned during the implementation, how operators will work with the existing and new solution prior to final cutover, and how users will be trained on the solution. Approach will detail how business rules and processes currently in place in the Airport's badging office will be implemented and potentially automated within the new solution.

Approach will detail the Contractor's experience managing IDMS implementation projects in and around an active airport airfield and terminal sterile facilities. Specific reference should be included as to how a safe and secure environment will be maintained throughout the implementation.

2.4.1.3 Identification of Anticipated Risks

The proposal should identify and describe any anticipated potential problems, the Contractor's approach to solving these problems, and any special assistance that will be requested from the Airport.

This section should specifically reference the Contractor's experience with IDMS, specifically interfaces with standard systems, and the lessons learned which will be utilized in implementing this project.

2.4.2 EXPERIENCE, QUALIFICATIONS AND REFERENCES

2.4.2.1 Experience

The Team seeks proposals from Contractors who can provide an IDMS and all components including warranty, support and maintenance as described in this RFP.

Describe the Contractor's experience in IDMS design, system interface design and development with Software House CCURE 9000, Transportation Clerance house (TSC). Describe projects that illustrate the Contractor's experience in managing implementations of a similar scope and size relative to the systems and interfaces described in this RFP.

2.4.2.2 Qualifications

The Contractor will provide qualification information as indicated below for the proposed Project team and their qualifications:

- Include a project organizational chart identifying the Project Manager and key staff needed to perform and manage the scope of work described in this RFP.
- Include the names, titles and task responsibilities of key staff and general staff who will be involved in this project.
- Provide a responsibility matrix indicating the reporting structure related to the scope of this project.
- Once a contract is awarded and executed, the Airport must approve any change(s) to the key staff assigned to the project.
- Provide resumes for all names listed above as key and general staff members. Indicate on resumes previous experience with IDMS projects. Limit resumes to one page and describe:
    - IDMS professional qualifications and years of experience.
    - Customer and project along with the start and end dates.
    - Related education, training, and applicable certifications.
    - Staff member's experience level. Example: Staff member's experience was as a Project Manager, Business Analyst, Programmer (include the name of software application) interfaces, training, etc.

At a minimum, the Contractor's Project Manager and technical lead staff assigned to this project should have previous experience with implementing IDMS's at up to three (3) similar size airports or similar facilities as indicated in this RFP.

2.4.2.3 References

Contractor's previous experience in implementing an IDMS at similar size US Airports – Provide up to three (3) airport references. Airport reference contacts provided by the Contractor should have direct knowledge of the Contractor's experience with similar work defined in this RFP.

The Team, in its sole discretion, reserves the right to contact all references and to request additional supporting information from the Contractors as necessary.

Airport References must include at a minimum:

i. Airport name.
ii. Airport contact person name and title (Project Manager or principal individual) with direct knowledge of contract and service performance.
iii. Telephone number.
iv. E-mail address.
v. ID count and quantity of badging workstations.
vi. Standard interfaces.

2.4.3 FUNCTIONAL AND TECHNICAL REQUIREMENTS

The Contractor will respond to all the functional and technical requirements listed in the RFP.

2.4.4 EXECUTION PLAN

The proposal will include an Execution Plan and schedule that includes consideration of coordination with the Airport's badging office staff, authorized signatories, operations staff, IT staff, any other required representatives, and the Transportation Security Administration (TSA).

The proposal will include a Work Breakdown Structure (WBS) to the most detailed task level. The WBS should specifically highlight the responsible party (IDMS Contractor, Airport, IT etc.) that will be executing the work.

The WBS will detail the parts of the project that Airport personnel will be required to have internal deliverables ready. This includes, specifically, the server and storage environment required for the implementation of the IDMS.

2.4.5 PRICING PROPOSAL

The pricing proposal will include all fees, costs, charges, and other amounts, associated directly or indirectly, with providing all things necessary to perform the implementation of this project as indicated in this RFP. Failure to comply fully with the requirements will be cause for the rejection of a proposal, as non-compliant, from further consideration.

Pricing Sheet: The Contractor will provide the cost detailed proposal as per the format provided in **Attachment E** of this document.

2.5 PROPOSAL PREPARATION OUTLINE

To facilitate the timely evaluation of the proposal, a standard format for proposal submission has been developed and is documented in this section. All Contractors are required to format their proposals in a manner consistent with the guidelines described below:

- The proposal must be no longer than fifty (50) pages of 10 pt. type with margins at a minimum of one inch.
- Proposals should include an original, five (5) copies, and one electronic sent to sdward@norfolkairport.com. Hard copies must include the proposal and all attachments in an envelope which shall be sealed, conspicuously endorsed with the Offeror's name, the words "Airport IDMS", the date, time and place the Proposal is to be received.
- The Norfolk Airport Authority (NAA) is soliciting proposals from qualified firms for a comprehensive and automated Identity Management System (IDMS) at the Norfolk International Airport, to be delivered to Shelia D. Ward, Vice President and Chief Operations Officer, at sward@norfolkairport.com. **Proposals must be accepted by 2:00 p.m. on February 20, 2024.**
- ORF may, at their option, allow all Contractors a five-calendar-day period to correct errors or omissions to their proposals. Should this necessity arise, ORF will contact each Contractor affected. Each Contractor must submit written corrections to the proposal within five (5) calendar days of notification. The intent of this option is to allow proposals with only minor errors or omissions to be corrected. Major errors or omissions, such as the failure to include prices, may result in disqualification of the proposal from further evaluation.
- The transmittal letter should be in the form of a letter. The proposals must be organized under the specific section titles as listed below:

	PROPOSAL OUTLINE
1	TRANSMITTAL LETTER
2	PROJECT APPROACH
3	EXPERIENCE, QUALIFICATIONS AND REFERENCES
4	RESPONSE TO ATTACMENT C AND D - FUNCTIONAL AND TECHNICAL REQUIREMENTS SPECIFICATIONS RESPONSE
5	EXECUTION PLAN INCLUDING PROJECT SCHEDULE
6	ATTACHMENT E - PRICING PROPOSAL (IMPLEMENTATION COSTS, SOFTWARE LICENSES, HARDWARE AND MAINTENANCE)
7	ATTACHMENT G – ACKNOWLEDGEMENT FORM FOR SERVICE PROVIDER AGREEMENT

2.5.1 TRANSMITTAL LETTER

The Transmittal Letter must address the following topics, except those specifically identified as “optional.”

Summary of Ability to Supply the Required Services

The transmittal letter must briefly summarize the Contractor's ability to supply the requested services that meet the requirements defined in Section One of this RFP.

The letter must also contain a statement indicating the Contractor 's willingness to provide the requested services subject to the terms and conditions set forth in the RFP.

Summary of Compensation

Contractor should specifically state the proposed fee for the services described in this RFP. If there are any services described in the proposal and scope section that would not be included in such compensation, the Contractor will state these deviations specifically, along with an indication.

of any proposed additional charges. See "disclosure" statement below for further information in completing the response regarding fee proposal and overall compensation.

The contractor should also include a detailed summary of any additional services including the price for all such services, if any, rendered that would be considered outside of the fee proposal.

Proposal Life

A statement must be included that indicates the length of time during which the ORF may rely on all proposal commitments. The ORF requires that this period not be less than ninety (90) days from the due date for submission of proposals. Any proposal accepted by the ORF for contract negotiations must remain as committed through the contract negotiation period.

Signature of Authorized Representative

An individual person legally authorized to act on behalf of and commit the Contractor to its representations must sign the transmittal letter. Written evidence of this authorization must be provided as part of the Proposal.

Other Information

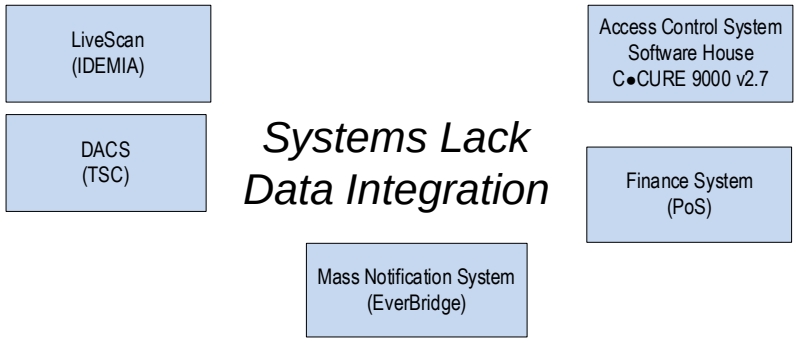
This item is optional. Any other information the Contractor may wish to briefly summarize will be acceptable.

All other proposal outline topics are defined in Section 2.4

ATTACHMENT A: EXISTING SYSTEMS, TECHNOLOGIES & BUSINESS PROCESSES

Airport Badging Office Systems / Applications

The Airport Badging Office uses various disparate and standalone systems. Below is a representation of the systems in places that are not interconnected or integrated with each other.



Access Control System (ACS) – The Airport ACS consists of a Software House C•CURE 9000 v2.7 application operating on physical servers within the Airport credentialing office. The Airport uses the C•CURE ID badging functionality to design badges, store badge holder information, capture photos and print badges using existing badge printers. The clearance codes are defined in the ACS and then assigned to badge holders. The Airport manages a Company clearance code binder. The clearance codes are defined at the time of company approval by the Chief Operations Officer (COO) working with the company representative or AS and based on the type of business at the Airport. This binder lists all the Companies at the Airport, and the clearance codes that can be assigned for a Company.

Card Technologies & Badge#- The Airport issues iClass Prox cards. The badge number (hot stamp) printed on the back of the badge by HID is programmed in C•CURE and used for access control. This number is entered in the C•CURE system, printed on the front of the badge and used by the access control system for opening /closing doors. The badge # changes every time the badge is issued including for renewal, lost, stolen or damaged scenarios.

Fingerprint Live Scan Systems – The Airport uses one (1) IDEMIA (**4100XDFS- M95)** to capture airport employee 10-prints for the Criminal History Records Checks (CHRC). The airport is satisfied with the performance of the IDEMIA finger printing machines and plans to extend the contract with IDMEIA as well as add a second fingerprint setup in the badging office as future expansion and integration with single unified IDMS badging workstation.

Designated Airport Channeling Service (DAC) – The Airport badging office enters all the new applicant's biographic information in to the TSC system (via web portal login) for submission to the TSA for Security Threat Assessment and Livescan fingerprints to the FBI for the Criminal History Records Checks (CHRC). The badging office daily monitors (some more than once a day) for changes or updates to the STA or CHRC. The CHRC results are reviewed in the FBI system. The applicants are enrolled in the RapBack program.

The Airport currently does not fingerprint all SIDA badge holders (one Airline submits case file and CHRC Results letter). However, the Airport is in the process of 100% fingerprinting and adjudication to be performed in the Airport badging office.

Financial Systems – The Airport currently uses a combination of monthly invoicing, escrow payments and Point of Sale (PoS) devices for credit / debit card transactions for badge related fees. The Airport is investigating the option to include the PoS devices to be installed in the badge office for collecting badge related fees.

Point-of-Sale (PoS) - Standalone Point of Sale devices in the finance department for processing credit / debit cards. The printed receipt from the PoS and the transaction # are documented. The paid receipt is printed in the Finance department and the applicant / badgeholder hand carries the receipt (proof of payment) to the Airport badging office.

Training Systems – The Airport implements manual and in-class setup for all training using DVD players. The applicants or badgeholders requiring training schedule with the badging office via email/ phones communications. The training courses included are SIDA, Movement and Non-Movement. The operations (Driver) training is currently managed by the Airport Operations team with some tenant trainers. The Airport is planning to make modifications to the program where all training, review and (check-ins) approvals will be performed by the Airport Operations team. More details in the later sections.

Mass Notification – The Airport uses the Everbridge mass notification system for critical operational notifications to all the Airport employees. Currently, a file is exported from the CCURE system on a weekly basis. The badging office staff reviewed the file for quality and formatting then the file is uploaded into the Mass Notification system. The Airport would like to eliminate this manual step with the IDMS platform. The intent for the IDMS is to capture and push active cardholder contact information to the Everbridge and when the badge is inactivated then remove the employee from Everbridge system.

Badging Office & Training Room Layout

The ORF Airport Badging Office, located in the main terminal, is accessible to all Airport employees. The Airport Badging Office is configured with a waiting area in the vestibule/lobby. The badging station is equipped with a total of 3 standalone computers performing various functions. There is one (1) workstation (CCURE 9000) for badge productions, one (1) ORF issued workstation for background checks entry and retrieval (TSC), other NAA applications (Outlook, etc.) and third standalone single workstation for fingerprinting (IDEMIA). The CCURE 9000 workstation is equipped with badging equipment – camera and badge printer.

Within the badging office is the Training room set up with four (4) stations that have monitors and DVD player for security and driver trainings.

#	BADGING EQUIPMENT	QUANTITY
1	Camera	1
2	Badge Printer	1
3	Laminate – Custom or Standard	1
4	Standard Paper Printer	1

Existing User Roles and Business Process

This section documents user roles, the employee badge issuance workflow, the company financial setup, and the citation program.

User Roles

There are multiple users managing the various badging business processes at ORF. A list of the users and responsibilities is provided below.

#	USER ROLE	RESPONSIBILITIES
1	Authorized Signatory	Fill paper forms, review and authorize new badge applications, authorization of renewals (badge), respond to badge audits and involved with citations hearings and coordinating trainings for applicants.
2	Applicant	Coordinate with Authorized User to complete badge application process.
3	Trusted Agents / Badging Office Staff	Badge applicant data entry in various disparate systems, fingerprinting, document verification and scanning, badge production, payment collection, receipt generation, tracking RAP back enrollment and removal in DAC system, paper log for keys, ramp permits and badge holder paper records.
4	Badging Office - Admin Analyst	Manage all tasks of Trusted Agents and management of keys, ramp permits, CHRC adjudication notifications, STA clearance, DAC provider contract maintenance, citations program, finance department coordination.
5	Badging Office - Supervisor	Manage all tasks of Admin. Analyst II, review of CHRC Rap sheets and security check adjudication, coordinate hearings for CHRC appeals, manage review of, issuance, adjudication and interview process for citation and violations (in lieu of Airport Security Manager).

6	Airport Security Manager	Manage the above tasks for Supervisor and be decision maker for citations and rap sheets adjudications,
7	Airport Operations	Conduct practical movement area training and coordinate with Badging Office for appropriate driver endorsement on the applicant badge. Update citation information (see citation workflow).

Business Processes / Workflows

This section describes various workflow processes.

Company Setup

The company contacts the Chief Operating Officer and provides details of the business name, business purpose at the airport, contract details, areas of access and the designated Authorized Signatory for the company. The COO will review all the details and send a letter of approval with various details including badge types, privileges, etc. to the ID Office.

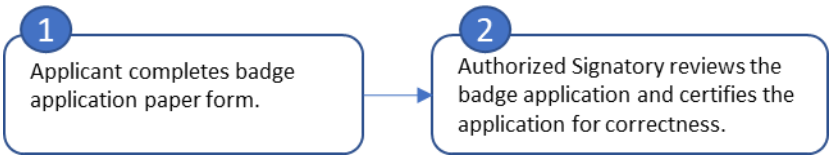
The Finance Department has categories for badge fee payment methods based on the type of the company. For example: Airlines will be billed monthly.

The letter of approval is sent to the company representative and the ID Office which is then filed for future reference.

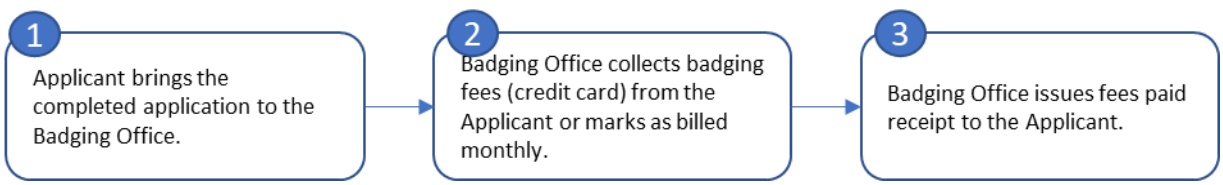
Employee Badge Issuance

The new badge request is explained below. The applicant submits paper application, the financial payment form to finance and the badging office for payment, then the badging office performs identity & document validation, fingerprinting and then again for required training and badge pickup.

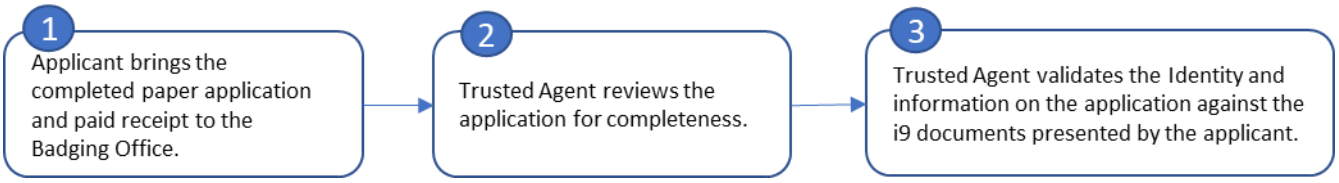
[A] Paper Application: The Authorized Signatory and the applicant work together to fill the paper badge application. The Authorized Signatory based on the applicant's job requirements requests the driving and unescorted/ escorted privileges.



[B] Badging Fees: The applicant submits financial payment form to finance and the badging office for payment and issues a receipt of payment.

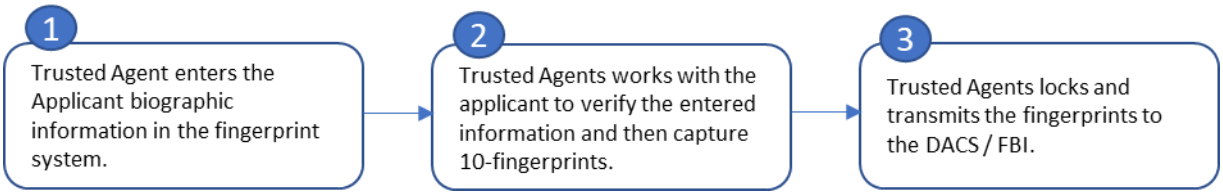


[C] Badging Office Visit 1: The applicants take the paper application, i9 documents and the payment receipt to the badging office.



NOTE: Currently, the I9 verification documents are not scanned, or copies preserved with the paper application.

[D] Fingerprint Process: The Trusted Agent and the applicant complete the fingerprinting process.

