IDENTITY MANAGEMENT SOLUTION AGREEMENT

BETWEEN

CITY AND COUNTY OF DENVER

AND

QUANTUM SECURE, INC.

_____

AT
DENVER INTERNATIONAL AIRPORT

AGREEMENT

THIS AGREEMENT FOR AN IDENTITY MANAGEMENT SOLUTION (Contract Number PLANE-20150608-00) ('Agreement"), made and entered into as of the date set forth on the signature page below (the "Effective Date") by and between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado ("City"), Party of the First Part, and **QUANTUM SECURE, INC.,** a corporation organized under the laws of the state of Delaware and authorized to do business in Colorado ("Contractor"), Party of the Second Part;

W I T N E S S E T H:

WHEREAS, the City owns and operates Denver International Airport ("DEN" or the "Airport"), and desires to purchase hardware, software, software upgrades, support, maintenance, and related equipment for an Identity Management Solution ("IDMS"), and will require professional services for the same, and such other work as may be requested by the City, at Denver International Airport; and

WHEREAS, the Contractor is qualified and ready, willing and able to provide the requested hardware, software and professional services to the City, in accordance with the terms of this Agreement;

NOW, THEREFORE, for and in consideration of the premises and other good and valuable consideration, the parties hereto agree as follows:

1.   LINE OF AUTHORITY:

The City's Chief Executive Officer of the Department of Aviation, her designee or successor in function (the "CEO of Aviation" or the "CEO") authorizes all work performed under this Agreement. The CEO hereby delegates his authority over the work described herein to the Airport's Senior Vice President of Airport Operations (the "SVP") as the CEO's authorized representative for the purpose of administering, coordinating and approving work performed by the Contractor under this Agreement. The SVP's authorized representative for day-to-day administration of the Contractor's services under this Agreement is the Assistant Director of Airport Security (the "Assistant Director"). The Assistant Director shall appoint a Project Manager to assist with the day-to-day administration of the Contractor's services under this Agreement. The Contractor shall submit its reports, memoranda, correspondence and submittals to the Project Manager. The CEO and the SVP may rescind or amend any such designation of representatives or delegation of authority and the Assistant Director may from time to time designate a different individual to act as Project Manager, upon notice to the Contractor.

2.   SCOPE OF WORK:

A.   The Contractor, under the general direction of, and in coordination with the CEO, or other designated supervisory personnel as set forth herein, shall diligently perform any and all authorized services provided under this Agreement. The Contractor shall provide the deliverables, professional services and software support and maintenance services provided in the attached

Exhibit A, "Scope of Work". **Exhibit A** consists of the following documents: Exhibit A, Attachment A-1, Attachment A-2, and Attachment A-3. Work performed under this Agreement shall be performed in accordance with the provisions of **Exhibit B, "Scheduling, Progress Reporting, Invoicing and Correspondence Control".** **Exhibit B** consists of: Exhibit B, Attachment B-1, Attachment B-2, Attachment B-3, Attachment B-4, and Attachment B-5.

B.   Additional Services: The Contractor may also perform services, hereinafter referred to as "Additional Services," which relate to the subject matter of this Agreement, but which the SVP determines to be not described in the Scope of Work or in excess of the requirements of the Scope of Work. Change orders and/or additional Statements of Work (SOWs) will be provided as needed to document work beyond that identified in **Exhibit A**. The Contractor shall be compensated for such Additional Services only if the services and the amount of fees and reimbursable expenses for the services have been authorized in writing in advance by the SVP. The total amount of fees and reimbursable expense costs for Additional Services shall not cause this Agreement to exceed the Maximum Contract Liability set forth herein, and in no event shall the approval of Additional Services and the cost of performing them be deemed to constitute an agreement by the City to an increase in the Maximum Contract Liability.

C.   The Contractor shall faithfully perform the work required under this Agreement in accordance with standards of care, skill, training, diligence and judgment provided by highly competent service providers who perform work of a similar nature to the work described in this Agreement.

3.   TERM:

The Term of this Agreement shall commence on the Effective Date, and shall terminate five (5) years thereafter, unless sooner terminated. The term of this Agreement may be extended for one additional period of two (2) years, by written amendment to this Agreement. Notwithstanding any other extension of term under this paragraph 3 the term of this Agreement may be extended by the mutual agreement of the parties, confirmed by written notice from the City to the Contractor, to allow the completion of any work which has been commenced prior to the date upon which this Agreement otherwise would terminate. However, no extension of the Term shall increase the Maximum Contract Liability stated herein; such amount may be changed only by a duly executed written amendment to this Agreement.

4.   COMPENSATION AND PAYMENT:

A.   Fee: The City agrees to pay to the Contractor, and the Contractor agrees to accept as its sole compensation for services rendered and costs incurred under this Agreement, the rates set forth on **Exhibit A, Attachment A-2 "Payment Schedule"**, and as may be further described herein or in any exhibit or attachment hereto.

B.   Reimbursement Expenses: Reimbursable expenses shall only be allowed under this Agreement where approved in writing, in advance, by the SVP.

C.   Invoicing: Contractor shall provide the City with invoices in a format and with a level of detail acceptable to the City as more fully described in **Exhibit B**. The City shall pay any undisputed amounts in accordance with its obligations under the City's Prompt Payment Ordinance.

D.   Maximum Contract Liability:

(i)   Any other provision of this Agreement notwithstanding, in no event shall the City be liable to pay for services rendered and expenses incurred by the Contractor under the terms of this Agreement for any amount in excess of Two Million Five Hundred Forty-One Thousand Two Hundred Eighty Dollars and 00 Cents ($2,541,280.00) (the "Maximum Contract Liability"). Funding under the provisions of this paragraph 4.D. may be payable from the City's Airport System Capital Replacement Fund and/or Airport Operations and Maintenance Fund. The Contractor acknowledges that the City is not obligated to execute an Order, agreement or an amendment to this Agreement for any services and that any services performed by Contractor beyond that specifically described in an Order are performed at Contractor's risk and without authorization under this Agreement.

(ii)   The Parties agree that the City's payment obligation, whether direct or contingent, shall extend only to funds appropriated as stated herein and encumbered for the purpose of this Agreement. The Parties agree that (a) the City does not by this Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years and (b) this Agreement is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

5.   TAXES AND COSTS:

A.   The Contractor, at its own expense, shall promptly pay, when due, all taxes, bills, debts and obligations it incurs performing work under this Agreement and shall allow no lien, mortgage, judgment or execution to be filed against land, facilities or improvements owned by the City.

B.   The City shall provide to Contractor, at no cost, all necessary clearances and permits necessary to install and/or deliver the products and/or services under Agreement. Where such clearances, permits, leases, or fees of a similar nature are required to be obtained and paid for directly by Contractor, the City shall reimburse Contractor the actual cost of such items.

C.   The City affirms that it is a tax-exempt entity under the Laws of the State of Colorado and this purchase qualifies for the Denver and Colorado sales tax exemption for sales to the United States government, the State of Colorado, its departments and institutions, and its political subdivisions (county and local governmental, school districts and special districts); is a government purchase used only in an official governmental capacity; and will be paid directly by a government agency. Taking into account the City's status, Contractor confirms that all Charges are inclusive of all taxes, levies, duties and assessments ("Taxes") of every nature in effect as of the Effective Date and due in connection with its performance of its obligations under this

Agreement. Contractor is responsible for payment of such Taxes to the appropriate governmental authority.

6.   STATUS OF CONTRACTOR:

It is agreed and understood by and between the parties hereto that the status of the Contractor shall be that of an independent contractor retained on a contractual basis to perform professional or technical services for limited periods of time as described in Section 9.1.1(E)(x) of the Charter of the City and County of Denver, and it is not intended, nor shall it be construed, that the Contractor or its personnel are employees or officers of the City under Chapter 18 of the Revised Municipal Code for any purpose whatsoever.

7.   NO AUTHORITY TO BIND CITY TO CONTRACTS:

The Contractor has no authority to bind the City on any contractual matters. Final approval of all contractual matters which obligate the City must be by the City as required by Charter and Ordinance.

8.   PERSONNEL ASSIGNMENTS:

A.   The Contractor shall assign a Project Manager to this Project that has experience and knowledge satisfactory to the City. The Project Manager shall be the contact person in dealing with the City's Project Manager on matters concerning this Project and shall have the authority to act for the Contractor's organization. Contractor's designated Project Manager shall remain assigned on this contract during the entire contract term, while in the employ of the Contractor, or, until such time that his performance is deemed unsatisfactory by the City and a formal written request is submitted which requests the removal of the Contractor's Project Manager.

B.   The Contractor may submit and the City will consider a request for reassignment of a Project Manager, should the Contractor deem it to be in the best interest of the City, the best interest of the Contractor's organization or in the best interest of the Contractor's Project Manager.

C.   If the City allows the removal of a Project Manager, the replacement Project Manager must have, at least, similar or equal experience and qualifications to that of the original Project Manager. The replacement Project Manager's assignment is subject to the approval of the SVP.

D.   All key professional personnel identified by the Contractor will be assigned by the Contractor or subcontractors to perform work under the Work. The SVP must approve additional personnel in writing. It is the intent of the parties hereto that all key professional personnel be engaged to perform their specialty for all such services required by the Work, and that the Contractor's and the sub-Contractor's key professional personnel be retained for the life of this Agreement to the extent practicable and to the extent that such services maximize the quality of work performed hereunder.

E.	If the Contractor decides to replace any of its key professional personnel, it shall notify the SVP in writing of the changes it desires to make. No such replacement shall be made until the replacement is approved in writing by the SVP, which approval shall not be unreasonably withheld. The SVP shall respond to the Contractor's written notice regarding replacement of key professional personnel within fifteen days after the SVP receives the list of key professional personnel, which the Contractor desires to replace. If the SVP or his designated representative does not respond within that time, the listed personnel shall be deemed to be approved.

F.	If, during the term of this Agreement, the SVP determines that the performance of approved key personnel is not acceptable, he shall notify the Contractor, and he may give the Contractor notice of the period of time, which the SVP considers reasonable to correct such performance. If the SVP notifies the Contractor that certain of its key personnel should be reassigned, the Contractor will use its best efforts to obtain adequate substitute personnel within ten days from the date of the SVP's notice.

## 9.	SUBCONTRACTORS:

A.	Although the Contractor may retain, hire and contract with outside subcontractors, no final agreement or contract with any such subcontractor shall be entered into without the prior written consent of the SVP or his authorized representative. Requests for such approval must be made in writing and include a description of the nature and extent of the services to be provided, the name, address and professional experience of the proposed subcontractor, and any other information requested by the SVP. Any final agreement or contract with an approved subcontractor must contain a valid and binding provision whereby the subcontractor waives any and all rights to make any claim of payment against the City or to file or claim any lien or encumbrance against any City property arising out of the performance or non-performance of the contract.

B.	Because the Contractor's represented professional qualifications are a consideration to the City in entering into this Agreement, the SVP shall have the right to reject any proposed outside subcontractor deemed by him, in his sole discretion, to be unqualified or unsuitable for any reason to perform the proposed services, and the SVP shall have the right to limit the number of outside subcontractors, or to limit the percentage of Work to be performed by them, all in his sole and absolute discretion.

C.	The Contractor shall not retain any subcontractor to perform work under this Agreement if the Contractor is aware, after a reasonable written inquiry has been made, that the subcontractor is connected with the sale or promotion of equipment or material which is or may be used on work related to or following on from this Agreement, or that any other conflict of interest exists.

10. NO EMPLOYMENT OF ILLEGAL ALIENS TO PERFORM WORK UNDER THE AGREEMENT:

      A.   The Agreement is subject to Article 17.5 of Title 8, Colorado Revised Statutes, and Den. Rev. Mun. Code 20-90 and the Contractor is liable for any violations as provided in said statute and ordinance.

      B.   <u>The Contractor certifies that</u>:

      (1)   At the time of its execution of this Agreement, it does not knowingly employ or contract with an illegal alien who will perform work under this Agreement.

      (2)   It will participate in the E-Verify Program, as defined in § 8 17.5-101(3.7), C.R.S., to confirm the employment eligibility of all employees who are newly hired for employment to perform work under this Agreement.

      C.   <u>The Contractor also agrees and represents that</u>:

      (1)   It shall not knowingly employ or contract with an illegal alien to perform work under the Agreement.

      (2)   It shall not enter into a contract with a subcontractor or subconsultant that fails to certify to the Contractor that it shall not knowingly employ or contract with an illegal alien to perform work under the Agreement.

      (3)   It has confirmed the employment eligibility of all employees who are newly hired for employment to perform work under this Agreement, through participation in the E-Verify Program.

      (4)   It is prohibited from using either the E-Verify Program or the Department Program procedures to undertake pre-employment screening of job applicants while performing its obligations under the Agreement, and it has complied with all federal requirements regarding the use of the E-Verify program, including, by way of example, requirements related to employee notification and preservation of employee rights.

      (5)   If it obtains actual knowledge that a subcontractor or subconsultant performing work under the Agreement knowingly employs or contracts with an illegal alien, it will notify such subcontractor and the City within three days. The Contractor will also then terminate such subcontractor or subconsultant if within three days after such notice the subcontractor or subconsultant does not stop employing or contracting with the illegal alien, unless during such three day period the subcontractor or subcontractor provides information to establish that the subcontractor or subconsultant has not knowingly employed or contracted with an illegal alien.

      (6)   It will comply with any reasonable request made in the course of an investigation by the Colorado Department of Labor and Employment under authority of § 8-17.5-102(5), C.R.S. or the City Auditor under authority of Den. Rev. Mun. Code 20-90.3.

11.   NO DISCRIMINATION IN EMPLOYMENT:

In connection with the performance of work under this Agreement, the Contractor agrees not to fail or refuse to hire, discharge, promote or demote, or to discriminate in matters of compensation, terms, conditions or privileges of employment against any person otherwise qualified, solely because of race, color, religion, national origin, gender, age, military status, sexual orientation, marital status, or physical or mental disability; and the Contractor further agrees to insert the foregoing provision in all subcontracts hereunder.

12.   DSBO GOALS:

The Contractor may be subject to the City's ordinance, DRMC Chapter 28, Article III (MBE/WBE Ordinance) which prohibits discrimination in the awarding of contracts and subcontracts and directs the DSBO Director to establish goals for MBE and WBE participation in the preconstruction and construction of City-owned facilities. The goal for this Agreement is: ***Ordinance Not Applicable.*** If it is determined that project goals apply, such project goals must be met with certified MBE and WBE participants or by demonstrating good faith efforts under the MBE/WBE Ordinance. The Contractor must comply with the terms and conditions of the MBE/WBE Ordinance in soliciting and contracting with its subcontractors in administering the performance of the work hereunder. It shall be an ongoing, affirmative obligation of the Contractor to maintain, at a minimum, compliance with the originally achieved level of MBE/WBE participation upon which this Agreement was awarded, for the duration of this Agreement, unless the City initiates a material alteration to the scope of work.

13.   PREVAILING WAGES:

Employees of the Contractor or its subcontractors may be subject to the payment of prevailing wages pursuant to D.R.M.C. 20-76, depending upon the nature of the Work. By executing this Agreement, the Contractor covenants that it is familiar with this Code Section and is prepared to pay or cause to be paid prevailing wages, if any, applicable to the work conducted by the Contractor's or its subcontractor's employees. The schedule of prevailing wage is periodically updated and Contractor is responsible for payment of then current prevailing wage. The Contractor may obtain a current schedule of prevailing wage rates at any time from the City Auditor's Office.

14.   PROMPT PAY:

The Contractor is subject to D.R.M.C. Section 20-112 wherein the Contractor is to pay its subcontractors in a timely fashion. A payment is timely if it is mailed to the subcontractor no later than seven days after receipt of any payment from City. Any late payments are subject to a late payment penalty as provided for in the prompt pay ordinance (Section 20-107 through 20-118).

15. CITY REVIEW OF PROCEDURES:

The Contractor agrees that, upon request of the SVP, at any time during the term of the Agreement or three years thereafter, it will make full disclosure to the City of the means, methods, and procedures used in performance of services hereunder.

16. COORDINATION OF SERVICES:

The Contractor agrees to perform its work under this Agreement in accordance with the operational requirements of DEN, and all work and movement of personnel or equipment on areas included within the DEN site shall be subject to the regulations and restrictions established by the City or its authorized agents.

17. INSURANCE:

A. The Contractor shall obtain and keep in force during the entire term of this Agreement, including any warranty periods, all of the minimum insurance coverage forms and amounts set forth in **Exhibit D**, which is incorporated into this Agreement by this reference. The Contractor shall submit to the City fully completed and executed certificates of insurance (ACORD form or equivalent approved by the City) which specifies the issuing company or companies, policy numbers and policy periods for each required form of coverage. The certificates for each insurance policy are to be signed by a person authorized by the insurer to bind coverage on its behalf, and must be submitted to the City at the time the Contractor signs this Agreement.

B. All certificates and any required endorsements must be received and approved by the City before any work commences. Each insurance policy required by this Agreement must be in effect at or prior to commencement of work under this Agreement and remain in effect for the duration of the project, including any warranty periods. Failure to maintain the insurance policies as required by this Agreement or to provide evidence of renewal is a material breach of the Agreement. All subcontractors' work shall also be subject to the minimum requirements identified in **Exhibit D**. All subcontractors' certificates and endorsements must be received and approved by the Contractor before work commences. The City reserves the right to request copies of these certificates at any time.

C. All certificates required by this Agreement shall be sent directly to Denver International Airport, Risk Management, Airport Office Building, Room 8810, 8500 Pena Boulevard, Denver, Colorado 80249. The City Project/Agreement number and project description shall be noted on the certificate of insurance. The City reserves the right to require complete, certified copies of all insurance policies required by this Agreement at any time.

D. The City's acceptance of any submitted insurance certificate is subject to the approval of the City's Risk Management Administrator. All coverage requirements specified in the certificate shall be enforced unless waived or otherwise modified in writing by the City's Risk Management Administrator.

E.   The Contractor shall comply with all conditions and requirements set forth in the insurance certificate for each required form of coverage during all periods in which coverage is in effect.

F.   The insurance coverage forms specified in this Agreement are the minimum requirements, and these requirements do not lessen or limit the liability of the Contractor under the terms of this Agreement, including the Indemnification provisions herein. The Contractor shall maintain, at its own expense, any additional kinds and amounts of insurance that it may deem necessary to cover its obligations and liabilities under this Agreement.

18.   DEFENSE AND INDEMNIFICATION:

A.   Contractor hereby agrees to defend, indemnify, and hold harmless City, its appointed and elected officials, agents and employees against all liabilities, claims, judgments, suits or demands for damages to persons or property arising out of, resulting from, or relating to the work performed under this Agreement ("Claims"), unless such Claims have been specifically determined by the trier of fact to be the sole negligence or willful misconduct of the City. This indemnity shall be interpreted in the broadest possible manner to indemnify City for any acts or omissions of Contractor or its subcontractors either passive or active, irrespective of fault, including City's concurrent negligence whether active or passive, except for the sole negligence or willful misconduct of City.

B.   Contractor's duty to defend and indemnify City shall arise at the time written notice of the Claim is first provided to City regardless of whether Claimant has filed suit on the Claim. Contractor's duty to defend and indemnify City shall arise even if City is the only party sued by claimant and/or claimant alleges that City's negligence or willful misconduct was the sole cause of claimant's damages.

C.   Contractor will defend any and all Claims which may be brought or threatened against City and will pay on behalf of City any expenses incurred by reason of such Claims including, but not limited to, court costs and attorney fees incurred in defending and investigating such Claims or seeking to enforce this indemnity obligation. Such payments on behalf of City shall be in addition to any other legal remedies available to City and shall not be considered City's exclusive remedy.

D.   Insurance coverage requirements specified in this Agreement shall in no way lessen or limit the liability of the Contractor under the terms of this indemnification obligation. The Contractor shall obtain, at its own expense, any additional insurance that it deems necessary for the City's protection.

E.   This defense and indemnification obligation shall survive the expiration or termination of this Agreement.

19. **COLORADO GOVERNMENTAL IMMUNITY ACT:**

The parties hereto understand and agree that the City and County of Denver, its officers, officials and employees, are relying on, and do not waive or intend to waive by any provisions of this Agreement, the monetary limitations or any other rights, immunities and protections provided by the Colorado Governmental Immunity Act, §§ 24-10-101 to 120, C.R.S., or otherwise available to the City and County of Denver, its officers, officials and employees.

20. **INTELLECTUAL PROPERTY INDEMNIFICATION AND LIMITATION OF LIABILITY:**

Contractor shall (i) defend City against any third party claim that the Work, or materials provided by Contractor to City infringe a patent, copyright or other intellectual property right, and (ii) pay the resulting costs and damages finally awarded against City by a court of competent jurisdiction or the amounts stated in a written settlement signed by Contractor. The foregoing obligations are subject to the following: the City (a) notifies the Contractor promptly in writing of such claim, (b) grants the Contractor sole control over the defense and settlement thereof subject to the final approval of the City Attorney, and (c) reasonably cooperates in response to request for assistance. Should such a claim be made, or in the Contractor's opinion be likely to be made, the Contractor may, at its option and expense, (1) procure for the City the right to make continued use thereof, or (2) replace or modify such so that it becomes non-infringing. If the preceding two options are commercially unreasonable, then Contractor shall refund the portion of any fee for the affected Work. The Contractor shall have no indemnification obligation to the extent that the infringement arises out of or relates to: (a) the use or combination of the subject Work and/or materials with third party products or services, (b) use for a purpose or in a manner for which the subject Work and/or materials were not designed in accordance with Contractor's standard documentation; (c) any modification to the subject Work and/or materials made by anyone other than the Contractor or its authorized representatives, if the infringement claim could have been avoided by using the unaltered version of the Work and/or materials, (d) any modifications to the subject Work and/or materials made by the Contractor pursuant to the City's specific instructions, or (e) any technology owned or licensed by the indemnitee from third parties. In no event will either party be liable to the other party for any special, incidental, consequential or exemplary damages of any kind, including but not limited to any lost profits and lost savings, however caused, whether for breach or repudiation of contract, tort, breach of warranty, negligence, or otherwise, whether or not such party was advised of the possibility of such loss or damages. THIS SECTION STATES THE INDEMNITEE'S SOLE AND EXCLUSIVE REMEDY AND THE INDEMNITOR'S ENTIRE LIABILITY FOR THIRD PARTY INFRINGEMENT CLAIMS.

21. **INTELLECTUAL PROPERTY RIGHTS; OWNERSHIP OF HARDWARE AND SOFTWARE:**

A. <u>Ownership</u>: Unless otherwise specified herein, no intellectual property rights shall pass from Contractor to the City under this Agreement.

B.   License Grant: Subject to the terms and conditions of this Agreement, Contractor grants City the license set forth in **Exhibit C**, the Quantum Secure, Inc. End User License Agreement.

C.   Reservation of Rights: Contractor reserves all rights not expressly granted to City in this Agreement. Except as expressly stated, nothing herein shall be construed to: (1) directly or indirectly grant to a receiving party any title to or ownership of a providing party's intellectual property rights in services or materials furnished by such providing party hereunder, or (2) preclude such providing party from developing, marketing, using, licensing, modifying or otherwise freely exploiting services or materials that are similar to or related to the Work or materials provided hereunder. Notwithstanding anything to the contrary herein, City acknowledges that Contractor has the right to use any City provided materials solely for the benefit of City in connection with the Work performed hereunder for City.

22.   OWNERSHIP OF WORK PRODUCT:

Except as otherwise set forth at paragraph 21, above, all plans, drawings, reports, other submittals, and other documents submitted to the City or its authorized agents by the Contractor shall become and are the property of the City, and the City may, without restriction, make use of such documents and underlying concepts as it sees fit. The Contractor shall not be liable for any damage which may result from the City's use of such documents for purposes other than those described in this Agreement.

23.   COMPLIANCE WITH PATENT, TRADEMARK, COPYRIGHT AND SOFTWARE LICENSING LAWS:

A.   The Contractor agrees that all work performed under this Agreement shall comply with all applicable patent, trademark, copyright and software licensing laws, rules, regulations and codes of the United States. The Contractor will not utilize any protected patent, trademark or copyright in performance of its work unless it has obtained proper permission and all releases and other necessary documents. If the Contractor prepares any design documents which specify any material, equipment, process or procedure which is protected, the Contractor shall disclose such patents, trademarks and copyrights in the construction drawings or specifications.

B.   The Contractor further agrees to release, indemnify and save harmless the City, its officers, agents and employees, pursuant to Paragraph 18, "Defense and Indemnification," and Paragraph 20, "Intellectual Property Indemnification and Limitation of Liability," from any and all claims, damages, suits, costs, expenses, liabilities, actions or proceedings of any kind or nature whatsoever, of or by anyone whomsoever, in any way resulting from, or arising out of, directly or indirectly, the performance of work under this Agreement which violates or infringes upon any patent, trademark, copyright or software license protected by law, except in cases where the Contractor's personnel are working under the direction of City personnel and do not have direct knowledge or control of information regarding patents, trademarks, copyrights and software licensing.

24.   SOFTWARE SOURCE CODE ESCROW:

Intentionally deleted.