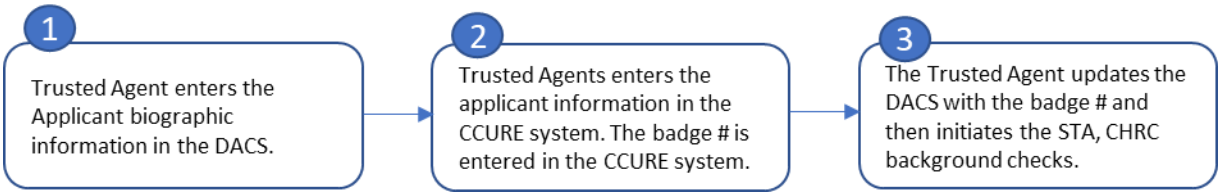


Note: The applicant leaves the badging office after successfully completing the fingerprinting capture process.

[E] Back Office Process (DACS and CCURE):

The Trusted agent enters applicants' biographic information in DACS. Then the same information is entered in the CCURE system. The CCURE system generates a badge # that is then entered in the DACS. After that, the Trusted Agent initiates the STA, CHRC and subscribes to Rapback.

The Trusted Agent will monitor the DACS daily for times for changes / updates to the applicant's STA, CHRC statuses. If there are any errors/ issues those are corrected by the Trusted Agent in DACS and security checks reprocessed.



[F]: Background Check Adjudication Process:

The Trusted agent confirms the STA is passed, then logs in to the FBI FPRD website to check the CHRC status. The Trusted agent will download and adjudicate the rap sheets and any other information available in the FBI FPRD system.

If the rap sheet has disqualifying crimes, then the Airport will notify via email (sent manually) to the Authorized Signatory of failure of background checks and the badge will not be issued.

If the applicant has no disqualifying offenses, then the Trusted Agent notifies the Authorized Signatory that the applicant has cleared the background checks, and the applicant should visit the ID office to complete the mandatory SIDA Trainings and other driver trainings as required.

[G]: Training:

The Applicant visits the ID office to complete the required trainings. If driver training is required, then the Applicant and Authorized Signatory coordinate with the Operations team to complete the necessary drivers' trainings. Once all training is completed, including the Operations approval (check-ins) then the ID office will issue the badge.

[H]: Badge Issuance:

The applicant in the ID office will capture the applicant's photo, set up the 4-digit PIN and print the badge.

[I]: Update DACS:

The Trusted Agent updates the badge expiration date in DACS.

Badge Audit

The Airport conducts 10% and 100% badge audits. The airport sends an email /letter to the authorized signatory asking them to fill and provide list of all active badges. Sample file attached in Appendix.

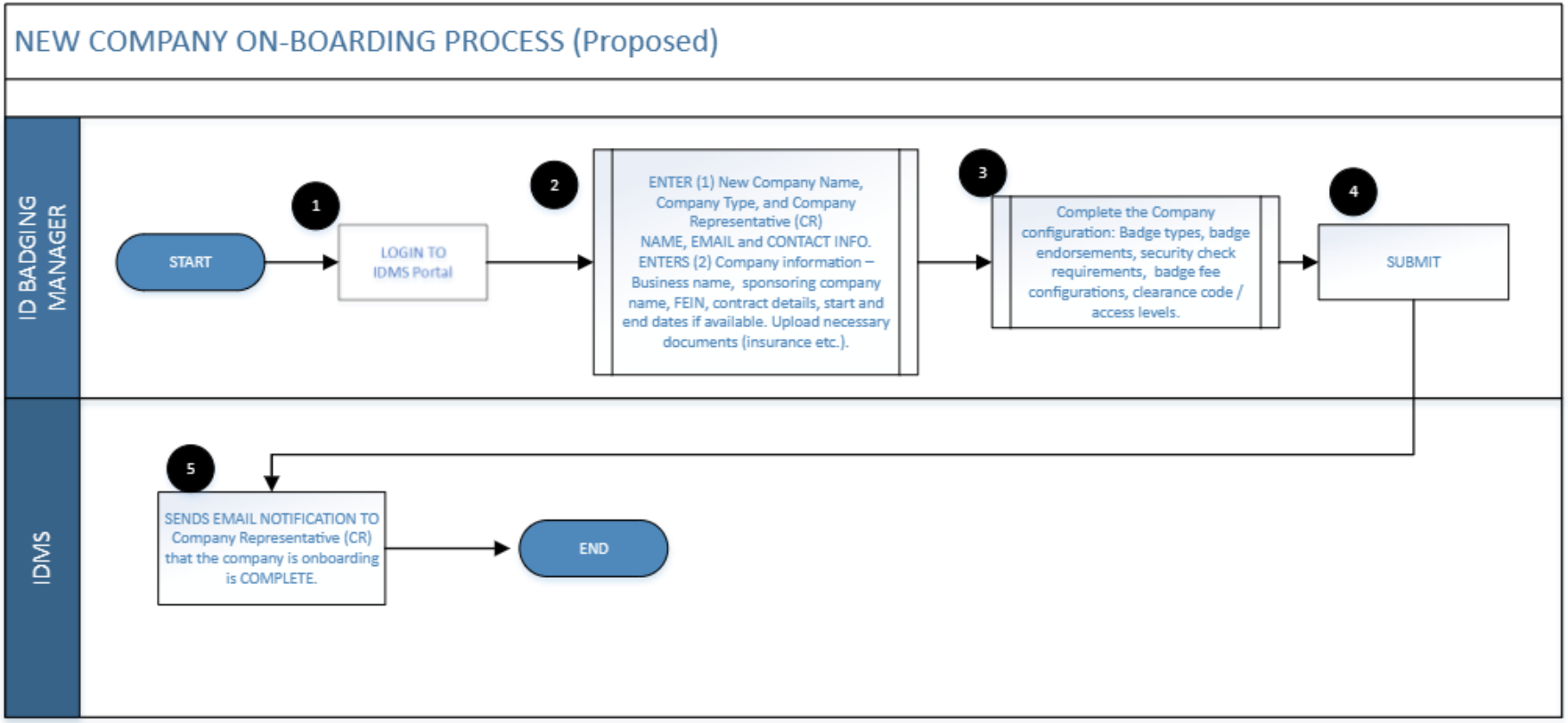
The Airport then reviews the completed audit spread sheet provided by the AS and reconciles the badge records manually against the CCURE report. If there is a discrepancy the airport informs the authorized signatory asking for an explanation.

The Airport conducts 100% badge audit annually in July and 10% in January every year. In addition, the Airport conducts badge audit spot checks for select companies (company with over 50 badges) and inspect the badge physically and visually.

ATTACHMENT B: FUTURE BUSINESS PROCESSES

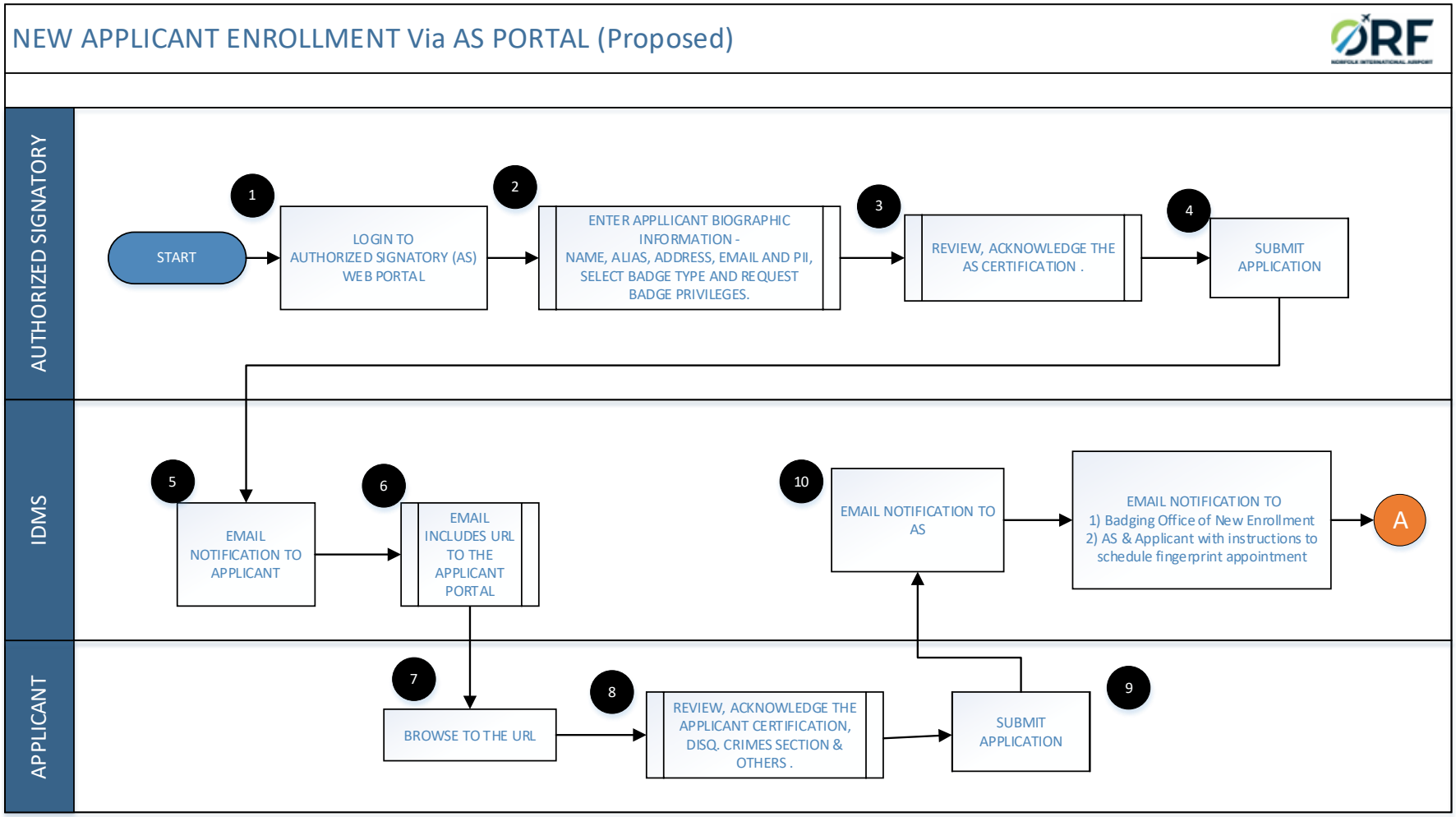
1.0 Company Onboarding

The IDMS will provide capability for the ID badging office to enter and configure company prior to processing any badge applications. The high-level workflow shows the approvals that will be required prior to activating a company. Once the company is onboarded then the badge application for the first employee or designated Authorized Signatory can begin.



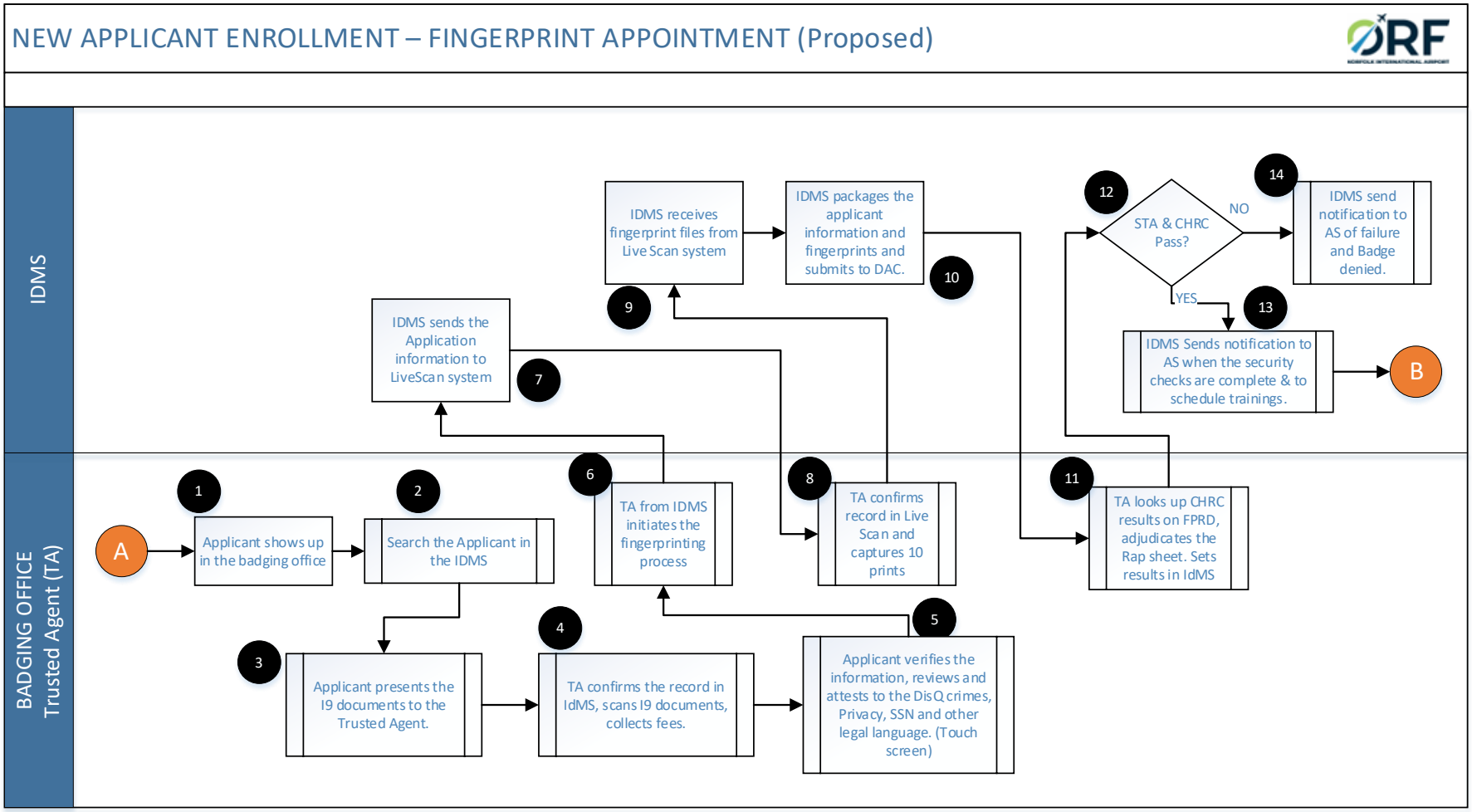
2.0 Badge Application Workflow – AS Badge application (Pre-Enrollment)

The AS will submit the application via the AS portal in this IDMS. The IDMS shall have capability for the applicant (via URL OR in the badging office) to respond to the Disqualifying Crimes questionnaire, Privacy Act, SSN wording and other airport specific cardholder responsibilities.



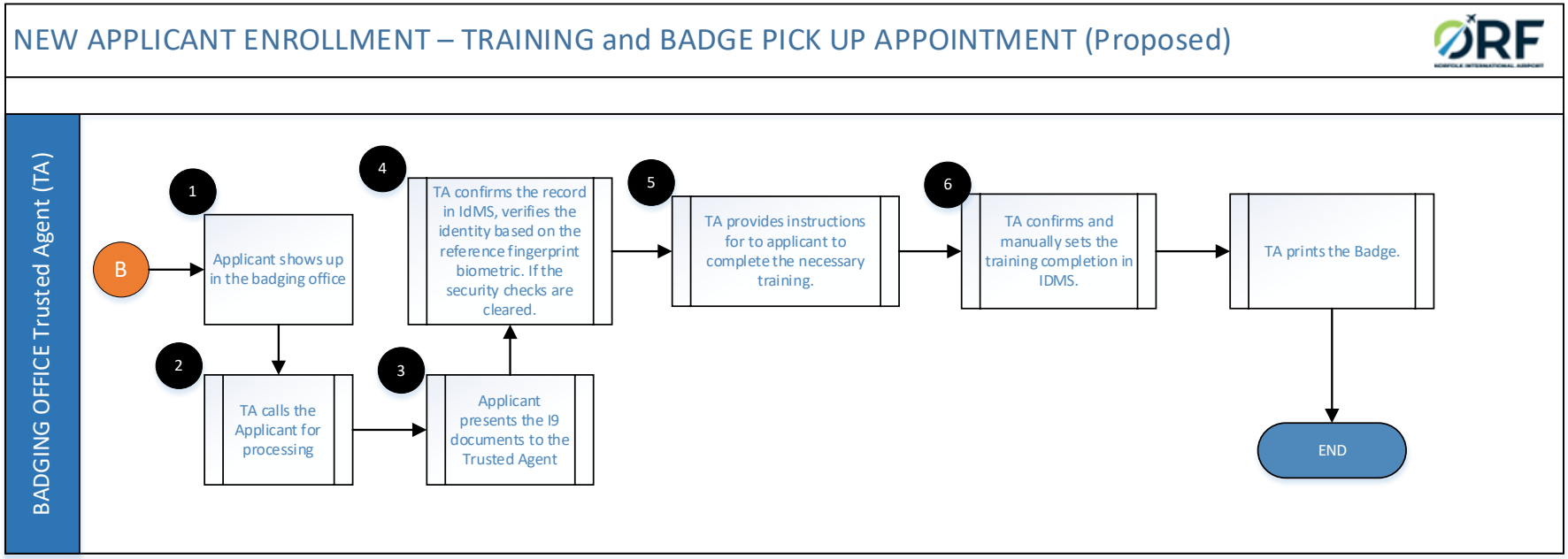
3.0 Badge Application Workflow – Applicant Fingerprint Appointment & Security Checks Process

The TA will verify the applicant and AS application in IDMS, confirm applicant has completed the Disqualifying crimes and other requirements, if not then have the applicant complete in the badging office using the touch screen. The TA will then verify the I9 documents, collect fees, scan the I9 docs in IDMS, then capture the 10-fingerprint from the IDMS and submit to DACS.



4.0 Badge Application Workflow – Applicant Training and Badge Pickup Appointment

After the security checks are complete, the AS receives email notification from the IDMS for the applicant to schedule training. The applicant shows up in the badging office. The TA will verify the applicant in IDMS, have the applicant complete the required SIDA, AS or driver training in the badging office. The TA will verify training is complete, then print the badge.



5.0 System User Groups

ORF expects at a minimum the following user group to be configured in the IDMS.

R = Read, W = Write

		Badge Applicant / Badge Holder Information										
User Groups	Company	Person Biographic	Documents	Payments/ Fees	Capture Fingerprint for CHRC	Security Checks & Adjudications	Training	Badge & Privileges	Badge Printing	Assets (Keys & Permits)	Citations / Infractions	Reports
System Administrator	R / W	R / W	R / W	R / W	R / W	R	R / W	R / W	R / W	R / W	R / W	R / W
Airport Security Coordinator(ASC)	R	R	R	R	R	R	R	R	R	R	R	R
Badging Office Manager	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W
Badging Office Trusted Agent	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R	R / W
Training Coordinator		R					R / W	R			R	R
Finance Dept	R											R / W
Authorized Signatory	R / W	R / W		R / W								
Badge Applicant		R										

ATTACHMENT C – FUNCTIONAL REQUIREMENTS

Functional Requirements				VENDOR Response	
ID	Category	Functional Area	Requirement Description	Identify the requirement meets as Product Feature (C) or Non-Compliant (NC)	Comments
R-001	Mandatory	Application Process	Provide capability for the applicant to electronically submit information related to Disqualifying crimes, Privacy Act, SSN, badgeholder responsibilities, other airport specific legal language currently available in the badge application.		
R-002	Mandatory	Application Process	IDMS shall provide capability for the applicant to electronically submit information as it relates to the badge type or company type. For example, Federal and local government employees are not required to respond to Disqualifying crimes, Privacy Act, SSN. However, they are required to respond/acknowledge airport specific legal language, badgeholder responsibilities and other information in the badge application.		
R-003	Mandatory	Application Process	The applicant portal shall be mobile friendly such that the web portal aligns to various mobile screen sizes without limiting functionality.		
R-004	Mandatory	Application Process	The IDMS shall have capability for a generic link/ website where the applicant can enter name, DoB, SSN and I9 document for identity verification and then respond to the regulatory information and acknowledgements. The applicants should not be required to create and maintain username and password credentials.		
R-005	Mandatory	Application Process	The IDMS shall have the capability to list all complete applications submitted by the AS. If the applicant portion of the application is not complete the badge application cannot be processed by the badging office.		
R-006	Mandatory	Application Process	The IDMS shall have capability to clearly identify the type to application such as new badge application, renewal badge application, badge change (for adding or removing privilege - escort, driving privilege), replacement badge application (name change or lost, stolen or mutilated).		
R-007	Mandatory	Application Process	The IDMS shall display to the applicant all the information entered by the AS in the application including biographic information, company / division, badge type and badge privileges requested, supporting documentation if uploaded by the AS (I9 documents, driver permits, key request forms, CBP forms for eBadge) and allow the applicant to respond to the disqualifying offenses questionnaire and acknowledgments and other information as per the current paper application.		
R-008	Mandatory	Application Process	The IDMS shall allow the Trusted Agent to review and modify as necessary all the information submitted by the AS and the applicant. The Trusted agent can Accept or Reject or Cancel the badge application review step. IDMS shall send notification to AS if application is rejected or accepted.		

R-009	Mandatory	Application Process	Once the applications are rejected, they will no longer appear in the application list for processing.		
R-010	Mandatory	Application Process	The IDMS shall alert the Trusted agent if the badge applicant is an existing person with DNI. The Trusted agent can then review and accept or reject the badge application. DNI can be due to security check DNI, citation /violation or another airport watch list or stop list.		
R-011	Mandatory	Application Process	The IDMS shall alert the Trusted agent if the new badge applicant already exists and allow the Trusted Agent to review the duplicate record and merge or process individually.		
R-012	Mandatory	Application Process	IDMS shall flag the application for Badging Office staff supervisor review if the employee had previously worked at the airport and their badge was revoked or suspended as a result of an NOV or the adjudication eligibility date has not passed.		
R-013	Mandatory	Audit	IDMS shall comply and allow conducting badge audits as per the Security Directive (SD) 1542-04-08O (or subsequent updates) and revisions to TSA-NA-19-02.		
R-014	Mandatory	Audit	Audit should allow selection of records for Audit based on company, specific individuals and badge type.		
R-015	Mandatory	Audit	IDMS should generate the Badge status report in pdf format and notify as attachment to the ASC.		
R-016	Mandatory	Audit	IDMS shall allow generating list of random records to be audited. Allow the badging office staff to edit the list of records prior to activating the badge audit.		
R-017	Mandatory	Authorized Signatory	The IDMS shall at all times check and enforce the AS to maintain an active badge, valid security checks, valid AS trainings, in order to keep the AS active and maintain access to the AS portal.		
R-018	Mandatory	Authorized Signatory	IDMS must assign each Authorized Signer a unique user account and password upon completion of the approval process and required training. This user account will be used for submission of employee badge applications and all other business activities performed using the web interface.		
R-019	Mandatory	Authorized Signatory	IDMS shall provide and describe mechanisms to incorporate multi-factor authentication for the Authorizing Signatory Portal. The IDMS shall have the capability to implement OTP / authentication codes via text or email.		
R-020	Mandatory	Authorized Signatory	The IDMS shall provide capability for the AS to perform at a minimum via the AS web portal, the following functions: enroll new applicants, authorize renewal of badges, submit badge replacement applications for lost, stolen, mutilated, name changes or privilege modification changes, respond to audits (badge and key), upload supporting documentation for I-9, CBP forms, driving permits, key request form, and other documentation as necessary for the airport operations.		
R-021	Mandatory	Authorized Signatory	The IDMS shall have capability to capture all the STA required fields during the badge application process.		
R-022	Mandatory	Authorized Signatory	Provide the ability to send via email to a new badge applicant (mandatory field for all applicants), an expiring link to enter -applicant regulatory information and acknowledgements application information and attest to a disqualifying felony statement.		

R-023	Mandatory	Authorized Signatory	The IDMS shall allow the badge application entered by the AS to be saved prior to submission. The application will be saved for 30 days or user defined timeframe prior to permanently deleting the application from IDMS.		
R-024	Mandatory	Authorized Signatory	The IDMS shall permit the Authorized Signer to select the badge type, privileges, and access level / clearance codes requests for a new badge application or for existing badges.		
R-025	Mandatory	Authorized Signatory	The IDMS shall allow AS to authorize renewal if the employee badge is due to expire within the 30 -45-60 days of badge expiration.		
R-026	Mandatory	Authorized Signatory	The IDMS shall allow Authorized Signatories to modify certain employee information while restricting changes to Date of Birth (DOB), SSN, Birth Country and other fields deemed to be critical to the STA process.		
R-027	Mandatory	Authorized Signatory	At a minimum, following should be displayed on the dashboard: The AS will see only those companies and badge holders, he / she is responsible for. The AS should see the list of applications submitted, pending, applicant acknowledgements submitted or pending, upcoming badge expirations and badge renewals, unaccounted badges.		
R-028	Mandatory	Badge Production	The IDMS will provide a badge layout design tool for Airport badges. The card layout shall allow creation of single sided and double-sided designs.		
R-029	Mandatory	Badge Production	IDMS shall permit system administrators to change the layout and design of Airport badge templates. The badge designer shall allow printing company name, division, company sponsoring name as required by the airport operations.		
R-030	Mandatory	Badge Production	Provides capability to easily add static and dynamic text data. The layout tool shall allow the addition of logos, graphics, images in various formats.		
R-031	Mandatory	Badge Production	Automatically calculate and default the maximum expiration date for each new or reissued badge based on current airport policy, attributes of the badge and document, training, security checks expiration dates.		
R-032	Mandatory	Badge Production	The IDMS shall allow at a minimum the following badge statuses with capability for the system administrators to add / modify statuses and reason for de-activation: Active, Inactive, Suspended, Terminated, Revoked, Returned, Lost, Stolen, Damaged, DNI. The IDMS shall also provide drop down list for "Reason for De-activation"		
R-033	Mandatory	Badge Production	The IDMS shall clearly indicate on the UI if the badge was returned, badge returned date, badge printed date, badge pick-up date.		
R-034	Mandatory	Badge Production	When the current date passes an assigned expiration date on a badge, automatically update the badge status to revoked with reason of expired and deactivate the badge in the PACS.		
R-035	Mandatory	Badge Production	Prevent printing a badge if any of the requirements such as background checks, trainings or documents are not completed in the IDMS.		
R-036	Mandatory	Badge Production	IDMS must support SEOS prox, ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693 and ISO/IEC 7501 smart-card technologies and must also support the Federal Information Processing Standard 201 (FIPS-201).		
R-037	Mandatory	Badge Production	IDMS must permit capture of identification photos with different industry standard formats, using digital cameras, and must be capable of exporting photo images to other systems (e.g. PACS).		

R-038	Mandatory	Badge Production	Provide for applicant photo capture, cropping, and digital enhancing from within the client application.		
R-039	Mandatory	Badge Production	Photo should be captured every time badge is printed (e.g. replacement, renewal)		
R-040	Mandatory	Badge Production	IDMS shall not be able to issue (print) badges until all applicable procedures (e.g. employment verification, I-9 Documents, CHRC/STA, and Training) have been successfully completed.		
R-041	Mandatory	Badge Production	IDMS shall provide capability to advance printing (e.g. company name changes, mergers or rebadges).		
R-042	Mandatory	Badge Production	Provide ability to pre-print badge when CHRC/STA are cleared or otherwise approved, while applicant is undergoing training (e.g. driver practical training or CBP Seal request is pending). This can be done using supervisor override feature.		
R-043	Mandatory	Badge Production	Allow creation of new badges as replacements for unaccounted (e.g. lost, stolen) badges by copying previous badge details, badge expiration date and establishing a new badge number.		
R-044	Mandatory	Badge Production	Notify the Trusted Agent of an individual whose previous badge(s) were not surrendered (e.g. lost, stolen, not returned, and otherwise unaccounted for). When a violation has occurred allow badge issuance after the fine is paid and / or the training has been completed.		
R-045	Mandatory	Badge Production	IDMS shall prevent printing of a new badge until the old badge has been surrendered to the Badging Office staff, unless the old badge was terminated as lost or stolen. In case of stolen badge, a certification box / acknowledgement from the applicant via touch screen or signature pad certifying that the previously issued badge is no longer in your possession and you are unaware of its whereabouts.		
R-046	Mandatory	Badge Production	Print a receipt and send notification to the badge holder and / or Authorized Signatory as proof the badge was issued or surrendered		
R-047	Mandatory	Badge Production	Provide capability of reprinting a badge with the same badge number and different credential number based on permission level (e.g. production error or production void). The badge number printed on the face of the badge remains constant for the individual for that company. The credential number (hot stamp) printed on the back of the badge by the card manufacturer is programmed in PACS and used for access control. The credential number changes every time the card is printed.		
R-048	Mandatory	Badgeholder Record Management	IDMS shall permit the Badging office or Badging Office staff to indicate the status of a badge as returned and destroyed or lost or stolen.		
R-049	Mandatory	Badgeholder Record Management	When an AS or badgeholder reports their badge as lost or stolen, the badge must immediately be deactivated in IDMS and the PACS.		
R-050	Mandatory	Badgeholder Record Management	Provide ability to issue single active badges to one individual working for multiple separate companies. (Up to 2 companies on the badge)		

R-051	Mandatory	Badgeholder Record Management	Provide the ability to issue a single badge for multiple companies.		
R-052	Mandatory	Badgeholder Record Management	The IDMS shall have capability for ASC or ASM to designate certain individuals as protected person (i.e. undercover law enforcement). These individuals will be exempt from security checks, fees and training. Only ASC or ASM or designee can access and modify records for these protected persons.		
R-053	Future	Citations/ Violations	Allow users with appropriate permissions to add new types (security and safety) of violations.		
R-054	Future	Citations/ Violations	Allow an unlimited number of violation types to be added.		
R-055	Future	Citations/ Violations	The IDMS shall incorporate the existing paper citation tickets information including violation #, name, issuing officer, location, company, badge # and corrective actions like fine, badge suspension and training required.		
R-056	Future	Citations/ Violations	Track the payment status if a fine is imposed and include the information in the appropriate financial reports.		
R-057	Future	Citations/ Violations	Manage a central record of employee's violations at the Airport.		
R-058	Future	Citations/ Violations	Record and track airport policy infractions in each identity profile (e.g. safety and security violations, no insurance).		
R-059	Future	Citations/ Violations	Record and track repeated infractions (including traffic violations), which may warrant re-training of the employee.		
R-060	Future	Citations/ Violations	Track the number of tickets, violations in each identity profile.		
R-061	Future	Citations/ Violations	Allow Airport to determine if a badge should be suspended but should not occur automatically unless defined by the System Administrator.		
R-062	Future	Citations/ Violations	Track penalties relating to a suspension.		
R-063	Future	Citations/ Violations	Track fulfillment of any necessary corrective actions (e.g. penalties, suspension, training).		
R-064	Future	Citations/ Violations	Track the payment status of a fine or ticket and automatically send email notification to Authorized Signatory.		
R-065	Future	Citations/ Violations	Provide ability to search existing or historical records (entered and migrated in IDMS) of infractions by multiple fields such as name, company, badge number, ticket number, and plate number.		
R-066	Future	Citations/ Violations	Provide ability to define and limit users access (e.g. data entry, read-only) to Violations/Citations tab.		
R-067	Future	Citations/ Violations	Send violation notices out via email automatically to the Authorized Signatory.		

R-068	Mandatory	Company	IDMS shall provide capability for the Badging Office staff to enroll a new company and provide at a minimum the following information including but not limited to company name, company start and end dates, company type (For Example: Airline, Local or Federal Government, Contract, Tenants, Vendors, Concessionaires, others) company status, division status, clearance codes/access level assignment configurations, contract information, contract start and end dates, sponsor contractor information.		
R-069	Mandatory	Company	IDMS shall provide ability to capture company names as - Business Legal name, doing business as, abbreviated name to be printed on the badge.		
R-070	Mandatory	Company	The IDMS shall check for duplicate company names. If the company name exists, the IDMS shall notify the ASC and Badging Office staff of a potential duplicate. At a minimum the "Doing Business as", FEIN / Tax ID, and the "abbreviated / badge printed" name for a company should be unique in the system.		
R-071	Mandatory	Company	IDMS shall provide the ability to store multiple company addresses, phone numbers and multiple company contacts information including name, email, job title.		
R-072	Mandatory	Company	IDMS shall provide capability to configure at company and division level the ID requirements (certain government employees can provide one I9 document), access levels/clearance codes, financials (monthly billing, pay-as-you-go, fee waived), payments (badge fees, other fees), badge limits, designation limits, security check exemptions (CHRC, STA, others).		
R-073	Mandatory	Company	IDMS shall provide capability for the Badging Office to scan and / or upload documents related to company enrollment. For example, company authorization letter, contract documents, insurance certificate, nominate first Authorized Signatory for the company, and others as required by the Airport. The documents will be saved in the IDMS and be available and the archived/ deleted as per the airport data retention policy.		
R-074	Mandatory	Company	The IDMS shall allow tracking of the Company statuses. At a minimum the following should be available Active, Inactive, Suspended, Terminated, and others as per the Airport business requirements.		
R-075	Nice to Have	Company	The IDMS shall have capability to add Reason for de-activation or add notes to company profile when the company status has changed from active to another status.		
R-076	Mandatory	Company	The IDMS shall allow suspension of a company such that existing active badges will not be automatically de-activated when the status has changed, however will enforce any future processing of the company employees for badge printing or badge renewals. (Example case: company has financial payments due/ defaulted)		
R-077	Nice to Have	Company	The IDMS shall allow configuration such that if a company is an airline (following TSR rules 1544) that conducts their own Criminal History Record Check (CHRC) background checks, IDMS shall require input of the applicant's CHRC case number. The IDMS shall have capability for AS to enter the case file number for 1544 carriers. Note: The Airport performs 100% fingerprinting of all airport SIDA badge applicants.		

R-078	Mandatory	Company	The IDMS shall enforce that a Company in Active status should have at least one (1) active Authorized Signatory. There is no limit on the number of Authorized signatories that a company can designate. Use of global AS or badging office manager for 1st AS enrollment is acceptable.		
R-079	Mandatory	Company	The IDMS shall have capability to allow the badging office to set an authorized signatory as Active or Inactive.		
R-080	Mandatory	Company	Provide capability to set maximum number of active badges (percentage of numeric) for specific badge type or badge privilege (e.g. Customs Seal, Sterile Area access, movement or non-movement, ramp permit) for a company. (e.g. 25% concessionaire rule or limiting driving privileges.) Notify and alert AS and the badging office (as a dashboard or queue report if limit about to be reached) and restrict badge printing if the limit is reached.		
R-081	Mandatory	Company	Provide capability for Badging Office to configure default access levels / clearance codes for an approved company. The default access levels / clearance codes will be visible in the company profile.		
R-082	Mandatory	Company	Provide capability for the Badging Office or system administrator to modify the default access levels / clearance codes per company business requirements.		
R-083	Mandatory	Company	The IDMS should provide capability for badging office manager to perform bulk / volume tasks such as de-activation of badges, badge printing, change access levels/clearance codes by badge type or company or divisions.		
R-084	Mandatory	Company	The IDMS shall provide the capability to track the expiration dates of the company's insurance policies and their contract terms to ensure that the badge or credentials are not issued for a period that exceeds the company's insurance expiration date or contract term. A supervisor must be able to override this function if it is not applicable to the company.		
R-085	Nice to Have	Company	The IDMS shall provide capability to manage driving privileges only if the company has valid certificate of insurance. If the insurance is expired or does not meet the insurance amounts required by the airport, then driving privileges cannot be assigned to the badge for that company.		
R-086	Mandatory	Company	The IDMS shall provide functionality to change company names (e.g. legal name changes and badge printed names) including providing report of all badge holders impacted. Allow corporate name changes while retaining relation to the former corporate name.		
R-087	Mandatory	Company	The IDMS shall provide functionality to allow merger of companies (e.g. legal name changes and badge printed names) including providing report of all badge holders impacted.		
R-088	Mandatory	Dashboard	The IDMS shall provide capability (as a dashboard or dynamic queue report) to clearly display in the company profile, if the company is reaching or reached badge quotas, is nearing (30 days ahead) company / contract end date, has no active AS, documents or insurance requirements have expired and other visual indicators as required by the Airport Badging Office.		
R-089	Mandatory	Dashboard	The IDMS shall provide immediate notification on dashboard and email notification to the system administrators, badging office and ASC if the connection to any DACS is lost.		