25.   ADVERTISING AND PUBLIC DISCLOSURES:

The Contractor shall not include any reference to this Agreement or to work performed hereunder in any of its advertising or public relations materials without first obtaining the written approval of the CEO. Any oral presentation or written materials related to DEN shall include only presentation materials, work product, and technical data which have been accepted by the City, and designs and renderings, if any, which have been accepted by the City. The CEO shall be notified in advance of the date and time of any such presentations. Nothing herein, however, shall preclude the Contractor's use of this contract and its component parts in GSA form 254 or 255 presentations, or the transmittal of any information to officials of the City, including without limitation, the Mayor, the CEO, any member or members of City Council, and the Auditor.

26.   COLORADO OPEN RECORDS ACT:

The Contractor acknowledges that the City is subject to the provisions of the Colorado Open Records Act, Colorado Revised Statutes §24-72-201 et seq., and the Contractor agrees that it will fully cooperate with the City in the event of a request or lawsuit arising under such act for the disclosure of any materials or information which the Contractor asserts is confidential and exempt from disclosure. Any other provision of this Agreement notwithstanding, including exhibits, attachments and other documents incorporated into this Agreement by reference, all materials, records and information provided by the Contractor to the City shall be considered confidential by the City only to the extent provided in the Open Records Act, and the Contractor agrees that any disclosure of information by the City consistent with the provisions of the Open Records Act shall result in no liability of the City.

27.   DATA CONFIDENTIALITY:

A.   For the purpose of this Agreement, confidential information means any information, knowledge and data marked "Confidential Information" or "Proprietary Information" or similar legend. All oral and/or visual disclosures of Confidential Information shall be designated as confidential at the time of disclosure, and be summarized, in writing, by the disclosing Party and given to the receiving Party within thirty (30) days of such oral and/or visual disclosures.

B.   The disclosing Party agrees to make known to the receiving Party, and the receiving Party agrees to receive Confidential Information solely for the purposes of this Agreement. All Confidential Information delivered pursuant to this Agreement:

(i)   shall not be distributed, disclosed, or disseminated in any way or form by the receiving Party to anyone except its own employees, corporate partners, affiliates and alliance partners who have a need to know said Confidential Information;

(ii)   shall be treated by the receiving Party with the same degree of care to avoid disclosure to any third Party as is used with respect to the receiving Party's own information of like importance which is to be kept confidential.

C.   These obligations shall not apply, however, to any information which:

(i)   is already in the public domain or becomes available to the public through no breach of this Agreement by the receiving Party; or

(ii)   was in the receiving Party's possession prior to receipt from the disclosing Party; or

(iii)   is received by the receiving Party independently from a third Party free to disclose such information; or

(iv)   is subsequently independently developed by the receiving Party as proven by its written records; or

(v)   is disclosed when such disclosure is compelled pursuant to legal, judicial, or administrative proceeding, or otherwise required by law, subject to the receiving Party giving all reasonable prior notice to the disclosing Party to allow the disclosing Party to seek protective or other court orders.

D.   Upon the request from the disclosing Party, the receiving Party shall return to the disclosing Party all Confidential Information, or if directed by the disclosing Party, shall destroy such Confidential Information.

28.   EXAMINATION OF RECORDS:

A. The Contractor agrees that the City's duly authorized representatives, including but not limited to the City's Auditor, shall, until the expiration of three (3) years after the final payment under this Agreement, have access to and the right to examine any directly pertinent books, documents, papers and records of the Contractor involving this Agreement.

B.   In connection with any services performed hereunder on items of work toward which federal funds may be received under the Airport and Airway Development Act of 1970, as amended, the City, the Federal Aviation Administration, the Comptroller General of the United States, and any of their duly authorized representatives, shall have access to any books, documents, papers and records of the Contractor which are directly pertinent to a specific grant program for the purpose of making audit, examination, excerpts and transcriptions. The Contractor further agrees that such records will contain information concerning the personnel, hours and specific tasks performed, along with the applicable federal project number.

29.   INFORMATION FURNISHED BY CITY:

The City will furnish to the Contractor available information concerning DEN and any such other matters that may be necessary or useful in connection with the work to be performed by the Contractor under this Contract. The Contractor shall be responsible for the verification of the information provided to the Contractor.

30.   TERMINATION:

A.   The City has the right to terminate this Agreement without cause on thirty (30) days written notice to the Contractor, and with cause on ten (10) days written notice to the Contractor. However, nothing herein shall be construed as giving the Contractor the right to perform services under this Agreement beyond the time when such services become unsatisfactory to the CEO.

B.   If the Contractor is discharged before all the services contemplated hereunder have been completed, or if the Contractor's services are for any reason terminated, stopped or discontinued because of the inability of the Contractor to provide service under this Agreement, the Contractor shall be paid only for those services satisfactorily performed prior to the time of termination.

C.   If this Agreement is terminated, the City shall take possession of all materials, equipment, tools and facilities owned by the City which the Contractor is using by whatever method it deems expedient, and the Contractor shall deliver to the City all drafts or other documents it has completed or partially completed under this Agreement, together with all other items, materials and documents which have been paid for by the City, and these documents and materials shall be the property of the City.

D.   Upon termination of this Agreement by the City, the Contractor shall have no claim of any kind whatsoever against the City by reason of such termination or by reason of any act incidental thereto, except as follows: if the termination is for the convenience of the City the Contractor shall be entitled to reimbursement for the reasonable cost of the Work to the date of termination, including multiplier, and reasonable costs of orderly termination, provided request for such reimbursement is made no later than six (6) months from the effective date of termination. The Contractor shall not be entitled to loss of anticipated profits or any other consequential damages as a result of any such termination for convenience, and in no event shall the total sums paid exceed the Contract Amount.

31.   RIGHTS AND REMEDIES NOT WAIVED:

In no event shall any payment by the City hereunder constitute or be construed to be a waiver by the City of any breach of covenant or default which may then exist on the part of the Contractor, and the making of any such payment when any such breach or default shall exist shall not impair or prejudice any right or remedy available to the City with respect to such breach or default; and no assent, expressed or implied, to any breach of any one or more covenants, provisions or conditions of this Agreement shall be deemed or taken to be a waiver of any other breach.

32. **SURVIVAL OF CERTAIN CONTRACT PROVISIONS**:

The parties understand and agree that all terms and conditions of this Agreement, including any warranty provision, which by reasonable implication contemplate continued performance or compliance beyond the termination of this Agreement (by expiration of the term or otherwise) shall survive such termination and shall continue to be enforceable as provided herein.

33. **NOTICES:**

Notwithstanding any other provision of this Agreement, notices concerning termination of this Agreement, notices of alleged or actual violations of the terms of this Agreement, and other notices of similar importance shall be made as follows:

by Contractor to: Chief Executive Officer
Department of Aviation
Denver International Airport
8500 Peña Boulevard, 9th Floor
Denver, Colorado 80249-6340

And by City to: Quantum Secure, Inc.
100 Century Center Court
San Jose, CA 95112

Said notices shall be delivered personally during normal business hours to the appropriate office above or by prepaid U.S. certified mail, return receipt requested. Mailed notices shall be deemed effective upon deposit with the U.S. Postal Service. Either party may from time to time designate substitute addresses or persons where and to whom such notices are to be mailed or delivered, but such substitutions shall not be effective until actual receipt of written notification thereof.

34. **NO THIRD PARTY BENEFICIARIES:**

It is expressly understood and agreed that enforcement of the terms and conditions of this Agreement and all rights of action relating to such enforcement shall be strictly reserved to the City and the Contractor, and nothing contained in this Agreement shall give or allow any such claim or right of action by any other or third person on such Agreement. It is the express intention of the City and the Contractor that any person other than the City or the Contractor receiving services or benefits under this Agreement shall be deemed to be an incidental beneficiary only.

35. **ASSIGNMENT:**

The Contractor shall not assign, pledge or transfer its duties and rights under this Agreement, in whole or in part, without first obtaining the written consent of the CEO. Any attempt by the Contractor to assign or transfer its rights hereunder without such prior written

consent shall, at the option of the CEO, automatically terminate this Agreement and all rights of the Contractor hereunder. Such consent may be granted or denied at the sole and absolute discretion of the CEO.

36. CONFLICT OF INTEREST:

The Contractor agrees that it and its subsidiaries, affiliates, subcontractors, principals, or employees will not engage in any transaction, activity or conduct which would result in a conflict of interest. The Contractor represents that it has disclosed any and all current or potential conflicts of interest. A conflict of interest shall include transactions, activities, or conduct that would affect the judgment, actions or work of the Contractor by placing the Contractor's own interests, or the interest of any party with whom the Contractor has a contractual arrangement, in conflict with those of the City. The City, in its sole discretion, shall determine the existence of a conflict of interest and may terminate this Agreement if such a conflict exists, after it has given the Contractor written notice which describes such conflict. The Contractor shall have thirty days after the notice is received in which to eliminate or cure the conflict of interest in a manner which is acceptable to the City.

37. GOVERNING LAW; BOND ORDINANCES; VENUE; DISPUTES:

A.   This Agreement is made under and shall be governed by the laws of Colorado. Each and every term, provision or condition herein is subject to the provisions of Colorado law, the Charter of the City and County of Denver, and the ordinances and regulations enacted pursuant thereto. Venue for any action arising hereunder shall be in the City and County of Denver, Colorado.

B.   This Agreement is in all respects subject and subordinate to any and all City bond ordinances applicable to the Denver Municipal Airport System and to any other bond ordinances which amend, supplement, or replace such bond ordinances.

C.   All disputes between the City and Contractor regarding this Agreement shall be resolved by administrative hearing pursuant to the procedure established by D.R.M.C. § 5-17.

38. COMPLIANCE WITH ALL LAWS AND REGULATIONS:

All of the work performed under this Agreement by the Contractor shall comply with all applicable laws, rules, regulations and codes of the United States and the State of Colorado, the charter, ordinances and rules and regulations of the City and County of Denver, and all Denver International Airport Rules and Regulations.

39. FEDERAL PROVISIONS:

This Agreement is subject and subordinate to the terms, reservations, restrictions and conditions of any existing or future agreements between the City and the United States, the execution of which has been or may be required as a condition precedent to the transfer of federal rights or property to the City for airport purposes and the expenditure of federal funds for the

extension, expansion or development of the Denver Municipal Airport System, including DEN. The provisions of the attached Federal Aviation Administration Contract Provisions are incorporated herein by reference.

40. AIRPORT SECURITY:

A.   It is a material requirement of this Contract that the Contractor shall comply with all rules, regulations, written policies and authorized directives from the City and/or the Transportation Security Administration with respect to Airport security. The Contractor shall conduct all of its activities at the Airport in compliance with the Airport security program, which is administered by the Security Section of the Airport Operations Division, Department of Aviation. Violation by the Contractor or any of its employees, subcontractors or vendors of any rule, regulation or authorized directive from the City or the Transportation Security Administration with respect to Airport Security shall be grounds for immediate termination by the City of this Contract for cause.

B.   The Contractor shall promptly upon notice of award of this Contract, meet with the Airport's Assistant Security Manager to establish badging and vehicle permit requirements for the Contractor's operations under this Contract. The Contractor shall obtain the proper access authorizations for all of its employees, subcontractors and vendors who will enter the Airport to perform work or make deliveries, and shall be responsible for each such person's compliance with all Airport rules and regulations, including without limitation those pertaining to security. Any person who violates such rules may be subject to revocation of his/her access authorization. The failure of the Contractor or any subcontractor to complete any required services hereunder shall not be excused on account of the revocation for good cause of access authorization of any person.

C.   The security status of the Airport is subject to change without notice. If the security status of the Airport changes at any time during the term of this Contract, the Contractor shall take immediate steps to comply with security modifications which occur as a result of the changed status. The Contractor may at any time obtain current information from the Airport Security Office regarding the Airport's security status in relation to the Contractor's operations at the Airport.

D.   The Contractor shall return to the City at the expiration or termination of this Contract, or upon demand by the City, all access keys or access badges issued to it or any subcontractor for any area of the Airport, whether or not restricted. If the Contractor fails to do so, the Contractor shall be liable to reimburse the City for all the City's costs for work required to prevent compromise of the Airport security system. The City may withhold funds in the amount of such costs from any amounts due and payable to the Contractor under this Contract.

41. USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS:

The Contractor and Contractor's agents shall cooperate and comply with the provisions of the City and County of Denver Executive Order No. 94 and Attachment A thereto concerning the use, possession or sale of alcohol or drugs. Violation of these provisions or refusal to cooperate with implementation of the policy can result in the City's barring the Contractor and Contractor's agents from City facilities or participating in City operations.