R-090	Mandatory	Dashboard	The IDMS will provide a dashboard for Badging Office staff and the AS. The dashboard should be configurable for each user group and user.		
R-091	Mandatory	Dashboard	Provide on dashboard those STA and CHRC results that have not been returned in 10 business days.		
R-092	Mandatory	Document Management	IDMS shall enable association of scanned documents with badge applications and functions in document management systems. IDMS must accommodate for all identification types shown on the Acceptable Documents List (List A, B & C).		
R-093	Mandatory	Document Management	Provide ability to restrict viewing of scan and stored documents (e.g. Rap sheets) and mark private based on user roles by permission levels.		
R-094	Mandatory	Document Management	Provide Badging Office staff an input form for capturing identification document data with appropriate fields displayed based on the type of identification provided.		
R-095	Mandatory	Document Management	Provide ability to scan, validate, and store breeder documents provided by applicants. Data retrieved from the documents should have the ability to auto-populate fields, reducing keying errors and saving time.		
R-096	Mandatory	Document Management	Be able to rotate and zoom in to review scanned documents. The upload document formats will be pdf or image files. Use of Adobe acrobat to rotate or zoom is acceptable for pdf files		
R-097	Mandatory	Document Management	When documents are scanned via driver's license scanner or passport scanner, the IDMS shall have the ability to alert the operator to mismatched data elements (e.g. name on document does not match demographic data previously captured for the applicant). Prevent operator from proceeding unless mismatched data elements are resolved.		
R-098	Mandatory	Document Management	Provide ability to compare the data retrieved from the documents against the data entered by the AS or Applicant including ability to select data fields to merge or ignore.		
R-099	Mandatory	Document Management	Provide the ability to archive electronic documents and badge records automatically on preset schedule following airport data retention policies.		
R-100	Mandatory	Email Notifications	The IDMS shall notify the badging office if a company is set to expire. Once the company has reached the expiration date, no further processing of the records can take place. The badging office can then decide if all existing active badges need to be deactivated.		
R-101	Mandatory	Email Notifications	IDMS shall support the use of templates for emails to the Security Badging Office staff, companies, and Authorized Signers.		
R-102	Mandatory	Email Notifications	Provide notification to the Authorized Signatory when a badge status changes within the Authorized Signatory's company.		
R-103	Mandatory	Email Notifications	IDMS shall allow system administrators to add / modify wording within and database references for field values in the email templates.		
R-104	Mandatory	Email Notifications	Provide ability to notify Airport or Badging Office and AS when a specified document in a record expires (e.g. driver's license, passport, authorization to work).		
R-105	Mandatory	Email Notifications	Provide capability to send various notifications with reminders and escalations to the Authorized Signatory, Airport Badging, ASC.		

R-106	Mandatory	Email Notifications	Notifications to AS, applicant and Badging Office for various statuses during badge application process (e.g. pre-enrollment, payment, fingerprinting, security checks complete, training complete (pass/fail), CBP Seals complete, badge issued, violations/citation issued); scheduling appointments (e.g. fingerprinting, document submissions, badge pickup, renewals, key and permit pick-ups, training, badge applicant -No show to appointments, applicant failed to pick up badge within 30 days from the security checks completed).		
R-107	Mandatory	Email Notifications	Notifications to AS, Applicant and Badging Office - Expirations: badge, training, CBP Seals, documents, contracts, audit responses.		
R-108	Mandatory	Email Notifications	Specific notifications to ASC: Terminations - badge, certain violations, company terminations, badge holder termination, automated STA or Rap Back hits, Trusted Agent is adding or removed from the Badging Office group, changes to default access levels / clearance codes for companies or privileges, AS is no longer active, or company does not have a single active AS.		
R-109	Mandatory	Email Notifications	Provide notification if the connection to PACS is lost.		
R-110	Mandatory	Financial/ Badge Payments	Allow payment methods to be defined at individual company levels. (e.g. while one company might be authorized to receive a single invoice at the end of the month for all services rendered by the Security Badging Office, another company may be required to pay for each badge or credential or service with a check or credit card at the time the service is rendered or at the time the appointment is booked.)		
R-111	Mandatory	Financial/ Badge Payments	Provide the capability to manage and track the fees / charges associated with badges, background investigations, and other items issued in the Security Badging Office (e.g. keys, permits, card holders).		
R-112	Mandatory	Financial/ Badge Payments	IDMS shall be capable to generate reports that show (itemized or grouped) all of the financial transactions by badgeholder (name, badge #, date, amount, payment method, payment type, etc.) grouped by company over any period of time (a day, a week, a month, year-to-date, or since system inception).		
R-113	Mandatory	Financial/ Badge Payments	Support user-defined badge billing rate classes by company and badge type, considering CHRC exemptions, external adjudication, and federal employee allowances.		
R-114	Mandatory	Financial/ Badge Payments	Restrict the ability to invoice badges only if the company is set up as billable.		
R-115	Mandatory	Financial/ Badge Payments	Integration with payment processing systems (Airport's PoS system) or with external services such as PayPal, Stripe, Square etc. - (vendor to suggest)		
R-116	Mandatory	General	The IDMS shall follow the badging procedures and regulatory requirements as outlined in the Code of Federal Regulations (CFR) Title 49 Chapter XII Part 1542, active aviation security policy enforcement, ASP amendments, National amendments issued and Security Directives (SD) 1542-04-08M or subsequent updates.		

R-117	Mandatory	General	IDMS shall assign a Unique ID number for each person employed at the airport regardless of the number of companies they work for and cannot be related to the person's name, SSN, or any other PII data. This ID will be used across all systems and will remain constant for that person.		
R-118	Mandatory	General	Allow capability to search the database using multiple fields and combinations of those fields as search criteria.		
R-119	Mandatory	General	IDMS shall be intuitive and easy to follow requiring minimum training. The UI shall drive the user to completing relevant tasks and clearly display next step and missing mandatory information.		
R-120	Mandatory	General	The IDMS shall clearly display on the badge holder record the stage / status the person is in at any given time. E.g. Pending security checks, incomplete training, fees not collected, etc.		
R-121	Mandatory	General	Ensure standard drop-down lists/master data values are sorted alphabetically (e.g. US states, Country names, Ethnicity,). Ensure commonly used drop down/ master data values are on the top (e.g. United states country when entering Passport or DL)		
R-122	Mandatory	General	The IDMS shall have field formatting and validations. For example: age minimum limit configurable, height cannot be in inches only and cannot be 10' or cannot accept alpha characters for age, height, weight. Ensure the UI enforces data type, field length, and formatting limitations as per all the dependent subsystems (i.e. PACS, fingerprinting etc.).		
R-123	Mandatory	General	Provide the capability to mask all or specific Personal Identifiable Information (PII) (e.g. SSN) and non-PII (e.g. PIN) data fields for display after initial input. The masking will be based on business rules and allow the airport to modify PII fields. The UI will clearly indicate if the data is entered or not entered or missing.		
R-124	Mandatory	General	Provide the capability that the masked data fields are viewable to certain user groups like Airport Security Manager, ASC or designees as determined by the Airport.		
R-125	Mandatory	General	Provide ability in the UI to override business rules (supervisor override) on a case-by-case basis to certain user groups (ASC, Security Manager). E.g.: applicant from Law enforcement agencies may not be always exempt from CHRC and STA, allows ASC or designee to override the global rule form the UI for the particular applicant)		
R-126	Mandatory	General	Allow field validations for name fields, date fields, zip codes, phone #s, SSN, DL#, Passports and ARN# etc. Allow selection of country, state where applicable.		
R-127	Mandatory	General	Provide ability to generate SSN's starting with 999-99 that is unique to the airport database for use by applicants that object to providing their own or are not required to provide SSN.		
R-128	Mandatory	General	Provide invalid or non-conforming entries (E.g. red color) on the screen and prevent invalid or incomplete submissions.		
R-129	Mandatory	General	Pop up indicating critical information (open citation/violation, terminated for cause, expiring documents, etc.) when record is opened by Authorized Signatory or Trusted Agents		

R-130	Mandatory	General	Support entering unlimited notes / comments associated with persons, company, security checks, training, badges, access levels, keys, each of which is automatically user/date/time stamped.		
R-131	Mandatory	General	Restrict Trusted Agent ability to change/delete comments they entered. Allow Security Manager or ASC or other designated Trusted agents to make modification to the comments entered by the Trusted agents.		
R-132	Mandatory	General	Provide ability to make comments private/ secured based on user roles		
R-133	Mandatory	General	Allow operators to flag a note/comment so that the note/comment will be immediately displayed when any user subsequently accesses the record until the user that made the comment, or a supervisor change or deletes the note/comment. For example: SOC users, LEO or CBP marks a record for suspension or revocation the Trusted Agent should get notification immediately.		
R-134	Mandatory	Integration Badging Equipment	DL/Passport credential verification system- to import information extracted from breeder documents - (new supplied by vendor)		
R-135	Mandatory	Integration Badging Equipment	Badge printers use existing or suggest alternate; Printer should have in-line encoding, laminate and internal reader to read the badge number back to IDMS.		
R-136	Mandatory	Integration Badging Equipment	Electronic signature capture - (new supplied by vendor)		
R-137	Mandatory	Integration Badging Equipment	Touchscreen - (new supplied by vendor)		
R-138	Mandatory	Integration Badging Equipment	Single fingerprint biometric enrollment and verification reader for person identity verification - (new supplied by vendor)		
R-139	Mandatory	Integration Badging Equipment	Multi-page high speed document scanner (new supplied by vendor)		
R-140	Mandatory	Integration Badging Equipment	External badge# reader and transmit badge number to IDMS - (new supplied by vendor)		
R-141	Mandatory	Integration DACS	The IDMS shall have capability to provide automated method to enroll badge holder in Rap back program upon submission of fingerprint to DACS and not wait for badge issuance. Standard Rap Back subscription, cancel and uncanceled rules applicable.		
R-142	Mandatory	Integration DACS	The IDMS shall have capability to integrate with DAC and submit the data for STA, CHRC and Rapback.		
R-143	Mandatory	Integration DACS	The IDMS shall have the capability to send notifications to the AS (via email to the AS) if the applicant has failed one or both (STA and CHRC) security checks. The IDMS shall track date when the security checks status was changed. The IDMS shall allow the Badging Office to set the background checks status to Appeals if the Applicant has appealed the CHRC results within 30 days. The IDMS shall limit further processing of training, badge issuance or payment for the applicant if the background check is in appeals process.		

R-144	Mandatory	Integration DACS	The IDMS shall track the date for the appeal review, interview and any additional documentation provided. The IDMS shall have capability to set the appeal result as Pass/ Fail, add notes and the date when the appeal process was complete. The IDMS shall limit the access to the appeals process and adjudication notes to ASM and Badging Office Superintendent user group.		
R-145	Mandatory	Integration DACS	The IDMS shall have capability to report on the appeals process timing, number of individuals that appealed the CHRC, interview dates, notes added for each individual.		
R-146	Mandatory	Integration DACS	The IDMS shall integrate with the LiveScan fingerprint devices.		
R-147	Mandatory	Integration DACS	The IDMS shall obtain change in status information from the DAC for CHRC and notify the Badging Office when the results are available on the FBI FPRD.		
R-148	Mandatory	Integration DACS	Automatically retrieve results from the DAC and update / populate matched STA results to the existing badge holder database.		
R-149	Mandatory	Integration DACS	The IDMS shall send notifications to AS and Applicant when security checks are complete, with instructions for next steps.		
R-150	Mandatory	Integration DACS	The IDMS shall have the capability to provide an automated method to enroll badge holders in the Rap Back program upon submission of fingerprint to DACS and not wait for badge issuance.		
R-151	Mandatory	Integration DACS	The IDMS shall provide capability to electronically submit the supporting documents to the DAC.		
R-152	Mandatory	Integration DACS	Provide the functionality to limit the review of background check results to authorized personnel.		
R-153	Mandatory	Integration DACS	DAC - for execution of STAs, CHRCs and (if possible CBP background checks); bi-directional, real time with demographic data - (existing system)		
R-154	Mandatory	Integration Fingerprint	Livescan Fingerprint system (existing system - GreenBit)		
R-155	Mandatory	Integration Mass Notification System	The IDMS shall integrate with the existing mass notification system (EverBridge) using the standard published APIs.		
R-156	Mandatory	Integration Mass Notification System	The IDMS shall integrate with the existing mass notification system (EverBridge) such that badge holders that have opted in and are Active in the system, their name and contact information (work phone, mobile, email, etc.) shall be broadcasted/ pushed to the EverBridge system.		
R-157	Mandatory	Integration Mass Notification System	The IDMS will keep track and report on all the companies and badge holders that are eligible for EverBridge notifications.		
R-158	Mandatory	Integration Mass Notification System	The IDMS will remove the badge holders from the EverBridge systems once the badge holder has either opted out or no longer has an Active badge at the airport.		
R-159	Mandatory	Integration Mass Notification System	The IDMS shall provide capability to report is the connection to the Ever bridge is lost.		
R-160	Mandatory	Integration Mass Notification System	EverBridge Version 8.2.0 -(existing system)		

R-161	Mandatory	Integration PACS	Update PACS with badge holder, badge, and clearance codes data immediately (within operational acceptable timeframe). Update requests shall be queued for processing without delay.		
R-162	Mandatory	Integration PACS	When an employee reports their badge as lost or stolen, the badge must immediately be deactivated in IDMS and the PACS.		
R-163	Nice to have	Integration PACS	Allow system to automatically grant and revoke access privileges in PACS, based on attribute changes, additions, and deletions.		
R-164	Mandatory	Integration PACS	Provide ability to display doors / gates access that is associated with a specific Clearance Codes.		
R-165	Mandatory	Integration PACS	Provide ability to manage higher level of grouping / mapping of clearance codes based on job titles, privileges (e.g. movement area driving would allow assignment of vehicle gate clearance and emergency privilege mapping to all access).		
R-166	Mandatory	Integration PACS	IDMS should have the ability to read back changes made in the PACS made by Security Operations Control Center for badge statuses. (e.g. Lost, stolen, revoked other available in PACS). All other changes should be tracked and reported / notified via email to the ASC, Security Manager		
R-167	Mandatory	Integration PACS	IDMS will provide a means to define and create templates or other methods of setting default clearance code / groups for employees of a company based on variables such as company name, company type, badge type, privileges, job title, department/division.		
R-168	Mandatory	Integration PACS	Provide capability to auto assign clearance codes at a minimum based on job title, company name, company type, badge type. Allow manual override of the clearance codes (adding or deleting) by the Trusted Agent.		
R-169	Mandatory	Integration PACS	Support an unlimited number of access levels per badge or credential type.		
R-170	Mandatory	Integration PACS	Bulk access levels assignments and removals from badge holders		
R-171	Mandatory	Integration PACS	Grouping of clearance codes and clearance groups		
R-172	Mandatory	Integration PACS	Physical Access Control System - C•CURE 9000 v2.7 - (existing system)		
R-173	Mandatory	Integrations Other	Airport Email system (Outlook, Office 365, etc.)		
R-174	Mandatory	Integrations Other	Airport's Active Directory for single sign-on for Airport's internal users (non-AS and non-Applicants)		
R-175	Mandatory	Reports	The IDMS shall provide reports for reconciling badge holder records between DAC and IDMS.		
R-176	Mandatory	Reports	The IDMS shall provide reports for financial reconciliation of fingerprinting, STA, CHRC and Rapback, eBadge fees against the DAC financial reports.		
R-177	Mandatory	Reports	Provide ability to list all open, closed, pending citations/violations.		
R-178	Mandatory	Reports	Generate reports based on the status of matches (e.g. cleared, under investigation, actual match), and be capable of being exported into multiple formats (at a minimum .csv, .pdf and .xlsx formats).		
R-179	Mandatory	Reports	Provide pre-defined reports, in a variety of formats that allow the user to select or specify the grouping and / or sorting criteria.		
R-180	Mandatory	Reports	Easily generate ad-hoc reports or queries without specialized skills (most easily via filtering, sorting, grouping).		

R-181	Mandatory	Reports	Provide ability for a system user to create new reports as well as modify existing reports.		
R-182	Mandatory	Reports	Daily and monthly reports will be created, stored, and managed within IDMS. Standard reporting tools, such as SQL Server Reporting Services or Crystal Reports must be supported.		
R-183	Mandatory	Reports	Reports sent using email will follow Sensitive Security Information (SSI) and Personally Identifiable Information (PII) policies.		
R-184	Mandatory	Reports	IDMS shall allow formatting of the report (e.g. header, footer, page #s, Airport logo, report titles, column headers).		
R-185	Mandatory	Reports	IDMS should provide following reports at a minimum: · Company names and company types · Company Count Total Badges (e.g. Active, Terminated, Expired, Unaccounted - lost/stolen, returned) · List of Authorized Signatories with details (e.g. Active/inactive, email, phone) · 30 -45- 60 Day Pending Badge Expirations · Active Badge Report with Badge type, privileges by Company · Security Checks reports by type and status (e.g. pending, submitted, results, DNI) including Rap Back · Security Checks (STA and CHRC) pending for more than 14 days · Badge Expiration By Company & Date · Badges Issued per day, month, quarter · No Badge pick-up after 30 days from security checks completion		
R-186	Mandatory	Reports	· Stop list, watch list, DNI list · Badgeholder Record with photo, all companies, privileges, biographic data · Training reports - practical training - administrator name, results, date taken, expiration date · 30 day pending Training expiration date · Audit Report by Company · Audit Report for all the badge holders badge status when the Audit is initiated · Audit Comparison Report of inaccuracy in the AS Audit AS closed report and the Audit Active status reports · IDMS User Activity Report · IDMS Audit report (all fields in IDMS old value, new value, date changed, user name who changed, workstation Id)		
R-187	Mandatory	Training	IDMS shall allow the manual entry security and operations training against the badgeholder profile. The IDMS shall have capability to track the name of the course, training coordinator, date completed and expiration dates.		
R-188	Future	Training	IDMS shall have capability to integrate with the computer-based training system to provision applicant records, training required based on the badge types and privileges requested and retrieve results (pass / fail), training language assistance if indicated in the badge application, training date and expiration dates automatically from the CBT.		

R-189	Mandatory	Training	IDMS shall allow the manual entering of additional non-CBT courses (e.g. practical driving training and other part 139 trainings) by Airport Operations staff and track the name of the training coordinator, date completed and expiration dates.		
R-190	Mandatory	Training	IDMS shall track the number of training attempts for specific training courses. IDMS will deny badge to applicants that do not pass after 3 attempts. Security Managers can override the condition.		
R-191	Mandatory	Training	Provide ability to add / modify training and set expiration date of training.		
R-192	Future	Training	The IDMS shall have the capability to restrict / control certain training courses. (e.g. Movement Area training is dependent on completing non-movement training.)		
R-193	Future	Training	Blank.		
R-194	Future	Training	Computer based training (CBT) platforms SSi or AAAE IET.		
R-195	Mandatory	User Roles	The IDMS shall allow at a minimum the following user role: Badging office Trusted Agents, Badging Office Manager, Airport Security Manager, Airport Security and Operations groups, Security Operations Center staff, other staff as per the airport requirements. Refer to the Future Business Process document for user roles and definitions.		
R-196	Mandatory	User Roles	Allow System Administrator the ability to assign a Trusted Agent, Airport Operations Control Center, etc. to a pre-defined user group. When a new person is assigned to that workgroup, the IDMS shall automatically receive all permissions associated with that user group definition.		