42. CITY SMOKING POLICY:

Contractor acknowledges that smoking is not permitted in Airport buildings and facilities except for designated Airport Smoking Concessions, and so agrees that it will prohibit smoking by its employees and the public in indoor areas and within 15 feet of entryways of the Airport Premises, except as may otherwise be permitted by the Colorado Clean Indoor Air Act, C.R.S. §§ 25-14-201 to 209. Contractor and its officers, agents, and employees shall cooperate and comply with the provisions of the Denver Revised Municipal Code, §§ 24-301 to 317 et. seq., the Colorado Clean Indoor Air Act, C.R.S. §§ 25-14-201 to 209, City's Executive Order No. 99 dated December 1, 1993, and Executive Order No. 13 dated July 31, 2002.

43. PARAGRAPH HEADINGS:

The captions and headings set forth herein are for convenience of reference only, and shall not be construed so as to define or limit the terms and provisions hereof.

44. CONTRACT DOCUMENTS; ORDER OF PRECEDENCE:

This Agreement consists of Sections 1 through 51 which precede the signature page, and the following attachments which are incorporated herein and made a part hereof by reference (the "Contract Documents"):

Federal Aviation Administration Contract Provisions	
Exhibit A:	Scope of Work and attachments A-1 to A-3 thereto
Exhibit B:	Scheduling, Progress Reporting, Invoicing and Correspondence Control and attachments B-1 to B-5 thereto
Exhibit C:	Quantum Secure, Inc. End User License Agreement
Exhibit D:	Certificate of Insurance

In the event of an irreconcilable conflict between a provision of Sections 1 through 51 and any of the listed attachments or between provisions of any attachments, such that it is impossible to give effect to both, the order of precedence to determine which document shall control to resolve such conflict, is as follows, in descending order:

Federal Aviation Administration Contract Provisions
Sections 1 through 51 hereof
Exhibit A and attachments A-1 to A-3 thereto
Exhibit B and attachments B-1 to B-5 thereto
Exhibit C
Exhibit D

45. AGREEMENT AS COMPLETE INTEGRATION; AMENDMENTS:

This Agreement is intended as the complete integration of all understandings between the parties. No prior or contemporaneous addition, deletion, or other amendment hereto shall have

any force or effect whatsoever, unless embodied herein in writing. No subsequent novation, renewal, addition, deletion, or other amendment hereto shall have any force or effect unless embodied in a written amendatory or other agreement properly executed by the parties. This Agreement and any amendments shall be binding upon the parties, their successors and assigns.

46. INUREMENT:

The rights and obligations of the parties herein set forth shall inure to the benefit of and be binding upon the parties hereto and their respective successors and assigns permitted under this Agreement.

47. FORCE MAJEURE:

Neither party shall be liable for any failure to perform any of its obligations hereunder due to or caused by, in whole or in part, fire, strikes, lockouts, unusual delay by common carriers, unavoidable casualties, war, riots, acts of terrorism, acts of civil or military authority, acts of God, judicial action, or any other causes beyond the control of the parties. Both parties shall have the duty to take reasonable actions to mitigate or prevent further delays or losses resulting from such causes.

48. SEVERABILITY; ENTIRE AGREEMENT:

If any part, portion or provision of this Agreement shall be found or declared null, void, or unenforceable for any reason whatsoever by any court of competent jurisdiction or any governmental agency having applicable authority, only such part, portion, or provision shall be affected thereby and all other parts, portions and provisions of this Agreement shall remain in full force and effect. The Contract Documents form the entire agreement between the parties and are fully binding on the parties. No oral representations or other agreements have been made except as specifically stated in the Contract Documents.

49. COUNTERPARTS OF THIS AGREEMENT:

This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.

50. ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS:

Contractor consents to the use of electronic signatures by the City. The Agreement, and any other documents requiring a signature hereunder, may be signed electronically the City in the manner specified by the City. The Parties agree not to deny the legal effect or enforceability of the Agreement solely because it is in electronic form or because an electronic record was used in its formation. The Parties agree not to object to the admissibility of the Agreement in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

51. CITY EXECUTION OF AGREEMENT:

This Agreement is expressly subject to and shall not be or become effective or binding on the City until it has been approved by City Council, if so required by law, and fully executed by all signatories of the City and County of Denver.

[SIGNATURE PAGE FOLLOWS]

Contract Control Number:

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of

SEAL   **CITY AND COUNTY OF DENVER**

ATTEST:

                                        By_____

_____

APPROVED AS TO FORM: REGISTERED AND COUNTERSIGNED:

                                        By_____

By_____

                                        By_____

Contract Control Number: PLANE-201523684-00

Contractor Name: Quantum Secure, Inc.

By: _____

Name: ___A JAY JAIN_____
       (please print)

Title: ___PRESIDENT & CEO_____
      (please print)

DATE: 7/7/2016

ATTEST: [if required]

By: _____

Name: _____
      (please print)

Title: _____
      (please print)

Federal Aviation Administration Required Contract Provisions

As used in these Contract Provisions, "Sponsor" means The City and County of Denver, Department of Aviation, and "Contractor" or "Consultant" means the Party of the Second Part as set forth in Contract Number PLANE 201523684

A.   Title VI Clauses for Compliance with Nondiscrimination Requirements

During the performance of this contract, the contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "contractor") agrees as follows:

1. Compliance with Regulations: The contractor (hereinafter includes consultants) will comply with the Title VI List of Pertinent Nondiscrimination Acts And Authorities, as they may be amended from time to time, which are herein incorporated by reference and made a part of this contract.

2. Non-discrimination: The contractor, with regard to the work performed by it during the contract, will not discriminate on the grounds of race, color, or national origin 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 Nondiscrimination Acts and Authorities, including employment practices when the contract covers any activity, project, or program set forth in Appendix B of 49 CFR part 21.

3. Solicitations for Subcontracts, Including Procurements of Materials and Equipment: In all solicitations, either by competitive bidding, or negotiation made by the 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 the contractor of the contractor's obligations under this contract and the Nondiscrimination Acts And Authorities on the grounds of race, color, or national origin.

4. Information and Reports: The contractor will provide all information and reports required by the Acts, the Regulations, and directives issued pursuant thereto and will permit access to its books, records, accounts, other sources of information, and its facilities as may be determined by the sponsor or the Federal Aviation Administration to be pertinent to ascertain compliance with such Nondiscrimination Acts And Authorities and instructions. Where any information required of a contractor is in the exclusive possession of another who fails or refuses to furnish the information, the contractor will so certify to the sponsor or the Federal Aviation Administration, as appropriate, and will set forth what efforts it has made to obtain the information.

5. Sanctions for Noncompliance: In the event of a contractor's noncompliance with the Non-discrimination provisions of this contract, the sponsor will impose such contract sanctions as it or the Federal Aviation Administration may determine to be appropriate, including, but not limited to:

      a. Withholding payments to the contractor under the contract until the contractor complies; and/or

b. Cancelling, terminating, or suspending a contract, in whole or in part.

6. Incorporation of Provisions: The contractor will include the provisions of paragraphs one through six in every subcontract, including procurements of materials and leases of equipment, unless exempt by the Acts, the Regulations and directives issued pursuant thereto. The contractor will take action with respect to any subcontract or procurement as the sponsor or the Federal Aviation Administration may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if the contractor becomes involved in, or is threatened with litigation by a subcontractor, or supplier because of such direction, the contractor may request the sponsor to enter into any litigation to protect the interests of the sponsor. In addition, the contractor may request the United States to enter into the litigation to protect the interests of the United States.

B.   Title VI List of Pertinent Nondiscrimination Acts and Authorities

During the performance of this contract, the contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "contractor") agrees to comply with the following non-discrimination statutes and authorities; including but not limited to:

• Title VI of the Civil Rights Act of 1964 (42 U.S.C. § 2000d et seq., 78 stat. 252), (prohibits discrimination on the basis of race, color, national origin);

• 49 CFR part 21 (Non-discrimination In Federally-Assisted Programs of The Department of Transportation—Effectuation of Title VI of The Civil Rights Act of 1964);

• The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, (42 U.S.C. § 4601), (prohibits unfair treatment of persons displaced or whose property has been acquired because of Federal or Federal-aid programs and projects);

• Section 504 of the Rehabilitation Act of 1973, (29 U.S.C. § 794 et seq.), as amended, (prohibits discrimination on the basis of disability); and 49 CFR part 27;

• The Age Discrimination Act of 1975, as amended, (42 U.S.C. § 6101 et seq.), (prohibits discrimination on the basis of age);

• Airport and Airway Improvement Act of 1982, (49 USC § 471, Section 47123), as amended, (prohibits discrimination based on race, creed, color, national origin, or sex);

• The Civil Rights Restoration Act of 1987, (PL 100-209), (Broadened the scope, coverage and applicability of Title VI of the Civil Rights Act of 1964, The Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1973, by expanding the definition of the terms "programs or activities" to include all of the programs or activities of the Federal-aid recipients, sub-recipients and contractors, whether such programs or activities are Federally funded or not);

• Titles II and III of the Americans with Disabilities Act of 1990, which prohibit discrimination on the basis of disability in the operation of public entities, public and private transportation

systems, places of public accommodation, and certain testing entities (42 U.S.C. §§ 12131 – 12189) as implemented by Department of Transportation regulations at 49 CFR parts 37 and 38;

• The Federal Aviation Administration's Non-discrimination statute (49 U.S.C. § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex);

• Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations, which ensures non-discrimination against minority populations by discouraging programs, policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations;

• Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting agency guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP). To ensure compliance with Title VI, you must take reasonable steps to ensure that LEP persons have meaningful access to your programs (70 Fed. Reg. at 74087 to 74100);

• Title IX of the Education Amendments of 1972, as amended, which prohibits you from discriminating because of sex in education programs or activities (20 U.S.C. § 1681 et seq).

C.   FAIR LABOR STANDARDS ACT

All contracts and subcontracts that result from this solicitation incorporate by reference the provisions of 29 CFR part 201, the Federal Fair Labor Standards Act (FLSA), with the same force and effect as if given in full text. The FLSA sets minimum wage, overtime pay, recordkeeping, and child labor standards for full and part time workers.

The [contractor | consultant] has full responsibility to monitor compliance to the referenced statute or regulation. The [contractor | consultant] must address any claims or disputes that arise from this requirement directly with the U.S. Department of Labor – Wage and Hour Division.

D.   OCCUPATIONAL SAFETY AND HEALTH ACT

All contracts and subcontracts that result from this solicitation incorporate by reference the requirements of 29 CFR Part 1910 with the same force and effect as if given in full text. Contractor must provide a work environment that is free from recognized hazards that may cause death or serious physical harm to the employee. The Contractor 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). Contractor 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.

Project 1403 – Identity Management-BadgEze Replacement

Deliverables required from Vendor

The following document explains the project deliverables and the order in which they are expected.

Tasks and Deliverables
This section describes project background and objectives and details deliverables for:

- **Task 1** – Project Preparation and Management
- **Task 2** – System Configuration
- **Task 3** – Historical Data/Report Conversion
- **Task 4** – Documentation and Training
- **Task 5** – Development and Quality Assurance Tier System Installation and Testing
- **Task 6** – Production Tier System Installation and Testing
- **Task 7** – Support and System Maintenance

Task 1: Project Preparation and Management

This section details the planning and documentation required to prepare for each remaining task.

Subtask 1.1: Project Management

The Vendor shall provide the necessary management, coordination and monitoring of all work activities throughout the term of the contract to ensure that the delivered system meets the project objectives while remaining on schedule and within budget.   The Vendor shall provide, for approval by the DEN Project Manager ("DEN PM"), a Project Management Plan that includes staffing, roles, responsibilities and skill sets for Vendor personnel assigned to the project as well as for those resources that will need to be provided by DEN.

The Vendor shall designate a Project Manager ("Vendor PM") as the single point of contact for the DEN PM, and assigned to work with DEN's project personnel for the duration of the project. The Vendor PM shall be responsible for managing and coordinating all Authorized Signatory Portal aspects of the work including project management, administration, coordination, status meetings, other necessary meetings and meeting summaries, invoicing, project reporting and subcontractor management. DEN shall approve the initial appointment and any replacement of the Vendor PM during the project term. DEN shall have the right to require replacement of the Vendor PM at any time during the project.

At a minimum to accomplish **Subtask 1.1**, the Vendor shall:

1. Have all Vendor project staff requiring access to DEN SSI and/or PII successfully complete security vetting process and comply with non-disclosure requirements.

2. Conduct a project kick-off meeting to be held on-site at DEN Airport. The project kick-off meeting shall provide a forum to familiarize project participants with the goals and objectives of the project, review the statement of work and planned deliverables, review the project schedule, identify critical success factors and potential risks, and confirm

expectations for user involvement. Establishing a mutual understanding of the project approach and details of the scope and objectives for the project shall set a reasonable expectation and address concerns of participants over their role in the project.