ATTACHMENT D – TECHNICAL REQUIREMENTS

Technical Requirements			VENDOR Response	
#	**Airport Requirement Description**	**Mandatory (M) Optional (O) Future (F)**	Identify the requirement meets as Product Feature (C) or Non-Compliant (NC)	Comments
1	**Hardware/ Software Integrations**			
1.01	Physical Access Control System - C•CURE 9000 v2.7 -(existing system)	M		
1.02	Livescan Fingerprint system - (new supplied by vendor)	M		
1.03	TSC DAC - for execution of STAs, CHRCs, RapBack and (if possible CBP background checks); bi-directional, real time with demographic data - (existing system)	M		
1.04	Integration with payment processing systems (Airport's PoS system) or with external services such as PayPal, Stripe, Square etc. - (vendor to suggest)	M		
1.05	EverBridge Version 8.2.0 -(existing system) - Future	M		
1.06	Computer based training (CBT) platforms - Future	F		
1.07	Customs and Border Protection (eBadge Program) - Future	F		
1.08	DL/Passport credential verification system- to import information extracted from breeder documents - (new supplied by vendor)	M		
1.09	Watch List and Stop List vetting of badge holders, badge applicants, and escorts	M		
1.10	Badge Printing using existing badge printers' system or suggest alternate)	M		
1.11	Touchscreen - (new supplied by vendor)	M		
1.12	Single fingerprint biometric enrollment and verification reader for person identity verification - (new supplied by vendor)	M		
1.13	Multi-page high speed document scanner (new supplied by vendor)	M		
1.14	External badge# reader and transmit badge number to IDMS - (new supplied by vendor)	M		
1.15	Airport Email system (Outlook, Office 365, etc.)	M		
1.16	Airport's Active Directory for single sign-on for Airport's internal users (non-AS and non-Applicants)	M		
2	**Platform**			
2.01	Architecture (hardware/software/networking) is based on industry standard practices and non-proprietary tools.	M		
2.02	The Airport is looking for on premise solutions that provide cost effective and operationally efficient IDMS.	M		

2.03	The Contractor shall provide server requirements, network requirements, database, storage, back-up server, badging workstations and other as needed to operate the IDMS.	M		
2.04	The Contractor shall provide details requirements for the network, firewall configurations, database, storage, back-up server and other as needed to operate the IDMS.	M		
2.05	Utilize communication links between the tiers of the application, which shall be encrypted using at least Transport Layer Security (TLS) 2.0 or latest, using at least a Secure Hash Algorithm (SHA)-256 certificate.	M		
2.06	Utilize servers that are capable of working with current versions of industry standard Anti-Virus software.	M		
3	**System Network requirements**			
3.01	System shall reside on an Airport provided secured Ethernet network. Network configuration and security will be the responsibility of the Airport in coordination with vendor system requirements.	M		
3.02	Vendor will coordinate IP addressing and routing with Airport network communications staff.	M		
3.03	Provide all communication paths within the application and to external interfaces and be documented by source Internet Protocol (IP), destination IP, and Transmission Control Protocol (TCP)/IP port.	M		
3.04	IDMS shall function in a network and server environment that is compatible with IEEE TCP/IP and 802.3 Ethernet series standards and 802.11X Wireless standards, shall support industry standard network protocols and ports, shall operate within the current Airport and Airport network architecture of local LANS and VLANS, and fiber backbones, and shall use and support industry standard network protocols and ports.	M		
3.05	The IDMS shall have capability to operate within a De-Militarized Zone (DMZ) with least common access rule base and any access to resources on the Internet must be approved by Airport IT.	M		
3.06	IDMS must support the use of firewalls, intrusion detection systems, virtual private networks, virus protection, encryption, access controls, password expiration, identity management, and other technologies to ensure that IDMS complies with all TSA Security requirements.	M		
3.07	IDMS shall provide system level tools (or protocols) to support network intrusion and performance monitoring by Airport IT applications.	M		
4	**Security requirements**			
4.01	Integration between IDMS on secure Airport network and systems connected via web services to external network (authorized signatory portal, Applicant portal, CBT, DAC, etc.) must be via secured protocol.	M		
4.02	Have the ability to encrypt sensitive and personally identifiable information at rest and in transit for internal as well as external users (AS and Applicant).	M		
4.03	The data should be encrypted using Transparent Data Encryption (TDE), when the selected Proposer's application database contains Personal	M		

	Identification Information (PII). The data needs to be encrypted in transit and at rest in the database.			
4.04	Provide the capability to mask all or specific Personal Identifiable Information (PII) (e.g. SSN) and non-PII (e.g. PIN) data fields for display after initial input. The masking will be based on business rules and allow the Airport to modify PII fields. The UI will clearly indicate if the data is missing.	M		
4.05	Interface to manage all secure user logins (trusted agents, authorized signatories, etc.	M		
4.06	Shall have capability to enforce password policy at a minimum follow the NIST Special Publication 800-63-3: Digital Authentication Guidelines: 1) Disallow use of vendor supplied password defaults for system passwords 2) Prevent passwords that are derivatives of the username 3) Enforce password requirements of > = 8 characters and contains characters from 4 of the following 4 categories: Uppercase alphabetic (i.e., A-Z), Lowercase alphabetic (i.e., a-z), - Numeric (i.e., 0-9), Special characters (e.g.,. ! %@*#^ () _+|~) 4) Require user to change password after first login 5) Require user to reset password after a set period (90 days or Airport configurable)	M		
4.07	System provides automated means for user password resets with authentication	M		
4.08	Times out IDMS web or client sessions according system administrator-configured period of idle time no longer than 30 minutes. The re-login should open the same screen/ page where auto logout triggered. IDMS mist saves work prior to auto time-out.	M		
4.09	Limit browser-based modules to accept only HTTPS connections for authentication purposes	M		
4.10	Prevent / Restrict storing of credit card data (number, expiration date, CSV# etc.) in the IDMS.	M		
4.11	Undo/rollback feature that reverts badge back to the prior state and logs it. For example, a badge is accidentally terminated, and the user can revert back to the prior state. Feature is controlled by user access and all rollbacks are logged	M		
4.12	Provide system security that is role-based allowing for update or read-only access to specific functions and obfuscation of defined data elements (i.e. SSN not visible or redacted on the screen for all users assigned to a specific role).	M		
4.13	Provide method(s) for the System Administrator to view and maintain user profiles such as: add new users, modify and delete user profiles.	M		
4.14	Provide details for cyber security based on NIS 800-171 and cyber security framework, including not limited to penetration testing, proprietary or 3rd-party, conducted by the vendor	M		
4.15	Provide details of a data breach Recovery Plan, including liability matrix	M		

4.16	As soon as security vulnerability is identified, the vendor shall be responsible to provide up-to-date IDMS application security patches and/ or hot fixes as it relates to access to IDMS or data within 30 days of risk identified or security patch release.	M		
5	**System Audit**			
5.01	Automatic audit trail logging and generate report of all data sent to integrated systems (PACS, DAC, CBT etc.), web calls, acknowledgement received from the integrated systems, status of messages - success/ fail, error coding of failure.	M		
5.02	IDMS shall provide system integration audit report with error codes and actionable information to fix error.	M		
5.03	The system should have capability to log and generate report for data updated by any user - table, field, old value, new value, user ID, date/time	M		
5.04	Automatic audit trail logging and generate report for all queries and reports run - query/report name or SQL code, date/time, user	M		
6	**System Performance requirements**			
6.01	System shall be available 24/7; design shall be reflective of that business environment such that no single point of failure will disrupt operations.	M		
6.02		M		
6.03	System performance measured in terms of responsiveness and stability under a particular workload, verifies other quality attributes of the system (e.g., scalability, reliability), or simulates the business operational use of a system solution to discover improvement requirements.	M		
6.04	Sub 5-second response time to return on individual screens and day-to-day activities such as typical searches, cardholder record search and load, certain reports, photo capture, on-save screen refresh etc.	M		
6.05	Ability to store an unlimited number of scanned documents so long as there is sufficient disk space.	M		
6.06	The IDMS shall be available at all times to support business operations. Provide details of (east coast hours) telephone or email customer support services. Provide access for the Airport to the vendor online tracking system with ticket numbers and real time updates for technical issues being resolved. Provide details of minimum and maximum response times that should be expected for vendor to resolve service issues.	M		
6.07	Provide details of vendors change management program and provide examples of change management documentation that is currently used.	M		
6.08	The IDMS shall be able to operate without being kicked out of the badging system and having to restart.	M		
6.09	Vendor shall support the utilization of backup and recovery management software that will allow for a recovery of full application functionality and data. Vendor shall propose recovery plan for Airport's review.	M		

6.10	Provide ability to monitor and automatically report system health, notifying support staff using standard technologies such as SMS and SNMP	M		
6.11	IDMS shall have capability to detect loss of connection with external systems, queue the messages and automatically re-transmit once the connection is re-established.	M		
6.12	The proposer shall comply with the Airport's data retention policy requirements.	M		
7	**Licenses required**			
7.01	All software and licenses necessary to run the IDMS system on Airport provided hardware (workstations with peripherals) must be included in the Proposal.	M		
7.02	The contractor shall clearly list the 3rd party licenses that will be provided by the contractor, unit price, quantities, and licenses that the Airport needs to provide for IDMS.	M		
7.03	If determined to be cost effective, the Airport may decide to provide certain equipment per Proposer specification for this project. The proposer should submit pricing, options, and roles for configuration as part of the proposed solution.	M		
8	**System Warranty**			
8.01	Warrantied for one year after formal written acceptance of system; Including all labor, version upgrades, upgrades to remain compliant with regulatory changes, support, and preventive maintenance typically included in annual maintenance	M		
8.02	Include an explanation of the system's warranty coverage, and includes optional extended maintenance agreement/warranty options. All non-emergency system maintenance will be completed after hours.	M		
8.03	Provide all software upgrades in the first-year warranty and included in subsequent years as part of any maintenance agreement.	M		
8.04	Includes all updates to remain compliant with TSA 49 CFR Part 1542 and other applicable regulatory requirements including Security directives, National Airport Security Programs (ASP) Amendments.	M		
8.05	New required fields created to comply with TSA SDs or other reasons must be prepopulated to prevent null values	M		
8.06	Includes all regular version upgrades	M		
8.07	Includes keeping integrations current with new releases of integrated products	M		
8.08	Provide updated SOPs for all software upgrades.	M		
8.09	Provide training for Airport staff for all significant software changes or upgrades at a minimum via web conferencing / videoconferencing.	M		
9	**System Support and Maintenance**			
9.01	Provide two consecutive weeks of onsite engineering support post "go live".	M		
9.02	Proposer shall explain active data storage and archiving methodologies.	M		

9.03	Proposer shall provide requirements for remote access to IDMS during implementation, testing and post implementation.	M		
9.04	Includes all updates to remain compliant with TSA 49 CFR Part 1542 and other applicable regulatory requirements	M		
9.05	New required fields created to comply with TSA SDs or other reasons must be prepopulated to prevent null values	M		
9.06	Includes all regular version upgrades	M		
9.07	Includes keeping integrations current with new releases of integrated products	M		
9.08	Provide updates, enhancements and/or bug fixes to the System at no additional charge (for license or labor) during the term of any maintenance/service agreements. All System changes shall be conducted after hours in coordination with Airport staff.	M		
9.09	Provide software license agreement that is not dependent on the maintenance agreement.	M		
9.10	Attend project completion and lessons learned meeting at the Airport approximately 4-5 months post "go live" to assess and comment on the project.	M		
10	**Data Migration - Data analysis, reconciliation and migrations**			
10.01	A data mapping exercise must be conducted to map existing fields in PACS and determine fields must be maintained in the IDMS.	M		
10.02	Data cleansing must be conducted prior to implementation for remediation of data issues. A review of existing badges must be completed for badge color and access consistency, data accuracy, missing data fields, and compliance. Manual and system automated cleansing may be used.	M		
10.03	The contractor shall perform data analysis and provide reconciliation reports across all data sources integrated in the IDMS including but not limited to PACS, DAC and Finance system.	M		
10.04	The contractor shall provide reconciliation reports clearly identifying the data mismatches, duplicates records, missing and inconsistent data fields (DoB, SSN, etc.) and action plan for normalizing the data. The recommendations can include automated scripts to fix the data by the contractor, manual clean up missing information by Airport or other 3rd party system updates.	M		
10.05	The new Unique Person ID number field must be generated for all existing employees during the data import to IDMS.	M		
10.06	The Unique Personal Identifier must be assigned to each existing badge holder during migration in IDMS and similarly provide plan to update other systems PACS, DAC etc.	M		
10.07	The contractor shall perform data analysis and provide reconciliation reports in progressively and iterative method.	M		
10.08	Identify all data to be migrated into the IDMS in a transition plan, which shall include a data migration validation. The contract shall perform data migrations during every system acceptance testing iteration.	M		

10.09	The contract shall perform data migrations Dry-run test to validate assumptions for time taken to migrate data, perform quality check of the migrated data.	M		
10.10	Proposer shall include a back out plan for all data and processes in the event the go-live event does not execute as planned	M		

ATTACHMENT E - COST PROPOSAL WORKSHEET

Norfolk International Airport Identity Management system (IDMS) Project

Vendor-

General Pricing Workbook Instructions

All costs must be identified within this pricing workbook. All proposal components (hardware, software, services, maintenance, misc) must be priced separately. Shipping costs and taxes must be identified. Vendor may return a copy of the Pricing Workbook as a PDF, but one submitted copy must remain in EXCEL format within the printed file and the electronic copy.

1- Hardware

Vendor will specify the following information (within the description field below) for all proposed hardware including (but not limited to); Make, Model, Type and Warranty. Pricing shall not be “bundled”, all hardware and software will be priced on a “per unit bases”. Vendor will use the sections "Proposal Reference Page Number" to identify where in their proposal the relevant information can be located.

Item	Description	Quantity	Unit Price	Extended Price	Proposal Reference Page Number	Notes
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
Sub-Total Hardware				$0.00		

2- Software						
Vendor will specify the following information (within the description field below) for all proposed software including (but not limited to); Name, Version and Type (O/S, application, interface). If the Vendor is proposing a "site license", the relevant terms and conditions must be referenced, including maximum number of licenses (concurrent or consecutive), location and agency restrictions. Vendor will use the sections "Proposal Reference Page Number" to identify where in their proposal the relevant information can be located.						
Item	Description	Quantity	Unit Price	Extended Price	Reference Page Number	Notes
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
Sub-Total Software				$0.00		

3- Services						
Vendor will specify the following information (within the description field below) for all proposed services, including (but not limited to); Project Management, Configuration and Implementation, Interface Configuration and Implementation, Hardware Installation and Setup, Training, Development of Training Materials and if applicable Sub-Contractor services. Vendor will use the sections "Proposal Reference Page Number" to identify where in their proposal the relevant information can be located.						
Item	Description	Quantity	Unit Price	Extended Price	Reference Page Number	Notes
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
Sub-Total Services				$0.00		

4- Interfaces						
All "Optional Services & Interfaces" identified in the RFP are to be included in this section. Vendor will use the sections "Proposal Reference Page Number" to identify where in their proposal the relevant information can be located.						
Item	Description	Quantity	Unit Price	Extended Price	Proposal Reference Page Number	Notes
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
Sub- Total Optional						

5 – Maintenance Software						
Vendor will specify the following information (within the description field below) for all proposed maintenance charges including (but not limited to); Proposed Maintenance Period. Vendor will use the sections "Proposal Reference Page Number" to identify where in their proposal the relevant information can be located.						
Item	Description	Quantity	Unit Price	Extended Price	Proposal Reference Page Number	Notes
Year 1 (Warranty)				$0.00		
Year 2				$0.00		
Year 3				$0.00		
Year 4				$0.00		
Year 5				$0.00		
Year 6				$0.00		
Year 7				$0.00		
Sub- Total Maintenance				$0.00		

6 – Maintenance Hardware						
Vendor will specify the following information (within the description field below) for all proposed maintenance charges including (but not limited to); Proposed Maintenance Period. Vendor will use the sections "Proposal Reference Page Number" to identify where in their proposal the relevant information can be located.						
Item	Description	Quantity	Unit Price	Extended Price	Proposal Reference Page Number	Notes
Year 1 (Warranty)				$0.00		
Year 2				$0.00		
Year 3				$0.00		
Year 4				$0.00		
Year 5				$0.00		
Year 6				$0.00		
Year 7				$0.00		
Sub- Total Maintenance				$0.00		

7- Miscellaneous						
Vendor will specify the following information (within the description field below) for all proposed miscellaneous charges including (but not limited to); Shipping, Travel, Documentation, Printing..etc. Vendor will use the sections "Proposal Reference Page Number" to identify where in their proposal the relevant information can be located.						
Item	Description	Quantity	Unit Price	Extended Price	Proposal Reference Page Number	Notes
				$0.00		
				$0.00		
				$0.00		
				$0.00		
				$0.00		
Sub- Total Miscellaneous				$0.00		

8- Project Cost Summary		
Item	Extended Price	Notes
8a- System Costs		
Hardware	$0.00	
Software	$0.00	
Services	$0.00	
Maintenance Software	$0.00	
Maintenance Hardware	$0.00	
Miscellaneous	$0.00	
Sub-Total System Costs	$0.00	
8b- Optional Costs		
Sub-Total Optional Costs	$0.00	
9- Project Total Costs		
Total All Costs	$0.00	

ATTACHMENT F: SERVICE PROVIDER AGREEMENT

NORFOLK AIRPORT AUTHORITY

SERVICE PROVIDER AGREEMENT

IDENTITY MANAGEMENT SYSTEM: RFP #

THIS SERVICE PROVIDER AGREEMENT ("AGREEMENT") is entered this _____ day of _____, 2023,between the **NORFOLK AIRPORT AUTHORITY**, a political subdivision and independent special district of the Commonwealth of Virginia ("Authority") located at 2200 Norview Avenue, Norfolk, Virginia 23518, and **[Contractor Name**], a [State of Incorporation] corporation, authorized to do business in the Commonwealth of Virginia and having a business address of [Address of Corporation], FEI No. [FEI Number], ("Contractor") (the Authority and Contractor are referred to throughout this Agreement as the "Parties").