3.   Prepare project status meeting agendas, conduct project status meetings, and provide written status reports to the DEN Project Team members no less than bi-weekly throughout the duration of the project and more frequently if deemed necessary by DEN. At a minimum, the status reports shall include:

   A.   Tasks accomplished and milestones achieved since last meeting
   B.   Identification of issues impacting the project
   C.   Summary of next steps and upcoming milestones
   D.   Status of any contract change requests

4.   Ensure the quality and timeliness of meeting agendas, draft and final written summaries of all workshops and meetings, and all other project deliverables.

5.   Be available by phone if necessary to provide information during internal DEN project meetings.

6.   Ensure that all Vendor and Subcontractor staff have sufficient availability and on-site presence such that they are able to understand the broad scope and technical details of the project, and are able to develop productive working relationships with appropriate DEN staff. Vendor staff shall be on-site for all software installations on DEN test and production platforms.

7.   Included in the price of his contract is the requirement that Vendor provide sixty-five (65) individual 8-hour labor days of personnel on-site at DEN. Additional time onsite at DEN will be negotiated between Vendor and DEN.

8.   With the exception of status reports, all project deliverables shall be submitted in both draft and final form to allow for review and comment by DEN staff. Digital submittals are acceptable in all cases, provided they have presentation-quality formatting should DEN choose to print them for distribution.

9.   At a minimum to accomplish **Subtask 1.1** and in support of all subsequent tasks and **Subtasks**, DEN shall:

   A.   Provide meeting facilities
   B.   Participate in conference calls and status meetings
   C.   Coordinate attendance of DEN staff and project stakeholders for project meetings and activities
   D.   Review and comment on all submittals in a timely manner
   E.   Provide the Vendor with space for on-site work including IDMS and internet access as required

Exhibit A – Scope of Work

Subtask 1.1: Deliverables

1. Bi-weekly (or more frequent) status call agendas, calls and summaries
2. Additional meetings, meeting summaries and project correspondence as required
3. Draft and final Project Management Plan

Subtask 1.1: Acceptance Criteria

1. Project shall remain on schedule and on budget, or Vendor shall provide ample notice and justification of anticipated deviations
2. Final documents shall reflect feedback from DEN stakeholder reviews of draft documents and shall meet with DEN approval.

Subtask 1.2: Work Schedule

As part of the Project Management Plan, the Vendor shall submit a detailed Work Schedule for approval by the DEN PM. The Work Schedule shall identify individual project milestones with dates including, but not limited to: contract deliverable submittals, on-site time, status meetings, knowledge acquisition meetings, work sessions, draft and final document delivery, DEN review periods, system configuration, historical data conversion, documentation and training, system installation and testing, roll-out, and support periods. The Work Schedule shall include task dependencies and highlight the critical path.

The Contract schedule shall be defined as the baseline, and initial Work Schedule shall be defined as a subsequent baseline. The Vendor shall be responsible for maintaining the schedule throughout the life of the project and documenting any divergences from the baselines.

At a minimum to accomplish **Subtask 1.2**, the Vendor shall:

1. Review preliminary schedule with DEN PM and appropriate project team staff to solicit feedback and identify uncover potential schedule impacts

2. Provide Vendor with information regarding DEN resource availability and schedule constraints

Subtask 1.2: Deliverables

1. Draft and final Work Schedule with baselines, dependencies and critical path

2. Revised Work Schedules as required

3. Documentation of any divergences from baselines

Subtask 1.2: Acceptance Criteria

1. Schedule shall clearly illustrate tasks, milestones, dependencies and critical path

2. Schedule milestones shall include all task and **Subtask** deliverables listed herein

3. Schedule shall provide sufficient time for DEN to complete supporting deliverables

4. Revised schedules shall clearly illustrate baseline comparison

Subtask 1.3: Work Plan

As part of the Project Management Plan, the Vendor shall submit for approval by the DEN PM a detailed Work Plan identifying all methods and procedures that will be used to complete the project. The Work Plan shall include but not be limited to: task descriptions, responsible parties, due dates, method for calculating percent complete, and comments/notes.

The Vendor shall ensure that the Work Plan is kept up to date throughout the project. If, during the life of the project, the Work Plan changes, the Vendor shall update the documents accordingly, resubmit them for approval to the DEN PM, and immediately redistribute them to all project team members.

At a minimum to accomplish **Subtask 1.3**, the Vendor shall:

1. Review work plan elements with DEN PM and appropriate project team staff

2. Recommend resources required to complete work plan elements

3. For work plan elements requiring DEN project team participation, explain expectations for participation, required skill set, and anticipated teaming with Vendor project staff

At a minimum to accomplish **Subtask 1.3**, DEN shall:

1. Provide Vendor with information on DEN project team skill sets

Subtask 1.3: Deliverables

1. Draft and final Work Plan

2. Draft and final revised Work Plans as required

3. Documentation of any divergences from the baseline plan

Subtask 1.3: Acceptance Criteria

1. Work Plan elements shall map clearly to Schedule tasks

2. DEN project team members shall be assigned as resources on work plan elements provided that they have the appropriate skill set to meet the objectives of the task

----

Subtask 1.4: System Requirements Analysis

The Vendor shall review and analyze DEN's system requirements including Attachment B (IDMS Functional Requirements), existing documented workflows, draft desired workflows, existing reports, and other pertinent documents and processes. The Vendor shall conduct Knowledge Acquisition Meetings with project stakeholders at DEN. Attendees shall include Trusted Agents, Authorized Signatories, department heads and other affected parties as appropriate. The Vendor shall use the information gathered during this phase to create IDMS Workflow Diagrams, Functional Specifications and Acceptance Criteria and submit for approval by the DEN PM.

At a minimum to accomplish **Subtask 1.4**, the Vendor shall:

1. Review documentation provided by DEN

2. Meet with stakeholders as appropriate to develop a comprehensive understanding of

    A. Existing processes
    B. Required functions
    C. Paper processes to be automated
    D. Information flows between badging and related systems
    E. Desired process improvements

3. Recommend methods, process revisions, and/or technologies as appropriate that may not have been anticipated by DEN project staff

4. Provide information necessary to aid DEN project staff in evaluating such options as may be available

At a minimum to accomplish **Subtask 1.4**, DEN shall:

1. Identify project stakeholders to participate in knowledge acquisition meetings

2. Provide Vendor with Final DEN current workflow diagrams

3. Provide Vendor with Draft DEN future workflow diagrams

Subtask 1.4: Deliverables

1. Knowledge Acquisition Meeting Agendas and Meetings

2. Knowledge Acquisition Meeting draft and final Summaries

3. Draft and final Functional Specification with Acceptance Criteria

4. Draft and final IDMS Workflow Diagrams for DEN

Subtask 1.4: Acceptance Criteria

Exhibit A – Scope of Work

1. Designed solution shall provide all functionality:

   A. currently provided by the BadgEze system unless specifically excluded by mutual agreement of Vendor and DEN
   B. included in Contract Attachment B IDMS Functional Requirements

2. Eliminate paper applications

3. Eliminate redundant data entry

Subtask 1.5: Hardware, Network and Security Design

The Vendor shall conduct meetings as necessary with DEN IT Operations staff to understand the current BadgEze credentialing process and the Maxxnet Physical Access Control System and share with them information about how data must flow between IDMS and all associated applications/services. Working closely with DEN IT Operations, the Vendor shall develop for approval by DEN IT a Networking and Security Plan that allows the necessary data flows while providing the appropriate protections for SSI and PII.

Upon development of test and production platforms, DEN shall provide reasonable remote access for Vendor to test updates and apply them to the production environment. Prior to making any changes in the production environment, Vendor shall provide a written account of the intended changes and acquire written authorization from DEN. After making changes to either the test or production environment, Vendor shall provide a written account of actual changes, test procedures and test results.

At a minimum to accomplish **Subtask 1.5**, the Vendor shall:

1. Review documentation provided by DEN

2. Meet with stakeholders as appropriate to develop a comprehensive understanding of

   A. Existing DEN Credentialing and Badging process and Maxxnet Physical Access Control System
   B. Requirements for PCI compliance
   C. DEN IT and networking standards
   D. DEN Cyber Security requirements

3. Recommend system design scenarios as appropriate that may not have been anticipated by DEN project staff

4. Provide information necessary to aid DEN project staff in evaluating system design options including, if available, costs/resources required to implement comparable system designs at similar airports

At a minimum to accomplish **Subtask 1.5**, DEN shall:

1. Identify project stakeholders to participate in knowledge acquisition meetings

2. Provide to Vendor current platform and security standards

3. Provide to Vendor preliminary platform design scenarios

4. Review all hardware, network and security documentation in the Vendor proposal

Subtask 1.5: Deliverables

1. Knowledge Acquisition Meeting Agendas and Meetings

2. Knowledge Acquisition Meeting draft and final Summaries

3. Draft and final Hardware, Network and Security Design

Subtask 1.5: Acceptance Criteria

1. Test and production platforms shall:

   A. Comply with DEN and PCI standards as appropriate
   B. Ensure protection and confidentiality of SSI and PII within SAFE and during integration with related systems
   C. Enable required transmission of information as defined in Attachment B and **Subtask 1.4** Functional Requirements

----

Subtask 1.6: Vendor System Installation, Configuration, and Testing: Development, Quality Assurance, and Production Tiers.

Subtask 1.6 declares DEN expectations for vendor system installation, configuration, and testing. The overall requirement is to develop this plan for the DEN Development tier and to edit it as necessary prior to implementation on the DEN Quality Assurance tier and then the DEN Production tier. The inputs for this subtask are business requirements documentation, technical requirements documentation, and contract requirements as signed.

Configuration rather than coding shall drive IDMS processes, data quality assurance and reporting. Much of this configuration exists in the current BadgEze solution and associated reports, and must be migrated to IDMS. The Vendor shall identify configuration requirements via knowledge acquisition meetings with IDMS stakeholders.

All testing will be concurrent with production operation of existing BadgEze and associated badging components

At a minimum to accomplish Subtask 1.6, the Vendor shall:

Exhibit A – Scope of Work

1. Meet with stakeholders as appropriate to develop a comprehensive, airport-specific understanding of:

    A. Business rules governing existing workflows and status dependencies
    B. Business rules and lookup tables governing data validation and Quality Assurance
    C. Existing users of BadgEze and related badging systems, along with potential future users including but not limited to authorized signatories.

2. Define comprehensive sets of configurable

    A. Business rules and lookup tables to govern:

        I. Workflows and status dependencies
        II. Data validation and data Quality Assurance

    B. User groups and associated user privileges

3. Develop scripts to populate:

    A. Business rules for workflows, status dependencies, data validation and Quality Assurance
    B. Users, user groups, user group privileges, and assignments of users to user groups

4. Develop DEN-specific testing plans and test scripts for business rules, user configuration, functionality, and load testing including but not limited to:

    A. Clear description of the configuration and/or business rule being tested
    B. Acceptance criteria
    C. Space for the tester to record:

        I. Actual results
        II. Pass/fail indicator
        III. One or more screen images
        IV. Detailed notes (repeated tests, keystrokes, etc.)
        V. Spaces for sign-offs (testers, observers, etc.)

5. Document the processes necessary to install and configure and IDMS system including actual or simulated integrations with test versions of associated systems including but not limited to:

    A. Crossmatch Guardian Fingerprint Scanners
    B. Telos ID Designated Aviation Channeler (DAC)
    C. AAAE IET – Computer based training
    D. MaxxNet Access Control System
    E. Enterprise Cashiering Solution (ECS) Point of Sale
    F. E-mail communications and alerts
    G. Evolis Securion Badge Printers (open to alternative if necessary)
    H. Biometric enrollment (CoproMetro StoneLock Facial Recognition and ATMEL FAP3010 fingerprint scanners)

6. Provide that the each tier's IDMS installation is able to reliably identify and address any issues that might arise with or between the Authorized Signatory Portal, Badge Management Application and all other integrated applications

7. Develop a Production Installation Plan that addresses all roll-out steps and responsibilities, airport phasing, timing and anticipated system down time, roll-out communications prior to and during system cutover(s), final data conversion, and alternate procedures to be used during system cutover(s), and system roll-back in the event of problems.

8. At a minimum to accomplish Subtask 1.6, DEN shall:

   A. Identify project stakeholders and to participate in knowledge acquisition meetings:
   B. Provide guidance as to the acceptable level of system downtime during production cutover

Subtask 1.6: Deliverables

1. Knowledge Acquisition Meeting draft and final Summaries

2. Documented information required:

   A. Knowledge Acquisition Meeting Agendas and Meetings
   B. DEN-specific BadgEze Business Rules
   C. DEN Business Rule Configuration Specification and Scripts that shall comply with:
   D. All applicable regulatory requirements
   E. Attachment B and **Subtask 1.4** Functional Requirements
   F. DEN System Installation Plan
      (NOTE: Overall document format must be agreed upon by DEN and Vendor).

3. DEN User Configuration Specification and Scripts

4. DEN System Configuration and Integration Testing Plan and Test Scripts

5. DEN Production Installation Plan including Configuration and Integration Testing Plan and Test Scripts

Subtask 1.6: Acceptance Criteria

1. Business Rule Configuration Scripts shall be fully automated and repeatable

2. Business Rule and User Configuration Scripts must perform sufficiently fast such that, when combined with all other roll-out components, the production roll-out process fits within an acceptable window of system downtime

3. User Configuration Scripts shall be fully automated and repeatable

4. User accounts must be configured for all

   A. Existing users of BadgEze and other defined source systems
   B. IDMS system administrators
   C. Authorized Signatories

5. System Configuration Testing Plan and Test Scripts shall address the entire testing process including test script development, Vendor script execution, on-site script execution, problem remediation, on-site re-testing, and issue tracking

6. Test System Installation Plan shall include all components to comply with:

   A. All applicable regulatory requirements
   B. Attachment B and **Subtask 1.4** Functional Requirements

7. Production Installation Plan shall contain all tasks necessary to prepare for and execute the IDMS production roll-out. Tasks shall be organized and sequenced for easy reference during cut-over, and each task shall indicate what resource is responsible for successful task execution.

8. Production System Software and Integration Testing Plan and Test Scripts shall address the entire testing process including test script development, Vendor script execution, on-site script execution, problem remediation, on-site re-testing, and issue tracking.

9. Production System Software and Integration Testing Plan and Test Scripts shall include a roll-back indicator for issues encountered. The roll-back indicator shall determine whether issues are of sufficient severity to mandate a roll-back to the existing BadgEze badging system.

Subtask 1.7: Historical Data/Report Conversion and Testing Plan

The existing databases including but not limited to BadgEze all contain several years' worth of historical data and reports which the Vendor shall convert to IDMS.

Please note that the actual data migration and conversion process will require three (3) iterations; to Development, Quality Assurance, and Production tiers. Unique Knowledge-Gathering and Documentation may not be required for Quality Assurance and Production tiers if the **Subtask 1.7** User Acceptance Criteria below are met.

At a minimum to accomplish **Subtask 1.7**, the Vendor shall:

1. Conduct knowledge acquisition meetings to identify all source databases and determine what information must be migrated to IDMS.

2. Define a series of Data Quality Control Reports/Scripts to identify for all source databases potential data issues including but not limited to: duplicate records, orphan records, missing data, invalid data, or other data quality problems to be addressed by DEN prior to data conversion.

3. Develop a Data Conversion Specification

    A. Mapping all source database/table/fields to IDMS tables/fields
    B. Defining all business logic required for data conversion.

4. Develop scripts for each airport fully automating data conversion to enable iterative testing and refinement. If multiple scripts are required, the Vendor shall ideally automate the sequencing of scripts and shall at a minimum fully document the conversion procedures to ensure repeatability.

5. Conduct knowledge acquisition meetings to review existing reports and identify additional required reports.

6. Develop a Report Specification listing all reports required for IDMS and identifying how the reporting objectives will be addressed via standard reports, custom reports or other method. The Specification shall contain all information necessary to develop the reports including but not limited to tables, fields, filters, parameters, headers, footers, grouping, sorting and aggregation.

7. Develop DEN-specific testing plans and testing scripts to ensure that all required data reflects the data cleanup recommended in the Data Quality Control Report, has been successfully converted as defined in the Data Conversion Specification, and that all reports defined in the Report Specification run successfully and accurately. The test scripts shall include but not be limited to:

    A. Clear description of the data conversion or report being tested
    B. Acceptance criteria (record counts, referential integrity, etc.)
    C. Space for the tester to record:
       i. Actual results
      ii. Pass/fail indicator
     iii. One or more screen images
     iv. Detailed notes (repeated tests, keystrokes, etc.)
      v. Spaces for sign-offs (testers, observers, etc.).

At a minimum to accomplish **Subtask 1.7**, DEN shall:

1. Identify stakeholders for knowledge acquisition meetings.

2. Perform data cleanup identified by Data Quality Control Reports/Scripts.

3. Make available to the Vendor all available source data model documentation.

4. Provide Vendor with access to source data for purposes of data conversion scripting and testing.

5. Provide Vendor with demonstrations of existing reporting and, as necessary, source files.

Subtask 1.7: Deliverables

1. Knowledge Acquisition Meeting Agendas and Meetings

2. Knowledge Acquisition Meeting draft and final Summaries

3. Draft and final Data Quality Control Reports/Scripts

4. Draft and final Data Conversion Specification and Scripts

5. Draft and final Report Specification

6. Draft and final Data and Report Conversion Testing Plan and Test Scripts

Subtask 1.7: Acceptance Criteria

1. Data Quality Control Reports shall contain all data cleanup that must be completed by DEN prior to commencement of historical data conversion

2. Data Conversion and Report Specifications shall comply with:

   A. All applicable regulatory requirements
   B. Attachment B and **Subtask 1.4** Functional Requirements

3. Data conversion scripts shall be fully automated and repeatable

4. Data conversion scripts must perform sufficiently fast such that, when combined with all other roll-out components, the production roll-out process fits within an acceptable window of system downtime

5. Data and Report Conversion Testing Plan and Test Scripts shall address the entire testing process including test script development, Vendor script execution, on-site script execution, problem remediation, on-site re-testing, and issue tracking

----

Subtask 1.8: Documentation and Training Plan

Thorough documentation and training are critical success factors in any software implementation. The Vendor shall prepare Documentation and Training Plans for IDMS system administrators, Badge Management Application users and Authorized Signatory Portal users.

At a minimum to accomplish **Subtask 1.8**, the Vendor shall:

1. Conduct knowledge acquisition meetings as needed to understand and clarify revised badging workflows and SOPs to be implemented in conjunction with IDMS

2. Develop an outline for System Administrator Documentation including but not limited to: user login and privilege management, data model documentation with table relationships and constraints, workflow diagrams, system integration requirements and specification, and business rule management.

3. Develop a System Administrator Training Plan including but not limited to class syllabus, estimated class sizes and lengths, and methodology to deliver training to all system administrators.

4. Develop an outline for Badge Management Application training including instructions on the use of all functionality and modules of IDMS's badge management interface, and clear documentation of all workflows and SOPs required for managing security badging.

5. Develop a Badge Management Application Training Plan including but not limited to class syllabus, estimated class sizes and lengths, and methodology to deliver training to all Badge Management Application users.

6. Develop an outline for Authorized Signatory Portal training including instructions on the use of all functionality and modules of IDMS's authorized signatory portal and clear documentation of all workflows and SOPs required for executing authorized signatory responsibilities.

7. Develop an Authorized Signatory Portal Training Plan including but not limited to class syllabus, estimated class sizes and lengths, and methodology to deliver training to all Authorized Signatories.

At a minimum to accomplish **Subtask 1.8**, DEN shall:

1. Identify stakeholders for knowledge acquisition meetings

Subtask 1.8: Deliverables

1. Knowledge Acquisition Meeting Agendas and Meetings

2. Knowledge Acquisition Meeting draft and final Summaries

3. Draft and final System Administrator, Badge Management Application User and Authorized Signatory Portal User Documentation Outlines

4. Draft and final System Administrator, Badge Management Application User and Authorized Signatory Portal User Training Plans

Subtask 1.8: Acceptance Criteria

1. Documentation and Training Plans shall reflect operation of the IDMS solution within DEN

workflows and SOPs

2. Training Plans shall account for all IDMS users reflected in the revised workflows and SOPs

----

Subtask 1.9: Support and System Maintenance Plan

Once IDMS has been implemented, it will be necessary to have the correct support structures and resources in place to ensure successful continuous operations of IDMS and required integrations, and to provide upgrades as necessary to remain compliant with regulatory requirements and upgrades to integrated solution components.

At a minimum to accomplish **Subtask 1.9**, the Vendor shall:

1. Provide on-site support for a minimum of four (4) weeks following production roll-out at DEN

2. Be on-site as necessary throughout the project term for meetings and deliverable testing

3. Develop for DEN approval a Warranty and Maintenance Agreement defining the service level including but not limited to:

    A. From the completion of **Task 7**: Support and System Maintenance, until the final day of the thirty-sixth (36th) month after the signing of this contract, the Vendor shall warrant that all the performance of all software, interfaces, setup and configuration services, software modifications, hardware, and changes performed or provided under this agreement meet the requirements contained in Attachment B and **Subtask 1.4** Functional Requirements, and are free of defects in workmanship or inconsistencies.
    B. The Agreement shall clearly document service levels including but not limited to coverage time, response time and acceptable system downtime. If any defects or inconsistencies are discovered during the warranty period, then the Vendor shall be responsible for rectifying them at no additional cost to DEN.
    C. As part of the maintenance the Vendor shall provide standard maintenance and technical support consisting of all labor, software upgrades, documentation revisions, support, and preventive maintenance services necessary to keep IDMS software, configuration and integration components in good operating condition, in full compliance with all applicable regulatory requirements, and in full compliance with Attachment B and **Subtask 1.4** Functional Requirements.

4. Develop for DEN approval a Standard Maintenance and Technical Support Agreement to commence, at DEN's option, at the completion of **Task 7**: Support and System Maintenance.

5. Agreement shall at a minimum:

    A. Clearly document service levels including but not limited to coverage time, response time and acceptable system downtime.

B. Include at a minimum all labor, software upgrades, documentation revisions, support, and preventive maintenance services necessary to keep IDMS software, configuration and integration components in good operating condition, in full compliance with all applicable regulatory requirements, and in full compliance with Attachment B and **Subtask 1.4** Functional Requirements.

C. Provide for at a minimum live phone support Monday-Friday from 6:30am-6:30pm EST, and on-call support via phone or web 24/7 with a maximum initial response time of one hour.

D. Provide a process for system upgrades whereby production system downtime shall not exceed one hour without prior approval from DEN.

At a minimum to accomplish **Subtask 1.9**, Vendor shall:

Subtask 1.9: Deliverables

1. Draft and final Warranty Agreement

2. Draft and final Maintenance and Technical Support Agreement

Subtask 1.9: Acceptance Criteria

1. Combination of standard Vendor warranty and warranty/support described herein shall provide for uninterrupted coverage of software, interfaces, setup and configuration services, software modifications, hardware, and changes performed or provided under this agreement

----

Task 2: System Configuration Testing

Upon completion of **Subtask 1.6**: **Vendor System Installation, Configuration, and Testing: Development, Quality Assurance, and Production Tiers** and collection of preliminary user configuration information, the Vendor shall begin iterative system configuration and testing, sequentially, first on the Development tier and then, upon DEN approval, on the Quality Assurance tier.

NOTE: <u>The requirement is to test the SAFE solution first on the DEN Development tier and to subsequently test the SAFE solution on the DEN Quality Assurance tier.</u>

At a minimum to accomplish **Task 2**, the Vendor shall:

1. Test all configuration scripts on Vendor's development system prior to running them on-site on the DEN test database

2. On the DEN on-site test database, execute the Business Rule Configuration Scripts and User Configuration Scripts developed under **Subtask 1.6** to generate the:

   A. Business rules required to support workflows and data Quality Assurance
   B. Users, user groups and user privileges to control function and data access in the Authorized Signatory Portal and Badge Management Application

3. Hold primary responsibility for:

   A. Executing on-site the System Configuration Testing Plan and Test Scripts developed under **Subtask 1.6**
   B. Clearly documenting the results
   C. Logging all issues, problems and/or defects as documented under **Subtask 1.6**
   D. Analyzing and remediating documented issues, rerunning scripts, and re-testing documented issues
   E. Signing off on all testing

At a minimum to accomplish **Task 2**, DEN shall:

1. Provide project team members to participate in testing as appropriate and log issues, problems and/or defects as documented under **Subtask 1.6**

2. Upon acceptable completion of testing, the DEN PM shall sign off on all test results to indicate approval that the testing was done in good faith, was complete, and the results were accurate and met the documented acceptance criteria

Task 2: Deliverables

1. Tested and DEN Approved Business Rule Configuration Scripts

2. Tested and DEN Approved User Configuration Scripts

Task 2: Acceptance Criteria
1. The test/log/analyze/remediate/rerun cycle shall be repeated as many times as necessary until both DEN and the Vendor agree that the results comply with Attachment B, **Subtask 1.4** Functional Requirements, and **Subtask 1.6** Acceptance Criteria.

Task 3: Historical Data/Report Conversion Testing

Upon completion of **Subtask 1.7**: Historical Data/Report Conversion and Testing Plan and correction by DEN of outstanding data quality issues, the Vendor shall begin iterative historical data and report conversion and testing.