W I T N E S S E T H:

WHEREAS, the Authority is seeking a comprehensive and automated Identity Management System (IDMS) for issuing Airport Identification badges (the "Project") to serve the Norfolk International Airport ("Airport" or "ORF"); and

WHEREAS, Authority has conducted a competitive selection process under the Virginia Public Procurement Act, Ch. 43, Virginia Code, issuing a Request for Proposals ("RFP") to obtain the services described above and more specifically described in the RFP, Scope of Services, and has selected Contractor to provide those services; and

WHEREAS, Contractor has submitted a proposal in response to RFP ____ seeking to providethose services and represents that it has expertise in the type of services required.

NOW, THEREFORE, in consideration of the above, the terms and provisions contained herein, and the mutual consideration described below, the Parties agree as follows:

ARTICLE 1 - RECITALS

The recitals as set forth above are true and correct and are incorporated into theterms of this Agreement as if set out herein at length.

ARTICLE 2 - SCOPE OF SERVICES

2.1. Contractor will provide all services necessary to build and deploy an automated Identity Management System to the Authorityfor the Project, as described in Exhibit "A", "Scope of Services," attached to this Agreement and incorporated herein, and as assigned by Authority during the term ofthis Agreement. These services will include serving as Authority's primary Contractor for all tasks described in Exhibit "A" and the RFP, and providing the customary services associated with implementation and deployment of the Project.

2.2. Contractor has represented to Authority that it has expertise in the type of services that will be required by the Scope of Services. Contractor agrees that all services provided by Contractor under this Agreement are subject to Authority's review and approval and will be performed according to the normal and customary standards of practice for firms with special

expertise in the type of services required by this Agreement, and in compliance with all laws, statutes, ordinances, codes,rules, regulations and requirements of any governmental agencies which regulate or have jurisdiction over those services. If Contractor becomes aware of any conflicts in these requirements, Contractor will notify Authority of such conflict in writing and utilize its best judgment to resolve the conflict.

ARTICLE 3 - TERM OF AGREEMENT

3.1 The term of this Agreement commences on the date first written above and continues for a term as described below. If a Contract Amendment or Task Authorization is issued that will require work to continue beyond the Expiration Date, neither Agreement nor Authorization may extend the term of this Agreement for more than six (6) months from the Expiration Date.

- IDMS Implementation and Go-live.
- Year 1: Warranty, Support & Maintenance (No cost to ORF)
- Years 2, 3, 4 & 5: Maintenance and Support
- Years 6 & 7: Maintenance and Support (Option Periods extended by the Authority)

3.2. Authority will have the option to extend the initial term of this Agreement forup to two (2) additional years in one (1) year increments from the Expiration Date of the initial term or any extended term. Each extension is subject to successful negotiation by the Parties of a scope of work and compensation schedule for the extended term.

3.3. To exercise its option to extend the initial term, or any extended term of this Agreement, Authority must give Contractor written notice of its intent to exercise its optionto extend at least ninety (90) days before the then current term expires. Any extended term will be agreed to in writing and executed by the Parties with the same formality as this Agreement.

ARTICLE 4 - CONTRACTOR'S RESPONSIBILITIES

Contractor will:

4.1. If necessary, obtain and maintain throughout the term of this Agreement all licenses required to do business in the Commonwealth of Virginia and in the City of Norfolk, including, but not limited to, all business and other licenses required by any governmental agency responsible for regulating and licensing the services provided by Contractor under this Agreement.

4.2. Agree that when services provided under this Agreement relate to services which, under Virginia law, require a license, certificate of authorization or other form of legal entitlement to practice such services, Contractor will employ and/or retain only qualified personnel to provide those services.

4.3. Employ and designate a qualified licensed individual to serve as Contractor's project manager ("Project Manager"). Contractor must designate its Project Manager in writing within five (5) calendar days after receiving an executed original of this Agreement. Contractor's Project Manager designation must be executed by the proper officers of the Contractor and will acknowledge that the Project Manager will have full authority to bind and obligate Contractor on all matters arising out of or relating to this Agreement. The Project Manager will be specifically authorized and responsible to act on behalf of Contractor with respect to directing, coordinating, and administering all aspects of the services provided under this Agreement. The person selected as Contractor's Project Manager will be subject to the prior approval and acceptance of the Authority. The contractor further agrees not to change its designated Project Manager, or the location or duties assigned to the Project Manager, without prior written consent of the Authority.

4.4. Agree to promptly remove and replace the Project Manager, or any other personnel employed or retained by Contractor, or any subcontractor, or any personnel of any such subcontractor, engaged by Contractor to provide services under this Agreement, within fourteen (14) calendar days of receipt of a written request from the Authority, which may make such requests in its sole discretion, with or without cause.

4.5 Agree to be responsible for the quality, technical adequacy and accuracy, timely completion, and the coordination of all data, studies, reports, memoranda, other documents and other services, work and materials performed, provided, and/or furnished by Contractor. The Contractor will, without additional compensation, correct or revise any errors, omissions, or other deficiencies in such data,studies and other services, work, and materials.

4.6 Agree that neither review, approval, nor acceptance by Authority of any data, studies, reports, memoranda, and incidental services, work or materials furnished hereunder by the Contractor will in any way relieve Contractor of responsibility for the adequacy, completeness and accuracy of its services and the quality of Contractor's work and materials. Neither the Authority's review, approval, or acceptance of, nor payment for, any part of the Contractor's services, work and materialswill be construed to operate as a waiver of any of the Authority's rights under this Agreement or any cause of action it may have arising out of the performance of this Agreement.

4.7. If requested by Authority, and needed for project implementation, maintain for the duration of this Agreement a localoffice at ORF staffed by Contractor's Project Manager.

4.8. Comply with all federal, state, and local laws and building requirements. Contractors will devote particular attention to complying with Federal Aviation Administration (FAA) regulations, requirements, and Advisory Circulars. The Contractor must also comply with all pertinent grant agreements and grant conditions applicable to each Contract Amendment or Task Authorization. Authority will provide the Contractor withone copy of any specific and unique grant or regulatory requirements on a task-by-task basis prior to or concurrent with issuance of any Contract Amendment or Task Authorization.

4.9. Acknowledge that Authority may be undertaking improvements or renovations at

the Airport and agrees to coordinate the performance of its services under this Agreement as directed and required by the Authority so as not to interfere with, disrupt or delay any work. The contractor further agrees to coordinate its efforts with the Authority's other architects, engineers, designers, or construction managers for that work.

ARTICLE 5 - ADDITIONAL SERVICES OF CONTRACTOR

Additional Services refer to services requested by the Authority that arenot specifically set out in the Scope of Services.

Additional Services may include, but are not limited to:

5.1. Preparation of applications and supporting documents (except those already to be furnished under this Agreement) for private or governmental grants, loans, for or advances in connection with any Project or Task.

5.2. Services resulting from significant changes in the general scope, extent or character of any assignment including, but not limited to, changes in size, complexity, Authority's schedule or character of construction; and revising previously acceptedstudies, reports, designs or documents when such revisions are required by changes in laws, rules, regulations, ordinances, codes or orders enacted subsequent to and not reasonably anticipated prior to the preparation of such studies, reports, designs or documents, or that are due to any causes beyond Contractor's control and fault.

5.3. Providing models for Authority's use.

5.4. Furnishing services of independent associates and Contractors for services other than those to be provided by Contractor under this Agreement.

5.5. Services during out-of-town travel required of Contractor and as directed by Authority, other than visits to any Project site or Authority's offices.

5.6. Assistance in connection with bid protests, rebidding or renegotiating contracts for construction, materials, equipment, or services, except as otherwise provided for herein.

5.7. Additional services rendered by Contractor in connection with any assignment, not otherwise provided for in this Agreement or not customarily furnished inaccordance with generally accepted information technology practices.

Any additional services may be authorized only by a written amendment to this Agreement, signed by both Parties prior to commencement of any additional services. Any additional services agreed to by the Parties will constitute a continuation of the services requested under this Agreement and must be provided and performed in accord with the terms of this Agreement and any amendment to this Agreement. Any amendment will describe: (1) the scope of the additional services requested; (2) the basis of compensation; and (3) the period or performance schedule forcompletion of the additional services.

ARTICLE 6 - RESPONSIBILITY FOR ESTIMATES

6.1 If the Contractor is required to evaluate a project budget and prepare preliminary

or detailed estimates of probable cost for any project or portion of aproject, Contractor will ensure that all evaluations and estimates represent Contractor's best judgment consistent with industry standards. For purposes of the Liability Provisions of this Article only, the Contractor's evaluations or estimate(s) will be considered valid and effective for a period of six (6) months from the date Authority accepts the evaluation or estimate(s).

6.2. Budget Evaluations - Budget in this case applies to the Authority's budget and not to the budget as a project-controlled document. A budget is prepared with the use of flowsheets, layouts, and equipment details. This type of evaluation will be accurate within twenty-five percent (25%) of the cost of construction of the Project. If thebids, as described above, fail to meet this prescribed accuracy, the cost associated withthe preparation of the Budget Evaluation will be repaid by Contractor to Authority or deducted from any fees owing Contractor by Authority.

6.3. Implementation Estimates - When preparing and submitting preliminary or detailed estimates of probable implementation and deployment cost to the Authority for any project or portion of the Project, the Contractor, by exercise of its experience, effort, knowledge and judgment, will insure that all estimates represent Contractor's best judgment consistent with industry standards will be held accountable, responsible and liable for the accuracy and completeness of any and all such cost estimates.

ARTICLE 7 - AUTHORITY'S RESPONSIBILITIES

Authority will:

7.1. Designate in writing a project manager to act as Authority's representative with respect to the issuance of Contract Amendment or Task Authorizations for services rendered under this Agreement ("Authority Project Manager"). The Authority's Project Manager, President/Chief Executive Officer, or other authorized designee(s) will have authority to execute Contract Amendments, Task Authorizations, and any modifications or changes to Contractor's (1) scope of services; (2) time of commencement or delivery; or (3) compensation related to services required under any Contract Amendment or Task Authorization. The Authority Project Manager will have authority to transmit instructions, receive information, and interpret and define the Authority's policies and decisions with respect to Contractor's services underthis Agreement. The Authority Project Manager will review and make appropriate recommendations on all requests for payment for services submitted by Contractor.

7.2. The Authority Project Manager is not authorized to, and will not, issue anyverbal orders or instructions to Contractor that would have the effect, or be interpreted tohave the effect, of modifying or changing in any way whatever the: (1) scope of services provided and performed by Contractor hereunder; (2) the time the contractor is obligated to commence and complete all such services; or (3) the compensation Authority is obligated or committed to pay Contractor.

7.3. Provide all criteria and information requested by Contractor as to Authority's requirements for any project or task, including design objectives and constraints, space, capacity and performance requirements, flexibility and expandability,and budgetary limitations.

7.4. Upon request from Contractor, make available to Contractor all available information in Authority's possession pertinent to any Contract Amendment or Task Authorization, including existing drawings, specifications, shop drawings, product literature, previous reports and any other data concerning design or construction of a project.

7.5. Arrange access, in accordance with Authority's security regulations, for Contractor to enter any Project site to perform services. The contractor acknowledges thatAuthority may provide such access during times that are not the Contractor's normal business hours.

7.6. Notify Contractor of any defects or deficiencies in services rendered by Contractor.

ARTICLE 8 – NOTICE TO PROCEED, CONTRACT AMENDMENTS, TASK AUTHORIZATIONS AND TIME FOR COMPLETION OF SERVICES

8.1. Contractor will not commence work under this Agreement until it receives a fully executed copy of this Agreement and a written Notice to Proceed. Following the Notice to Proceed and during the term of this Agreement, Authority may assign specific tasks by Contract Amendment or Task Authorization, to be signed by both Parties. Each contract amendment or Task Authorization must include a lump sum or not-to-exceed compensation amount and a schedule of services required or a delivery date for all services.

8.2. All tasks outlined in the Agreement are contingent upon execution of a Task Authorization Form.

8.3 Time is of the essence for all services provided under this Agreement. Authority may suffer damage if Contractor does not complete the required services in a timely manner. Contractor therefore agrees to employ or retain adequate personnel and subcontractors throughout the term of this Agreement to complete all services in a timely and diligent manner.

8.4. If Contractor is obstructed or delayed in the prosecution or completion of its services as a result of unforeseeable causes beyond the control of Contractor, and not due to its own fault or neglect, including but not restricted to: acts of God or of public enemies, acts of government or of Authority, fires, floods, epidemics, quarantine regulations, strikes or lock-outs, then Contractor must notify the Authority in writing withinseventy-two (72) hours after commencement of such delay, stating the cause or causes thereof, or be deemed to have waived any right which Contractor may have had torequest a time extension.

8.5. No interruption, interference, inefficiency, suspension, or delay in the commencement or progress of Contractor's services from any cause whatsoever, including those for which Authority may be responsible in whole or in part, will relieve Contractor of its duty to perform services or give rise to any right to damages or additional compensation from Authority. Contractor's sole remedy against Authority will be the right to seek an extension of time to its schedule. This paragraph will expressly apply to claims for early completion, as well as claims based on late completion. Provided, however, if through no fault or neglect of Contractor, the services relating to a specific Contract Amendment or Task Authorization hereunder have not been completed within twenty-four (24) months of the date that Contract Amendment or Task Authorization was signed by both Parties, Contractor's compensation for that Contract Amendment or Task Authorization will be equitably adjusted, with respect to those services that have not yet been performed, to reflect the incremental increase in costs experienced by Contractor after expiration of said twenty-four (24) month period.

8.6. If Contractor fails to commence, provide, perform or complete any of the services to be provided hereunder in a timely and diligent manner, in addition to any otherrights or remedies available to Authority hereunder, Authority at its sole discretion and option may withhold any and all payments due and owing to the Contractor until such time as the contractor resumes

performance of its obligations in such a manner so as to establish toAuthority's satisfaction that Contractor's performance is or will shortly be back on schedule.

ARTICLE 9 - COMPENSATION AND METHOD OF PAYMENT

9.1. Authority will pay Contractor for all authorized services provided by Contractor under this Agreement as prescribed in Exhibit "B", "Basis of Compensation," which is attached hereto and incorporated by reference, and as set forth in this agreement or any individual Task Authorizations executed by the Parties. Contractor willbe compensated on a lump-sum basis on completion of a particular Task over the courseof Contractor's services for Work in Progress, based on a monthly statement of services,as follows:

a. **Lump Sum** - Upon Authority's acceptance of Contractor's work, Authority will pay Contractor a lump sum as specified in the Task Authorization or Contract Amendment.

Lump Sum is a contracting method utilized by the Authority whereby scope equals fee. Lump Sum fees will be based on assumptions/estimates of personnel, hourly rates, man hours, indirect expenses, time durations, etc. needed to effectively accomplish the scope of work. As such, the project assumptions made duringgood faith negotiations are the basis for the Lump Sum fee. The Lump Sum scope equals the Lump Sum fee. As such, the Lump Sum fee is not guaranteed regardless of scope or time impacts to the project. If at any time during the progression of work underthis Contract the project assumptions and resulting agreed upon scope of work substantially or materially change, then the Lump Sum fee will be adjusted to reflectthese changes by a Contract Amendment.

Lump Sum Fees are understood and agreed to include all direct and indirect labor costs, personnel related costs, overhead and administrative costs, costs ofsub-Contractor(s) and/or subcontractor(s), out-of-pocket expenses and costs, service fee(s) and any other costs or expenses which may pertain to the services and/or work to be performed, provided and/or furnished by the Contractor as may be required and/or necessary to complete each and every task set forth in the Scope of Services, or as may be set out in subsequent Contract Amendments, and/or Task Authorizations agreed to in writing by both Parties to this Agreement.

b. **Monthly Statements** - Contractor may submit an invoice to Authority's Development Division each calendar month covering services rendered and completed during the preceding calendar month. Contractor's invoice must be itemizedto correspond to the basis of compensation as set forth in the Task Authorization or Contract Amendment, expressed as a percentage of the total work to be performed underthat Task Authorization or Contract Amendment.

c. **Non-Personnel Reimbursable Expenses** – If authorized, Authoritywill further compensate Contractor for non-personnel reimbursable expenses and costs as set out in Exhibit "B-1", attached and incorporated by reference.

d. **Not-To-Exceed Fee(s)** - When all, or any portion, of the Contractor'scompensation for performing services required in the Scope of Services or any ContractAmendment or Task Authorization(s), is established on a Not-to-Exceed (N.T.E.) amountbasis, it is mutually understood and agreed that such compensation for each CompletedTask will be made on the following basis:

i. For the actual hours necessary, required and expended by the Contractor and

technical personnel, multiplied by the applicable hourlyrates for each classification or position as set forth in Exhibit "B" to this Agreement; and

ii. For the actual necessary, required and expended non-personnel reimbursable expenses and costs, multiplied by the applicable charge foreach item as set forth in Exhibit "B-1"; and

iii. With the understanding and agreement that the Authority will pay the Contractor for all such costs and expenses within the established Not-to-Exceed amount for each Task or Sub-Task subject to the Contractor presenting an itemized and detailed invoice with appropriate supporting documentation attached thereto to show evidence satisfactory to the Authority covering all such costs and expenses; and

iv. With the understanding and agreement that the Contractor's invoices and all payments to be made for all Not-to-Exceed amounts will be subject to the review, acceptance, and approval of the Authority; and

v. With the understanding and agreement that when the Contractor's compensation is established on a Not-to-Exceed basis for a specific Task(s)or Sub-Task(s) the total amount of compensation to be paid the Contractor to cover all personnel costs, non-personnel reimbursable expenses and costs, and Sub-Contractor and Sub-Contractor costs for any such specific Task(s) or Sub-Task(s) will not exceed the amount of the total Not-to-Exceed compensation established and agreed to for eachspecific Task(s) or Sub-Task(s).

e. **Authorization to Commit Funds** - All Tasks outlined in the Agreement are contingent upon execution of a Contract Amendment or Task Authorization Form. The Board of Port Commissioners' approval and execution of this Agreement does not commit the Authority to the expenditure of any federal, state, local orfunds for any service listed in this Agreement. Only by execution of a Contract Amendment and subsequent Task Authorization is the expenditure of funds authorized and committed. Contractor and Authority understand, recognize, and agree that there isno presumption of funding availability, authorization to work or commitment for future work until an appropriate Contract Amendment or Task Authorization is executed by both parties. Tasks may be authorized in whole or in part.

9.2. Authority will issue payment to Contractor within forty-five (45) calendar days after receipt of an invoice in an acceptable form and containing the requested breakdown and detailed description and documentation. If Authority objects or takes exception to the amount of any Contractor invoice, Authority will notify Contractor in writing of such objection or exception within the forty-five (45) day period. If such objection or exception remains unresolved at the end of the forty-five (45) day period, Authority will withhold the disputed amount and make payment to Contractor of all amounts not in dispute. Payment of any disputed amount will be resolved by mutual agreement of the Parties.

9.3. Failure by the Contractor to follow the instructions set out above will result inan unavoidable delay in payment by the Authority.

9.4. If this Agreement is terminated for the convenience of the Authority, the Authority will compensate the Contractor for: (1) all services performed prior to the effective date of termination; (2) reimbursable expenses then due; and (3) reasonable expenses incurred by the Contractor in effecting the termination of services and work, and incurred by the submittal to the Authority of any Project documents.

9.5. If Authority suspends the Contractor's services or work on all or part of theservices required by this Agreement, the Authority will compensate the Contractor for allservices performed prior to the effective date of suspension and any reimbursable expenses then due along with any reasonable expenses incurred or associated with or incurred as a result of such suspension.

9.6. If services required under this Agreement are terminated, canceled, or decreased due to: (1) termination; (2) suspension in whole or in part; and (3) and/or aremodified by the subsequent issuance of Contract Amendment(s); the Contractor will not be entitled to receive compensation for anticipated fees; profit, general and administrativeoverhead expenses or any other anticipated income or expense which may be associated with the services which are terminated, suspended, eliminated, canceled or decreased.

9.7. The Contractor may cross-utilize funds from the various Tasks assigned to accomplish the overall purpose and goal of this Agreement provided Contractor has obtained prior written approval from the Authority. The Authority will review the need for such request and the impact on other assigned Tasks. In doing so, the Authority retains the authority to delete any Task outlined in the Scope of Services.

ARTICLE 10 – NON-APPROPRIATION CLAUSE

All funds for payment by the Authority under this Agreement are subject to the availability of an annual appropriation for this purpose by the Authority. In the event of non-appropriation of funds by the Authority for the services provided under this Agreement, the Authority will terminate the Agreement, without termination charge or other liability, on the last day of the then current fiscal year or when the appropriation made for the then-current year for the services covered by this Agreement is spent, whichever event occurs first. If at any time funds are not appropriated for the continuanceof this Agreement, cancellation will be accepted by the Contractor on thirty (30) days prior written notice, but failure to give such notice will be of no effect and the Authority will not be obligated under this Agreement beyond the date of termination.

ARTICLE 11 - FAILURE TO PERFORM

If Contractor fails to commence, perform and/or complete any of the services andwork required under this Agreement in a timely and diligent manner, the Authority may consider such failure as cause to terminate this Agreement. As an alternative to termination, the Authority may, at its option, withhold any or all payments due and owingto the Contractor, not to exceed the amount of the compensation for the work in dispute,until such time as the Contractor resumes performance of its obligations in accordance with the time and schedule of performance requirements set forth in this Agreement.

ARTICLE 12 - PUBLIC RECORDS

Contractor acknowledges that any information concerning its services may beexempt from disclosure under the Virginia Freedom of Information Act (“FOIA”). All information relating to the security systems for any property owned by or leased to the Authority and all information relating to the security systems for any privately-owned or leased property which is in Authority's possession, including all records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to or revealing such systems or information, and all meetings relating directly to or that would reveal suchsystems or information, is confidential and exempt from disclosure.

Contractor agrees not to divulge, furnish, or make available to any third person, firm or organization, without Authority's prior written consent, or unless incidental to the proper performance of Contractor's obligations hereunder, or in the course of judicial or legislative proceedings where such information has been properly subpoenaed, any confidential or exempt information concerning the services to be rendered by Contractorhereunder. The contractor will require all its employees, agents, subcontractors to comply with the provisions of this Article.

ARTICLE 13 – CONTRACTOR'S PUBLIC RECORDS OBLIGATIONS

Contractor specifically acknowledges its obligation to comply with Virginia law regarding public records, and will:

(1) Keep and maintain public records that ordinarily and necessarily would be required by the Authority to perform the services required under this Agreement.

(2) Upon request from the Authority, provide the Authority with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided under FOIA or as otherwise provided by law.

(3) Ensure that public records that are exempt or confidential and exempt frompublic records disclosure requirements are not disclosed, except as authorized by law; and

(4) Meet all requirements for retaining public records and transfer, at no cost tothe Authority, all public records in possession of Provider upon terminationof this Agreement and destroy any duplicate public records that are exemptor confidential and exempt from public records disclosure requirements. All records stored electronically must be provided to the Authority in a formatthat is compatible with the information technology system of the Authority.

ARTICLE 14 - OWNERSHIP OF DOCUMENTS

Upon completion or termination of this Agreement, all records, documents, tracings, plans, specifications, maps, evaluations, reports, and other technical data, otherthan working papers, prepared, or developed by Contractor under this Agreement must bedelivered to and become the property of Authority. Contractors may retain copies thereoffor files and internal use.

ARTICLE 15 - MAINTENANCE OF RECORDS

The contractor will keep adequate records and supporting documentation which concerns or reflect its services hereunder. The records and documentation will be retainedby Contractor for a minimum of five (5) years from the date of expiration or termination ofthis Agreement or the date all work under this Agreement is complete, whichever is later.Authority, the FAA, the Comptroller General of the United States, the Virginia Department of Aviation, or any duly authorized agent or representative of any of them will have the right to audit, inspect and copy all such records and documentation as often as they deem necessary during the period of this Agreement and during the five (5) year period thereafter; provided, however, such activity will be conducted only during normal business hours.

ARTICLE 16 - INDEMNIFICATION

General Indemnification. To the fullest extent permitted by law, Contractor shall defend, indemnify and hold the Authority and its Commissioners, officers, employees (collectively "Indemnitees") harmless from and against any and all claims, actions, damages, expenses

(including reasonable attorneys' fees), losses or liabilities incurred by or asserted against the Authority or any of its Indemnitees arising from the performance of Contractor's obligations under the Agreement and any and all fees, costs or penalties incurred by the Authority or any of its Indemnitees, to the extent that such claims, actions, damages, expenses, losses, liabilities, fees, costs or penalties are caused by or arise out of Contractor's performance; provided that Contractor shall not be required to indemnify the Authority or any of its Indemnitees for any loss or claim to the extent such loss or claim is due to the negligence or willful misconduct of the Authority or any of its Indemnitees.

Intellectual Property Indemnification. Contractor will defend, indemnify and hold the Authority, its Commissioners, officers and employees (collectively "Indemnitees") harmless from and against any liability, loss, damage, cost and expense (including without limitation reasonable attorneys' fees) suffered as a result of any claim, demand, action or suit made or raised against Authority of any of its Indemnities, by reason of Contractor's infringement of any patent, trade secret, trademark, copyright or any other intellectual property right of any third party in relation to work delivered to Authority by Contractor in connection with the Agreement. This commitment is conditioned upon Authority (i) providing Contractor with prompt written notice of the claim, (ii) giving Contractor sole control of the defense to the claim including settlement negotiations if any; and (iii)providing at Contractor's costs reasonable cooperation in the defense against the claim. Under this commitment, Contractor will indemnify Authority (as well as its Commissioners, officers and employees) for the payment of (i) any damages awarded by any competent court by way of a final decision, (ii) any settlement indemnity agreed upon by Contractor with Authority's prior written approval which shall not be unreasonably withheld, and (iii) related costs of investigation and expertise as well as reasonable attorneys' fees if any, to the exclusion of any other payment whatsoever.

ARTICLE 17 – SOVEREIGN IMMUNITY

Contractor acknowledges and agrees that Authority does not waive its sovereign immunity by entering into this Agreement and that nothing herein will be interpreted as awaiver of Authority's rights, including the limitation of waiver of immunity under Virginia law, and Authority expressly reserves those rights to the fullest extent allowed by law.

ARTICLE 18 – INSURANCE

During the term of this Agreement, Contractor will provide, pay for, and maintain,with companies satisfactory to Authority, the types of insurance described herein. Promptly after execution of this Agreement by both Parties, the Contractor must obtain the insurance coverages and limits as set out below. All insurance will be fromresponsible companies duly authorized to do business in the Commonwealth of Virginia and/or responsible risk retention group insurance companies registered with the Commonwealth of Virginia.

The Authority reserves the right to reject insurance written by an insurer it deems unacceptable because of poor financial condition or other operational deficiency. All insurance must be placed with insurers who are duly licensed or authorized to do business within the Commonwealth of Virginia, and with an A.M. Best Rating of not less than A-VII.Regardless of this requirement, the Authority in no way warrants that the required minimum insurer rating is sufficient to protect the Contractor from potential insurer insolvency.

All policies of insurance will contain provisions that advance written notice will be given to Authority's Risk Manager of any cancellation, intent not to renew, material change or alteration, or reduction in the policies' coverages, except in the application of the Aggregate Limits provision of any policy. If there is a reduction in the Aggregate Limitof any policy, the Contractor will immediately take steps to have the Aggregate Limit reinstated to the full extent permitted under such policy. If there is a cancellation, Provideragrees to obtain replacement coverage as soon as possible.

The acceptance by Authority of any Certificate of Insurance evidencing theinsurance coverages and limits required in this Agreement does not constitute approval or agreement by Authority that the insurance requirements have been met or that the insurance policies shown in the Certificates of Insurance are in compliance with the requirements of this Agreement.

All of Contractor's insurance coverages will be primary and non-contributory to any insurance or self-insurance program carried by Authority and applicable to work under this Agreement and will include waiver of subrogation in favor of Authority.

No work may commence on any Task assigned under this Agreement unless anduntil the required Certificates of Insurance are received and approved by Authority. During the term of this Agreement, Contractor will provide, pay for, and maintain, with companies satisfactory to Authority, the types of insurance described herein.

18.1. INSURANCE REQUIRED

Before starting and until acceptance of any work by the Authority, the Contractor will procure and maintain insurance of the types and to the limits specified in paragraphs 18.2.1 through 18.2.6, inclusive below. All liability insurance policies obtained by the contractor to meet the requirements of this Agreement, other than Worker's Compensation and Employer's Liability and Professional Liability policies, will name Authority as an additional insured as to the services of Contractor under this Agreementand will contain the severability of interest's provisions.

18.2. COVERAGES

The amounts and types of insurance described below are the minimum requirements and are not intended to limit the Authority's access to additional coverage ifmore coverage is available. All amounts and types of insurance will conform to the following minimum requirements with the use of Insurance Service Office (ISO) forms andendorsements or broader where applicable:

18.2.1.Professional Liability Insurance - Prior to the start of any work under the Contract, the Contractor shall provide to the Authority Certificates of Insurance approved by the Authority and shall maintain such insurance until the completion of all Work under the Contract, including but not limited to errors and omissions and liability insurance. The Contractor shall carry liability insurance covering negligent acts, errors, and omissions in an amount acceptable to the Authority. In no event shall the amount of liability insurance be less than $1,000,000.

18.2.2.Commercial General Liability Insurance - Contractor will maintain commercial general liability insurance. Coverage will include, but not be limited to, Personal Injury, Contractual for this Agreement, Independent Contractors, Broad Form Property Damage including Completed Operations, Broad Form Contractual Liability andXCU Coverages. If Contractor provides any construction work, it must also include Products & Completed Operations, with the Completed

Operations Coverage maintained for any project under this Agreement and then for not less than five (5) yearsfollowing completion and acceptance of the work by Authority. Limits of coverage will not be less than the following:

If the General Liability insurance required herein is issued or renewed on a "claims made" form, as opposed to the "occurrence" form, the retroactive date for coverage will be nolater than the commencement date of any Task under this Agreement and will provide that in the event of cancellation or non-renewal the discovery period for insurance claims(Tail Coverage) will be unlimited.

18.2.3.Automobile Liability Insurance will be maintained, if necessary, by Contractor asto ownership, maintenance, and use of all owned, non-owned, leased or hired vehicles with limits of not less than:

18.2.4.Worker's Compensation and Employers Liability Insurance will be maintained, if necessary, by the Contractor during the term of this Agreement for all employees engaged inthe work under this Agreement, in accordance with the laws of the Commonwealth of Virginia. The amount of such insurance will not be less than:

18.2.5.Environmental Liability and/or Contractors Pollution Liability Insurance and/or Errors and Omissions Liability Applicable to the Work Performed – If necessary, Contractor will maintain pollution liability insurance, including the cost of defense duringthe term of this Agreement and for a period of five (5) years following completion of all services under this Agreement. Such coverage will apply specifically to the services/scope of work outlined in this Agreement and will include, but not limited to, Pollution Legal Liability (legal liability arising out of fumes, acids, alkalis, toxic chemicals, liquids or gasses, hazardous materials, waste materials or other irritants, contaminants, or pollutants) into or upon land, the atmosphere, or any watercourse or body of water, including groundwater at, under, or emanating from the site of services:

18.2.6.Crime Insurance/Fidelity Bond – If necessary, Contractor will maintain crime insurance coverage, or at the discretion of Authority, a Fidelity Bond, with limits equal to fifty percent (50%) of the Agreement value or $50,000.00 whichever is greater. The bond or policy will include coverage for all directors, officers, agents, and employees ofthe contractor. The bond or policy will include coverage for third party fidelity and namethe Authority as Loss Payee. The bond or policy will include coverage for extended theft and mysterious disappearance. The bond or policy will not contain a condition requiring an arrest and conviction. Policies will be endorsed to provide coverage for computer crime/fraud.

18.2.7.The contractor must provide evidence of the required insurance coverage using Authority's Certificate of Insurance attached as Exhibit "C", or similar formacceptable to Authority's Risk Manager, to verify coverages. The Certificate of Insurance must be completed on a "sample only" basis by Contractor's insurance representatives and must be submitted for Authority's review as to acceptability. Upon acceptance, the Certificates must be signed by an Authorized Representative of the insurance company/companies shown on the Certificates with proof that he or she is an authorized representative thereof. In addition, copies of all insurance policies will be provided to the Authority, on a timely basis, if requested by the Authority. If any insurance provided under this Agreement will expire prior to the completion of the services provided under this Agreement, renewal Certificates of Insurance on an acceptable form and copies of the renewal policies, if requested by Authority, must be furnished to Authority'sRisk Manager at least thirty (30) days prior to the date of expiration.

18.2.8.If Contractor does not maintain the insurance coverages required by this Agreement, Authority may cancel the Agreement or at its sole discretion is authorizedto purchase such coverages and charge Contractor for such coverages purchased. The authority will be under no obligation to purchase such insurance, nor will it be responsible for the coverage purchased or the insurance company/companies used. The decision of Authority to purchase such insurance coverages will in no way be construed to be a waiver of its rights under this Agreement.

ARTICLE 19 - SERVICES BY CONTRACTOR'S OWN STAFF

19.1. Services performed hereunder will be performed by Contractor's own staff, unless otherwise authorized in writing by Authority. The employment of, contract with, or use of the services of any other person or firm by Contractor, as independent contractor or otherwise, will be subject to the prior written approval of Authority. No provision of this Agreement will, however, be construed as constituting an agreement between Authority and any such other person or firm. Nor will anything contained herein be deemed to give any such party or any third party any claim or right of action against Authority beyond such as may otherwise exist without regard to this Agreement.

19.2. Authority hereby gives its prior approval to Contractor to subcontract with for certain services. Provided, however, this prior approval by Authority is subject to Authority's rights under Article 4 above.

ARTICLE 20 - WAIVER OF CLAIMS

Contractor's acceptance of final payment will constitute a full waiver of allclaims, except for insurance company subrogation claims, by it against Authority for services rendered under this Agreement, except those previously made in writing and identified by Contractor as unsettled at the time of the final payment. Neither the acceptance of Contractor's services nor payment by Authority will be deemed to be a waiver of any of Authority's rights against Contractor.

ARTICLE 21 - AIRPORT SECURITY REQUIREMENTS

The contractor acknowledges that the Authority is subject to strict federal security regulations limiting access to secure areas of the Airport and prohibiting violations of theadopted Airport Security Program. Contractor may need access to these secure areas to complete the work required by this Agreement.

Contractor therefore agrees, in addition to the other indemnification and assumption of liability provisions set out above, to indemnify and hold harmless the Authority and Norfolk, Virginia, and their respective commissioners, officers and employees, from any duty to pay any fine or assessment or to satisfy any punitive measure imposed on the Authority or City of Norfolk by the FAA or any other governmental agency for breaches of security rules and regulations by Contractor, its agents, employees, subcontractors, or invitees.

The contractor further acknowledges that its employees and agents may be required to undergo background checks and take Airport Security and Access Procedures ("S.I.D.A.") training before receiving an Airport Security Identification Badge.

Immediately upon the completion of any work requiring airport security access under this Agreement, or upon the resignation or dismissal or conclusion of any work justifying airport

security access to any agent, employee, subcontractor, or invitee of theContractor, Contractor will notify the Airport's Police Department that the Contractor's access authorization or that of any of Contractor's agents, employees, subcontractors, or invitees has changed. The contractor will confirm that notice, by written confirmation on company letterhead, within twenty-four (24) hours of providing initial notice to the Airport's Police Department.

Upon termination of this Agreement, or the resignation or dismissal of any employee or agent, or conclusion of any work justifying airport security access to any agent, employee, subcontractor, or invitee of the Contractor, Contractor will surrender any Airport Security Identification Badge held by the Contractor or by Contractor's agents, employees, subcontractors, or invitees. If Contractor fails to surrender these items within five (5) days, the Contractor will be billed to the Contractor or deducted from any money owed to the Contractor, at the Authority's discretion.

ARTICLE 22 – ASSIGNMENT, TRANSFER AND SUBCONTRACTS

The contractor will not assign or transfer any of its rights, benefits, or obligations hereunder, without the prior written consent of Authority. The Contractor will have the right, subject to the Authority's prior written approval, to employ other persons and/or firms to serve as subcontractors in connection with the Contractor's performance of services under the requirements of this Agreement.

ARTICLE 23 – PROVIDER AN INDEPENDENT CONTRACTOR

The contractor is an independent contractor and is not an employee or agent of the Authority. Nothing in this Agreement will be interpreted to establish any relationship other than that of an independent contractor between the Authority and Contractor, its employees, agents, subcontractors, or assigns, during or after the performance of this Agreement.