NOTE: The requirement is to convert and migrate data and test first to the DEN Development tier and to subsequently convert and migrate data and test the SAFE solution on the DEN Quality Assurance tier.

At a minimum to accomplish **Task 3**, the Vendor shall:

1. Test all data conversion scripts and reports on Vendor's development system prior to running/installing them on-site on the DEN test database

2. On the DEN on-site test database, execute the Data Conversion Scripts and install Reports

developed under **Subtask 1.7** to generate the:

    A. Data required to support all IDMS functionality
    B. Reports required to provide required access to IDMS data

3.   Hold primary responsibility for:

    A. Executing on-site the Data and Report Conversion Testing Plan and Test Scripts developed under **Subtask 1.7**
    B. Clearly documenting the results
    C. Logging all issues, problems and/or defects as documented under **Subtask 1.7**
    D. Analyzing and remediating documented issues, rerunning scripts, and re-testing documented issues
    E. Signing off on all testing

At a minimum to accomplish **Task 3**, DEN shall:

1. Provide project team members to participate in testing as appropriate and log issues, problems and/or defects as documented under **Subtask 1.7**
2. Upon acceptable completion of testing, the DEN PM shall sign off on all test results to indicate approval that the testing was done in good faith, was complete, and the results were accurate and met the documented acceptance criteria

Task 3 Deliverables

1. Tested and DEN Approved Historical Data Conversion Scripts
2. Tested and DEN Approved IDMS Reports

Task 3 Acceptance Criteria

1. The test/log/analyze/remediate/rerun cycle shall be repeated as many times as necessary until both DEN and the Vendor agree that the results comply with Attachment B, **Subtask 1.4** Functional Requirements, and **Subtask 1.7** Acceptance Criteria.

Task 4: Documentation and Training

Upon completion of **Subtask 1.8**: Documentation and Training Plan, **Task 2**: System Configuration Testing, and **Task 3**: Historical Data/Report Conversion Testing; the Vendor shall have sufficient information to complete development of the System Administrator, Badge Management Application User, and Authorized Signatory Portal User and Training Documentation outlined under **Subtask 1.8**.

At a minimum to accomplish **Task 4**, the Vendor shall:

1. Work with the DEN Project Team to develop and distribute documentation to the appropriate user groups

2. Conduct training for a subset of IDMS users selected to participate in system testing

3. Using feedback from the initial training sessions and from user testing, revise the documentation as appropriate. Documentation will be considered final when approved by the DEN PM.

4. Prior to **Task 6**: Production System Installation, work with the DEN Project Team to conduct training for all IDMS Badge Management Application users, Authorized Signatory Portal users, and system administrators.

At a minimum to accomplish **Task 4**, DEN shall:

1. Participate in development of documentation to ensure that all workflows and SOPs are accurately reflected.

2. Provide iterative feedback on draft user/administrator and training documents

3. Coordinate communication with and schedule training for IDMS Badge Management Application users, Authorized Signatory Portal users and system administrators

Task 4: Deliverables

1. Draft and final System Administrator and Training Documentation

2. Draft and final Badge Management Application User and Training Documentation

3. Draft and final Authorized Signatory Portal User and Training Documentation

4. Training executed for all users

Task 4: Acceptance Criteria

1. Documentation reflects IDMS functionality as it will be used within DEN workflows and SOPs

2. Documentation meets with project team approval for completeness, clarity, and ease of use.

3. All system administrators, Badge Management Application users and Authorized Signatory Portal users have been trained and are ready to convert production operations to IDMS

Task 5: Test System Installation and Testing

Upon completion of **Subtask 1.6**: Test System Installation and Testing Plan, **Task 2**: System Configuration Testing, and **Task 3**: Historical Data/Report Conversion Testing; the Vendor shall work with the DEN Project Team and IT Operations to install IDMS on an on-site test platform and execute testing.

Exhibit A – Scope of Work

NOTE: <u>The requirement is to install and test the SAFE solution first on the DEN Development tier (5a) and to subsequently install and test the SAFE solution on the DEN Quality Assurance tier (5b).</u>

At a minimum to accomplish **Task 5**, the Vendor shall:

1. Supply, install and configure at the Vendor site all hardware, software, networking, and security necessary to sufficiently simulate DEN's target production environment.

2. Work with DEN PM and IT Operations team to supply, install, and configure a secure, on-site testing platform capable of supporting functionality and load testing for all system modules and integrations

3. Using the secure, on-site test platform, install and configure all IDMS components and integrations for training and testing.

4. Hold primary responsibility for

   A. Executing on-site the Test System Software and Integration Testing Plan and Test Scripts developed under **Subtask 1.6**
   B. Clearly documenting the results
   C. Logging all issues, problems and/or defects as documented under **Subtask 1.6**
   D. Analyzing and remediating documented issues, rerunning scripts, and re-testing documented issues
   E. Signing off on all testing

At a minimum to accomplish **Task 5**, DEN shall:

1. Supply space and infrastructure necessary to support installation and configuration of hardware, software, networking and security for on-site test environment

2. Provide project team members to participate in testing as appropriate and log issues, problems and/or defects as documented under **Subtask 1.6**

3. Upon acceptable completion of testing, the DEN PM shall sign off on all test results to indicate approval that the testing was done in good faith, was complete, and the results were accurate and met the documented acceptance criteria

Task 5: Deliverables

1. Supply and configuration of secure, on-site testing environment

2. Functioning IDMS test system for use by select users in parallel testing

3. DEN Acceptance of IDMS test system

Task 5: Acceptance Criteria

1. The test system must include all required IDMS modules and actual or simulated integrations with test versions of associated systems including but not limited to:

    A. Crossmatch Guardian Fingerprint Scanners
    B. Telos ID Designated Aviation Channeler (DAC)
    C. AAAE IET – Computer based training
    D. MaxxNet Access Control System
    E. Enterprise Cashiering Solution (ESC) Point of Sale
    F. E-mail communications and alerts
    G. Evolis Securion Badge Printers (open to alternative if necessary)
    H. Biometric enrollment (CoproMetro StoneLock Facial Recognition and ATMEL FAP3010 fingerprint scanners)

2. The test system must provide the ability to reliably identify and address any issues that might arise with or between the Authorized Signatory Portal, Badge Management Application and all other integrated applications

3. Test system performance must comply with Attachment B, **Subtask 1.4** Functional Requirements, and **Subtask 1.5** Acceptance Criteria.

4. The test/log/analyze/remediate/rerun cycle shall be repeated as many times as necessary until both DEN and the Vendor agree that the results comply with Attachment B, **Subtask 1.4** Functional Requirements, and **Subtask 1.6** Acceptance Criteria.

Task 6: Production System Installation and Testing

Upon completion of **Task 5**: Test System Installation and Testing, DEN sign-off on the IDMS test system, and preparation of the necessary production hardware and networking; the Vendor shall work with the DEN Project Team and IT Operations to install IDMS on the production platform and convert production operations from BadgEze and other required systems to IDMS.

At a minimum to accomplish **Task 6** for each airport, the Vendor shall:

1. Install all required IDMS modules and integrations on the production platform

2. Run scripts to configure:

    A. Business rules governing workflows and status dependencies
    B. Business rules governing data validation and Quality Assurance
    C. User groups and privileges
    D. User accounts for all required system administrators, Badge Management Application users and Authorized Signatory Portal users

3. Run scripts to convert historical data from all appropriate source databases

4. Install all required standard and custom reporting

5. Hold primary responsibility for

A. Executing on-site the Production System Software and Integration Testing Plan and Test Scripts developed under **Subtask 1.6**
B. Clearly documenting the results
C. Logging all issues, problems and/or defects as documented under **Subtask 1.6**
D. Analyzing and remediating documented issues, rerunning scripts, and re-testing documented issues
E. Signing off on all testing

6. Prepare interim status communications to be delivered prior to and during production cut-over

7. Roll back production cutover to pre-IDMS systems if directed to do so by DEN PM

At a minimum to accomplish **Task 6**, DEN shall:

1. Supply space and infrastructure necessary to support installation and configuration of hardware, software, networking and security for on-site production environment

2. Install and configure on-site production platform hardware, networking and security

3. Provide project team members to participate in production testing as appropriate and log issues, problems and/or defects as documented under **Subtask 1.6**

4. Coordinate and deliver interim status communications to be delivered prior to and during production cut-over

5. Determine at the earliest possible time whether any identified issues warrant rolling back to the use of pre-IDMS systems and recommencing parallel testing

6. Upon acceptable completion of testing, the DEN PM shall sign off on all test results to indicate approval that the testing was done in good faith, was complete, and the results were accurate and met the documented acceptance criteria

7. Upon successful completion of testing, the DEN PM shall provide formal written acceptance of production IDMS for subject airport(s)

Task 6: Deliverables

1. Fully functioning IDMS production system

2. Punch list of issues to be addressed during post roll-out on-site support

Task 6: Acceptance Criteria

1. Production cutover is fully executed for DEN within the acceptable downtime established under **Subtask 1.6**

2. Production IDMS complies with Attachment B, **Subtask 1.4** Functional Requirements, and all Acceptance Criteria developed under this contract.

3. Production IDMS allows for full and immediate retirements of BadgEze and other migrated systems

---

Task 7: Support and System Maintenance

Upon completion of **Task 6**: Production System Installation and Testing, the Support and System Maintenance period shall commence. At the conclusion of the thirty-sixth month after the signing of this contract, DEN may optionally purchase additional yearly support and maintenance to remain current with version releases, regulatory requirements and integration upgrades.

At a minimum to accomplish **Task 7**, the Vendor shall:

1. Provide a minimum of four (4) weeks of on-site support as defined in **Subtask 1.9**.

2. Provide all software upgrades and associated support services as defined under **Subtask 1.9**

At a minimum to accomplish **Task 7**, DEN shall:

1. Maintain supported versions of test and production platform hardware, software, networking and security

2. Pay yearly maintenance fees to continue optional yearly support

Task 7: Deliverables

1. Minimum four (4) weeks of on-site support following production cutover. Up to eighteen (18) months year of full IDMS warranty and system support and maintenance as defined in **Subtask 1.9**

2. Additional support and maintenance as optionally purchased by DEN as defined in **Subtask 1.9**

Task 7: Acceptance Criteria

Exhibit A – Scope of Work

1. Punch list of issues addressed during post roll-out on-site support

2. Ongoing support for all IDMS software, configuration and integration components

----

Requirement #	Functionality
1.0 Badge Type	
1.1-1	Manage application, enrollment and issue of Secured and Sterile Area Only badges
1.1-2	Manage application, enrollment and issue of Public Area ID badges
1.1-3	Support existing encoding for low frequency cards and 13.56 mhz for high-frequency cards
1.1-4	Manage application, enrollment and issue of temporary visitor passes
2.0 Authorized Signatory Portal	
2.1-1	Restrict renewal of badges to those badges expiring within a pre-configured time period (e.g., 30 days)
2.1-2	Ability to allow portal access by other parties with approval from Security (DEN OHR, CBP, Denver Police Department, DEN Operations, etc.)
2.1-3	Must be accessible from one or more kiosks and associated scanner to be installed near the badge office
2.1-4	Usability features such as auto-moving cursor to next logical field, alpha-sorted drop down menus and look-up lists, on-screen required field indicators, links, hyperlinks, sub tabs, etc.
2.1-5	Ability to download/print relevant forms including blank application and/or approval forms
2.1-6	Ability to retrieve badge by name and title, DOB, badge number, SSN, etc.
2.1-7	On-line interface for use by Authorized Signatory with employee to enter badge application information
2.1-8	On-line lost/stolen/damaged badge reporting
2.1-9	Work with DEN IT to transfer BadgEze current calendar year Sterile Area visitor badge and Secured Area visitor events into IDMS.
2.1-10	Default field values for badge renewal based on previous badge for that badge holder / company. If new company, allow Authorized Signatory to select badge to use for default values (see current badge renewal paperwork)
2.1-11	For scanned/photographed documents, require Trusted Agent to select document type from a predefined list and enter key fields relevant to that document type
2.1-12	Notes sections include formatting tools, spelling checks and grammar checks
2.1-13	Default door access by company, department and access level
2.1-14	Set badge expiration date based on combination of endorsements, contract (if applicable), breeder document and work visa expiration dates
2.1-15	Ability to view image of badge - Print preview only at the time of printing
2.1-16	Require Trusted Agent approval of applications for temporary visitor passes by employees who have any active Secured Area badges, any unresolved unaccounted for badges, or recently expired badges for the same company
2.1-17	Require reason for badge (e.g., new, renewal, replacement, revised access, name change) and do not default any fields that should have different values based on the reason for the badge
2.1-18	Form generation - Authorization to transmit FP results to CBP - required once Authorized Signatory indicated need for Customs seal - gather required fields, produce form or export files for CBP
2.1-19	Require valid driver's license if applicant requires movement or non-movement driving privileges. Prohibit addition of endorsement without Trusted Agent approval if not provided by Authorized Signatory.
2.1-20	Restrict driving access to only requesting individuals associated with companies having valid airfield driving insurance and who have passed driving training
2.1-21	Ability to store notes with the badge holder and/or with an individual badge
2.1-22	Clear and concise data error/validation messages indicating action required to address