ARTICLE 24 - TERMINATION OR SUSPENSION

24.1. Contractor will be considered in material default of this Agreement and such default will be considered cause for Authority to terminate this Agreement, in wholeor in part, as further set forth in this section, for any of the following reasons: (a) failureto begin work under the Agreement within the times specified under any Contract Amendment or Task Authorization, or (b) failure to properly and timely perform the services as directed by Authority as provided for in the Agreement, or (c) the bankruptcy or insolvency or a general assignment for the benefit of creditors by Contractor, or (d) failure to obey laws, ordinances, regulations or other codes of conduct, or (e) failure to perform or abide by the terms or spirit of this Agreement, or (f)for any other just cause. Authority may so terminate this Agreement, in whole or in part, by giving Contractor seven (7) calendar days written notice.

24.2. If, after notice of termination of this Agreement, it is determined for any reason that Contractor was not in default, or that its default was excusable, or that Authority was not entitled to the remedies against Contractor provided herein, then Contractor's remedies against Authority will be the same as and limited to those afforded Contractor under paragraph 24.3. below.

24.3. Authority will have the right to terminate this Agreement, in whole or in part, without cause upon thirty (30) calendar days written notice to Contractor. In the event of such termination for convenience, Contractor's recovery against Authority willbe limited to that portion of the fee earned through the date of termination, together with any retainage withheld and any costs reasonably incurred by Contractor that are directlyattributable to the termination, but Contractor

will not be entitled to any other or furtherrecovery against Authority, including, but not limited to, anticipated fees or profits on worknot required to be performed.

24.4. Upon termination, Contractor will deliver to Authority all original papers, records, documents, drawings, models, and other material set forth and described in thisAgreement.

24.5. Authority will have the power to suspend all or any portions of the servicesto be provided by Contractor hereunder upon giving Contractor two (2) calendar days prior written notice of such suspension. If all or any portion of the services to be rendered hereunder are so suspended, Contractor's sole and exclusive remedy will bean extension of time to its schedule.

ARTICLE 25 - NOTICES AND ADDRESS OF RECORD

All notices required or made under this Agreement to be given by either party to the other will be in writing and will be delivered by hand or by United States Postal Service, first class mail service, postage prepaid, and addressed to the following addresses of record:

Authority:

Norfolk Airport Authority

President/CEO

2200 Norview Avenue

Norfolk, VA 23518

Contractor:

Either party may change its address of record by written notice to the otherparty given in accordance with the requirements of this Article.

ARTICLE 26 - NO THIRD-PARTY RIGHTS

Nothing contained in this Agreement will create a contractual relationship with athird party, or any duty, obligation, or cause of action in favor of any third party, against either the Authority or Contractor.

Services performed by Contractor under the Agreement are solely for the benefit of the Authority. This Agreement will not be construed to create any contractual relationship between Contractor and any third party. It is the intent of the Parties that there be no third-party beneficiaries to this Agreement. The fact that the Authority may enter into other agreements with third Parties that give Contractor and Authority the rightto observe work being performed by those third Parties, will not give rise to any duty orresponsibility on the part of Contractor in favor of such third Parties.

ARTICLE 27 – MISCELLANEOUS

27.1 The contractor, in representing Authority, will promote the best interest of Authority and assume towards Authority a relationship of the highest trust, confidence, and fair dealing. Services provided under this Agreement must be performed in a workmanlike manner consistent with that degree of care and skill ordinarily exercised by members of the same profession currently practicing under similar circumstances in the same geographic location.

27.2 No modification, waiver, suspension, or termination of the Agreement or of any terms thereof will impair the rights or liabilities of either party.

27.3 Waiver by either party or a breach of any provision of this Agreement willnot be deemed to be a waiver of any other breach and will not be construed to be a modification of the terms of this Agreement.

27.4 The headings of the Articles, Sections, Schedules, and Attachments as contained in this Agreement are for the purpose of convenience only and will not be deemed to expand, limit, or change the provisions in such Articles, Sections, Exhibits andAttachments.

27.5 This Agreement, including any Addenda and referenced Exhibits and Attachments hereto, constitutes the entire agreement between the Parties hereto and will supersede, replace, and nullify any and all prior agreements or understandings, written or oral, relating to the matter set forth herein, and any such prior agreements or understanding will have no force or effect whatever on this Agreement.

ARTICLE 28 - APPLICABLE LAW

Unless otherwise specified, this Agreement will be governed by the laws, rules, and regulations of the Commonwealth of Virginia, and by the laws, rules, and regulations of the United States when providing services funded by the United States government. Any suit or action brought by either party to this Agreement against the other party relating toor arising out of this Agreement may only be brought in Circuit Court for the City of Norfolk. The prevailing party in any such suit or action will be entitled to recover from the other party their reasonable attorneys' fees and court costs, including any appeals.

ARTICLE 29 - E-VERIFY

Contractor certifies that it has enrolled and is using in the U.S. Department of Homeland Security's E-Verify Program for Employment Verification in accordance with the terms governing use of the Program and is eligible to enter this Agreement. The Contractor further agrees to provide the Authority with proof of such enrollment within thirty (30) days of the date of this Agreement.

Contractor agrees to use the E-Verify Program to confirm the employment eligibility of:

29.1 All persons employed by Contractor during the term of this Agreement.

29.2 All persons, including subcontractors, assigned by the Contractor to perform work or provide services under the Agreement.

Contractor further agrees that it will require each subcontractor performing work or providing services under this Agreement to enroll in and use the U.S.Department of Homeland Security's E-Verify Program for Employment Verification to verify the employment eligibility of all persons employed by the subcontractor during the term of this Agreement.

Contractor agrees to maintain records of its participation and compliance with the provisions of the E-Verify Program, including participation by its subcontractors as provided

above, and to make such records available to the Authority orother authorized state or federal agency consistent with the terms of this Agreement.

Compliance with the terms of this Article is made an express condition of this Agreement, and the Authority may treat failure to comply as a material breach of the Agreement and grounds for immediate termination.

ARTICLE 30 - COVENANTS AGAINST DISCRIMINATION

During the performance of this Agreement, Contractor, for itself, its assignees and successors in interest agrees as follows:

30.1 Compliance with Regulations. Contractor will comply with the Regulations relative to nondiscrimination in federally assisted programs of the Department of Transportation (the "DOT") Title 49, Code of Federal Regulations, Part 21,as they may be amended from time to time, (the "Regulations"), which are herein incorporated by reference and made a part of this Agreement.

30.2 FAA Nondiscrimination Clause. Contractor will not discriminate based on race, color, national origin, or sex in the performance of this Agreement. The contractor will carry out all applicable requirements of 49 CFR Part 23 and Part 26 in the award and administration of DOT-assisted contracts. Failure by Contractor to carry out these requirements is a material breach of this Agreement, whichmay result in the termination of this Agreement or such other remedy as Authority (recipient) deems appropriate. Every contract that Contractor enters with subcontractor for services under this Agreement must contain this clause.

30.3 Solicitations for Subcontracts, Including Procurements of Materials and Equipment. In all solicitations, either by competitive bidding or negotiation made by Contractor for work to be performed under a subcontract, including procurements of materials or leases of equipment, each potential subcontractor or supplier will be notified by Contractor of Contractor's obligations under this Agreement and the Regulations relative to nondiscrimination on the grounds of race, color, or national origin.

30.4 Information and Reports. Contractor will provide all information and reports required by the Regulations or directives issued pursuant thereto and will permitaccess to its books, records, accounts, other sources of information, and its facilities as may be determined by Authority or the FAA to be pertinent to ascertain compliance with such Regulations, orders, and instructions. Where any information required of Contractor is in the exclusive possession of another who fails or refuses to furnish this information, Contractor will so certify to Authority or the FAA, as appropriate, and willset forth what efforts it has made to obtain the information.

30.5 Sanctions for Noncompliance. In the event of Contractor's noncompliancewith the nondiscrimination provisions of this Agreement, Authority will impose such contract sanctions as it or the FAA may determine to be appropriate, including, but not limited to:

(a) withholding of payments to Contractor under the Agreement until Contractor complies; and/or

(b) cancellation, termination, or suspension of the Agreement, in whole or in part.

30.6 DBE Policy. It is the policy of the Department of Transportation that Disadvantaged

Business Enterprises ("DBE's") as defined in 49 CFR Part 23and Part 26 will have the maximum opportunity to participate in the performance of contracts financed in whole or in part with Federal funds under this Agreement. Consequently, the DBE requirements of 49 CFR Part 23 and Part 26 apply to this Agreement. The Contractor agrees to ensure that DBEs as defined in 49 CFR Part 23and Part 26 have the maximum opportunity to participate in the performance of contracts and subcontracts financed in whole or in part with Federal funds provided under this Agreement. In this regard, Contractor will take all necessary and reasonable steps in accordance with 49 CFR Part 23 and Part 26 to ensure that DBE's have the maximum opportunity to compete for and perform contracts.

30.7 Prompt Payment Requirements. Authority has adopted a DBE Program in compliance with 49 CFR Part 26, therefore, the following requirement will apply to all contracts funded, either wholly or in-part, with FAA financial assistance:

Contractor agrees to pay each subcontractor under this contract for satisfactory performance of its contract no later than fifteen (15) days from the receipt of each payment Contractor receives from Authority. Contractor agrees further to return any retainage payments to each subcontractor within thirty (30) days after the subcontractor's work is satisfactorily completed. Any delay or postponementof payment beyond these time limits may occur only for goodcause following written approval of the delay by the Authority. This clause applies to both DBE and non-DBE subcontractors.

30.8 Incorporation of Provisions. The contractor will include the provisions of paragraphs 36.1. through 36.7. in every subcontract, including procurements of materialsand leases of equipment, unless exempted by the Regulations or directives issued pursuant thereto. The Contractor will take such action with respect to any subcontract or procurement as Authority or the FAA may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, however, that in the event the Contractor becomes involved in, or is threatened with, litigation with a subcontractor or supplier as aresult of such direction, Contractor may request Authority to enter into such litigation to protect the interests of Authority and, in addition, Contractor may request the United States to enter into such litigation to protect the interests of the United States.

ARTICLE 31 - NONDISCRIMINATION CLAUSE

Pursuant to Title 49, Code of Federal Regulations, Department of Transportation,Subtitle A, Office of the Secretary, Part 21, Nondiscrimination in Federally Assisted Programs of the Department of Transportation-Effectuation of Title VI of the Civil Rights Act of 1964, the Restoration Action of 1987, the Virginia Civil Rights Act, and as said Regulations may be amended, the Contractor/Contractor must assure that "no person in the United States will on the basis of race, color, national origin, sex, creed ordisability be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity," and in the selection and retention of subcontractors, including procurements of materials and leases of equipment.

The Contractor will not participate directly or indirectly in the discrimination prohibited by the Acts and the Regulations, including employment practices when the contract covers any activity, project, or program set forth in Appendix B of 49 CFR Part 21.

ARTICLE 32 - GENERAL CIVIL RIGHTS CLAUSE

The Contractor agrees to comply with pertinent statutes, Executive Orders and such rules as are promulgated to ensure that no person will, on the grounds of race, creed, color, national origin, sex, age, or disability be excluded from participating in any activity conducted with or benefiting from Federal assistance.

This provision binds the Contractor and subcontractors from the bid solicitation period through the completion of the contract. This provision is in addition to that requiredby Title VI of the Civil Rights Act of 1964.

ARTICLE 33 - AMENDMENTS OR MODIFICATIONS

No amendment or modification to this Agreement will be valid or binding upon theParties unless in writing as an Amendment to this Agreement and executed by both Parties intended to be bound by it.

This Agreement will become effective upon concurrence by the Federal Aviation Administration and/or the Virginia Department of Aviation, if required, and otherwise on the date first written above.

IN WITNESS WHEREOF, the Parties have executed this Agreement effective theday and year first written above.

AUTHORITY	**CONTRACTOR**:
NORFOLK AIRPORT AUTHORITY	
_____ Signature	_____ Signature
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
WITNESS: Name: _____	_____ Signature

EXHIBIT A

SCOPE OF SERVICES

REFER TO ATTACHMENT C & D

EXHIBIT B

BASIS OF COMPENSATION

REFER TO ATTACHMENT E

EXHIBIT "C"

FAA REQUIREMENTS

1 - ACCESS TO RECORDS AND REPORTS

The Contractor must maintain an acceptable cost accounting system. The Contractor agrees to provide the Owner, the FAA and the Comptroller General of the United States or any of their duly authorized representatives access to any books, documents, papers and records of the Contractor which are directly pertinent to the specific contract for the purpose of making audit, examination, excerpts and transcriptions. The Contractor agrees to maintain all books,records and reports required under this contract for a period of not less than three years after final payment is made and all pending matters are closed.

2 – CLEAN AIR AND WATER POLLUTION CONTROL

Contractor agrees to comply with all applicable standards, orders, and regulations issued pursuant to the Clean Air Act (42 USC § 740-7671q) and the Federal Water Pollution ControlAct as amended (33 USC § 1251-1387). The Contractor agrees to report any violation to theOwner immediately upon discovery. The Owner assumes responsibility for notifying the Environmental Protection Agency (EPA) and the FAA. The contractor must include this requirement in all subcontracts that exceeds $150,000.

3 – DEBARMENT AND SUSPENSION

The successful Contractor, by administering each lower tier subcontract that exceeds $25,000as a "covered transaction", must verify each lower tier participant of a "covered transaction"under the project is not presently debarred or otherwise disqualified from participation in thisfederally assisted project. The successful bidder will accomplish this by: 1. Checking the System for Award Management at website: http://www.sam.gov. 2. Collecting a certification statement similar to the Certification of Offeror /Bidder Regarding Debarment, above. 3. Inserting a clause or condition in the covered transaction with the lower tier contract. If the FAA later determines that a lower tier participant failed to disclose to a higher tier participantthat it was excluded or disqualified at the time it entered the covered transaction, the FAA may pursue any available remedies, including suspension and debarment of the non-compliant participant.

4 – TEXTING WHILE DRIVING

In accordance with Executive Order 13513, "Federal Leadership on Reducing Text Messaging While Driving", (10/1/2009) and DOT Order 3902.10, "Text Messaging While Driving", (12/30/2009), the FAA encourages recipients of Federal grant funds to adopt and enforce safety policies that decrease crashes by distracted drivers, including policies to ban text messaging while driving when performing work related to a grant or subgrant. In support of this initiative, the NAA encourages the Contractor to promote policies and initiatives for its employees and other work personnel that decrease crashes by distracted drivers, including policies that ban text messaging while driving motor vehicles whileperforming work activities associated with the project. The Contractor must include the substance of this clause in all sub-tier contracts exceeding $3,500 that involve driving a motorvehicle in performance of work activities associated with the project.

5 – ENERGY CONSERVATION REQUIREMENTS

Contractors and Subcontractors agree to comply with mandatory standards and policies relating to energy efficiency as contained in the state energy conservation plan issued incompliance with the Energy Policy and Conservation Act (42 USC 6201et seq).

6 – EQUAL OPPORTUNITY CLAUSE

During the performance of this contract, the Contractor agrees as follows:

a) The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, sexual orientation, gender identify, or national origin. Such action will include, but not be limited to, the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff, or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

b) The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive considerations for employment without regard to race, color, religion, sex, or national origin.

c) The Contractor will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, anotice to be provided advising the said labor union or workers' representatives of the Contractor's commitments under this section and will post copies of the notice in conspicuous places available to employees and applicants for employment.

d) The Contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

e) The Contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, andorders.

f) In the event of the Contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this contract may be canceled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, orby rule, regulation, or order of the Secretary of Labor, or as otherwise provided bylaw.

g) The Contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (7) in every subcontractor purchase order unless exempted by rules, regulations, or orders of the Secretaryof Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing suchprovisions, including sanctions for noncompliance: Provided, however, that in theevent a Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency the Contractor may request the United States to enter into such litigation to protectthe interests of the United States.

7 – CERTIFICATION REGARDING LOBBYING

The Contractor certifies by signing and submitting proposals, to the best of his or her knowledge and belief, that:

h) No Federal appropriated funds have been paid or will be paid, by or on behalf of theContractor, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress,or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

i) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employeeof a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned will complete and submit Standard Form-LLL, "Disclosure Form to Report

Lobbying," in accordance with its instructions.

j) The undersigned will require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all sub-recipients will certify and disclose accordingly.

This certification is a material representation of the fact upon which reliance was placed whenthis transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification will be subject to a civil penalty of

not less than $10,000 and not more than $100,000 for each such failure.

8 - OCCUPATIONAL SAFETY AND HEALTH ACT OF 1970

All contracts and subcontracts that result from this solicitation incorporate by reference therequirements of 29 CFR Part 1910 with the same force and effect as if given in full text. The employer must provide a work environment that is free from recognized hazards that may cause death or serious physical harm to the employee. The employer retains full responsibility to monitor its compliance and their subcontractor's compliance with the applicable requirements of the Occupational Safety and Health Act of 1970 (20 CFR Part 1910). The employer must address any claims or disputes that pertain to a referenced requirement directly with the U.S. Department of Labor – Occupational Safety and Health Administration.

9 – CERTIFICATION REGARDING TAX DELINQUENCY AND FELONY CONVICTIONS CERTIFICATION

k) The Contractor represents that it is not a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.

l) The Contractor represents that it is not a corporation that was convicted of a criminal violation under any Federal law within the preceding 24 months.

10 – VETERANS' PREFERENCE

In the employment of labor (excluding executive, administrative, and supervisory positions), the Contractor and all sub-tier Contractors must give preference to covered veterans as defined within Title 49 United States Code Section 47112. Covered veterans include Vietnam-era veterans, Persian Gulf veterans, Afghanistan-Iraq war veterans, disabled veterans, and small business concerns (as defined by 15 USC 632) owned and controlled by disabled veterans. This preference only applies when there are covered veterans readily available and qualified to perform the work to which the employment relates.

ATTACHMENT G: ACKNOWLEDGEMENT FORM - SERVICE PROVIDER AGREEMENT

NORFOLK AIRPORT AUTHORITY

Agreement Acknowledgement

This is to certify that I, _____ (name), in the position of _____ hereby acknowledge that I am aware of the terms and conditions of the attached Service Provider Agreement (SPA) as it relates to the Identity Management System (IDMS) contract. I acknowledge that I have no issue with the terms and conditions of this agreement.

Company: _____

Signed: _____

Print Name (Company Officer): _____

Title: _____

Date: _____