2.1-23	Prevent submission of application until all validation checks have been passed
2.1-24	Perform regular timed saves of data entered via portal in case of computer crash or time out
2.1-25	Ability to store partially completed applications and automatically delete them if not completed after a pre-configured period of time
2.1-26	Clearly track progression of badge through statuses as configured in site-specific workflow business rules - i.e., awaiting: application acceptance, fingerprinting, STA, CHRC adjudication, in-person CBP visit, CBP checks, CBT, driver training, badge pickup, badge suspension or termination, badge return and recovery
2.1-27	On-line user documentation that contains guidelines currently in DEN badge renewal letter, Authorized Signatory Portal and website
2.1-28	Ability to scan (or photograph) and digitally link breeder documents (IDs) to badges/identities
2.1-29	Ability to utilize existing scanned documents for future applications
2.1-30	Ability to capture electronic signatures from authorized signatories
2.1-31	Require Authorized Signatory to authorize applications prior to submission, thus supplying their digital signature
2.1-32	On-line notification of badge suspension/termination
2.1-33	Ability for Authorized Signatory to request badge be temporarily deactivated
2.1-34	Ability for Authorized Signatory to request scheduled permanent or temporary deactivation of badge
2.1-35	Ability to report change in CHRC status for arrest, conviction or disqualifying offense
2.1-36	Ability to request application cancellation
2.1-37	Provide self-service web portal with the capability to enable Authorized Signatory functions (applicant processing, badge cancellation request, reporting, auditing, etc.)
2.1-38	Make physical access privilege requests via Authorized Signatory portal
2.1-39	Receive physical access privilege change approvals via Authorized Signatory portal
2.1-40	Provide ability to complete and submit NEW badge application request via Authorized Signatory portal prior to arrival in the Security Badging Office
2.1-41	Provide ability to complete and submit RENEWAL/CHANGE badge application request via Authorized Signatory portal prior to arrival in the Security Badging Office
2.1-42	Support email notifications of the approved access privilege to all Authorized Signatories as defined in the policy
2.1-43	Provide a company notification system that utilizes email and a secure website portal for notifications and report distribution (See notification section for all notifications)
2.1-44	Provide automated Authorized Signatory notifications (via email): vetting approval and subsequent training requirements, expiration/renewal reminder with subsequent training requirements, etc. (See notification section for all notifications)
2.1-45	Provide provision for approved companies to submit certification for CHRC adjudication
2.1-46	Provide method for companies certifying CHRC adjudication to indicate (certify) TSA privacy policy has been presented to applicant by the Authorized Signatory
2.1-47	Allow Authorized Signatories to modify the employee information or request changes to access levels and privileges while restricting changes to name, DOB and other fields deemed to be critical to the STA process
2.1-48	Allow Authorized Signatories to request keys, vehicle permits and other assets
2.1-49	Prevent Authorized Signatories from sending incomplete application forms through Authorized Signatory portal

2.1-50	Provide ability for Authorized Signatory to upload certain documents to portal to attach to badge record
2.1-51	Provide ability to provide email notification to selected Authorized Signatories that there has been a cipher code change for jet bridge access, without transferring the new cipher code itself.
2.1-52	Show badges under suspension on Authorized Signatory dashboard and when activated again
2.1-53	Provide list of "expiring" CHRC dates for Authorized Signatory's company based on DEN's defined parameter
2.1-54	Provide on dashboard 30-day notice of badge expiration for company employees. Highlight in red those expiring in less than 10 days
2.1-55	Authorized Signatory should be able to respond to a violation notice via the Authorized Signatory portal
2.1-56	Allow an access level for CBP to add/remove an FIS seal authorization to individual records per individual employer/ badge
3.0 Fingerprinting	
3.1-1	Automatically determine if an applicant needs to be (re)fingerprinted based on access level and recurrent CHRC interval. If prior CHRC are to be used, link that fingerprint record to the current or new badge application
3.1-2	Capture electronic signature of applicant prior to fingerprint capture; associate with statement re: disqualifying offenses
3.1-3	Capture both Type 14 images (slaps) from existing Crossmatch Guardian or other recommended fingerprint capture device(s) with equal or greater capabilities
3.1-5	Track fingerprint collection date and ID of person capturing print. Associate fingerprint information with person and badge records. SAFE does not capture the ID of the person capturing the fingerprints. All other information is captured related to date and person information.
3.1-6	Ability to use an alternative to a fingerprint biometric in the event an acceptable image cannot be captured (PIN, etc…)
3.1-7	Capture a biometric during the card applicant enrollment process
3.1-8	At a minimum, support the capture of ANSI 378 fingerprint biometric templates
3.1-9	Capture biometrics into the database for card production and use reference biometric when the cardholder physically is issued the badge to ensure the person accepting the badge and the reference biometric in the system are the same
3.1-10	Provide capability to use a reference biometric to identify an individual when checking in for any integrated training
4.0 Background Checks	
4.1-1	Have business rules that determine what background checks are necessary for various access levels (e.g., STA, CHRC, etc.)
4.1-2	Business rules to determine if background checks can be skipped if previously completed within a predefined period of time. If prior background checks are to be used, link them the current badge application
4.1-3	Require fingerprinting and background checks as appropriate if application submitted more than 30 days (configurable number) after prior badge deactivation
4.1-4	Ability to automatically validate applicants against TSA's No-Fly, Selectee and DEN internal lists and notify the Trusted Agent of any matches
4.1-5	Ensure that FP, CHRC and STA are sent to DAC simultaneously

4.1-6	Ability to submit additional documents to the selected DAC if required to complete background checks
4.1-7	Report indicating pending correction of disqualifying offenses on CHRC older than user-defined period of days to enable denial of credential
4.1-8	Limit access to background check results to only those users with sufficient privileges
4.1-9	Automatically update application record with STA results
4.1-10	Ability to log when an applicant intends to correct disqualifying information on a CHRC
4.1-11	Enable a second set of fingerprints to be taken when prints are returned as unclassifiable. Associate subsequent prints with the original CHRC record.
4.1-12	If second set of prints is returned as unclassifiable, ability to record the applicant for a name-based background check
4.1-13	Ability to configure automatic creation of an DEN interview task if CHRC and/or STA do not clear
4.1-14	If there is an issue with CHRC and/or STA results, automatically set status of the background check task to indicate that attention is required
4.1-15	Ensure compliance with the applicable requirements under Security Directive 1542-04-08K or subsequent updates. Vendor may contact John O'Connor at john.oconnor@flydenver.com for Security Directive information. NOTE: Quantum Secure works with its AV Community to agree the requisite system configuartions to meet compliance to TSA regulations. Through this mechanism we maintain compliance, but we are not responsible for designing the system's compliance or in any way certifying it as compliant. We must collaborate with our customers and the industry organizations that help us stay aligned. The software support and maintenance include updates based on these community agreed configurations at no license cost, but professional services may apply, depending on the changes and testing required.
4.1-16	Automatically retrieves results from the TSA-approved DAC and update/populate matched results to the existing cardholder database
4.1-17	Provide an automated method of reconciling IDMS records with the current DAC
4.1-18	Allow for badge applicant to be marked as exempt based on 1542-04-08H and not undergo STA assessment
4.1-19	Provide the functionality to limit the review of background check results to authorized personnel/defined users
4.1-20	Provide ability to create a DEN "DNI" or "DEN-Internal WL" (allows DEN to flag records so if an individual reapplies under another company or name (using same SSN) the flag would be identified
4.1-21	Maintain separate dispositions for CHRC's, STA's, and badges. Dispositions must match those defined by the current DAC: Badges are maintained seperately too with their respective attributes.
4.1-22	Capability to add unlimited types of background investigations (beyond CHRC/STA), configurable by the System Administrator.
4.1-23	Record background investigations (security checks), inclusive of the date the background investigation is submitted to an outside entity (i.e., an investigative source), the date of receipt of information from outside entities, and the final adjudication and status determination made by DEN personnel after reviewing the information provided by outside entities.
4.1-24	Provide CBP user role the ability to receive authorization for CBP seal from the local CBP office

4.1-25	Provide the ability for automated renewal of CHRC checks as defined by rules set by City to meet 1542-04-08I requirements
4.1-26	Provide ability to print new badge after a renewal CHRC is submitted and that all access is granted even though the security checks are not completed
4.1-27	Support the importation of the Transportation Security Administration's (TSA) "No-Fly" and "Selectee" Lists and provide automatic cross-comparison and matching against the current City cardholders, and Visitor badges. Ensure compliance with the applicable requirements under Security Directive 1542-01-10H

4.1-29	Provide the capability to import these lists and run the comparisons as often as the System Administrator desires
4.1-30	Utilize phonetic algorithms to form matches ("Andersen" sounds like "Anderson")
4.1-31	Allow for reverse order of names to form matches (last_name = first_name AND first_name = last_name)
4.1-32	Scrub titles and honorifics from the source list ("Dr.," "Mrs.," "Ms.," "Mr.," etc.)
4.1-33	Allow the System Administrator the ability to edit the list of titles and honorifics
4.1-34	Provide process for visually comparing and resolving Watch List matches where the DEN badgeholder information is simultaneously shown with all available Watch List entries
4.1-35	Provide a method for manager or authorized user to clear up any matches by entering notes about how the manager determined that the DEN badgeholder is not the same individual in the Watch List
4.1-36	Flag a cardholders record when "cleared," in such a manner that the record shall not appear as a match if the same record appears again in future Watch Lists
4.1-37	Provide capability to check against the Watch List when an application is processed and each time it is changed
4.1-38	Generate reports based on the status of matches (cleared, under investigation, actual match, etc.), and be capable of being exported into multiple formats at a minimum, .csv, .pdf and .xlsx formats
4.1-39	Ensure the UI enforces data type, field length, and formatting limitations dictated by lowest common denominator of dependent subsystems (i.e. Telos Clearinghouse ICD)
4.1-40	Provide capability to reconcile IDMS database against the DAC and FDMS/FPS databases
4.1-41	Provide validation tables used to enforce the input of data elements also validated by the City DAC (Currently Telos) must be user-maintained, allowing for easy updates to maintain data compliance
5.0 Credential Verification	
5.1-1	Apply business rules to ensure the appropriate breeder documents are supplied given the applicant's citizenship and POB
5.1-2	Provide on-line context sensitive guidance as to which IDs are acceptable
5.1-3	Require supplemental identification when appropriate (e.g., name change forms, J-1 and F-1 visas, etc.)
5.1-4	For U.S.-born applicants, require birth certificate or US Passport verifying citizenship
5.1-5	Prevent submission of inconsistent breeder documents - e.g., US Passport with resident alien card
5.1-6	Ability to manage status of non-standard documents to require specific rules to review and/or accept those documents.
5.1-7	Ability to generate report for batch vetting / re-vetting of applicants via external database
5.1-8	Compare auto-extract key fields from standard ID formats, verify match to application data (ID type, name, DOB, SSN, etc.)

5.1-10	Develop business rules to automatically flag applicants who should not get badges if they apply in the future and the reason why (e.g., fired, previously denied badge, document fraud, no legal work authorization, imposter, infractions, etc.). Automatically compare badge applications against this flag and set status to denied pending Security Admin review if applicants are flagged for badge denial.
5.1-11	Prevent issuance of badge to applicants whose IDs do not allow working in the US
5.1-12	Prevent issuance of badge to applicants with expired IDs
5.1-13	Prevent issuance of badge when key ID fields (name, DOB, SSN, etc.) do not match application
5.1-14	Verify biometric at each step after fingerprinting has occurred - CBT, badge issue
5.1-15	Track last date worked and termination date
5.1-16	Track instances of fraudulent document submission; link to badge application and badge holder
5.1-17	Track applicants who were denied badges, date denied and reason denied
5.1-19	Display photo with person's account
5.1-20	Handle name change forms to supply backup for disparate names on IDs (e.g., divorce decree, marriage license, etc.)
5.1-21	Provide ability to pre-populate record fields with scanned document
5.1-22	Provide ability to alert the Trusted Agent to mismatched data elements (i.e. name on document does not match demographic data previously captured for the applicant). Prevent operator from proceeding unless mismatched data elements resolved
5.1-24	Provide capability to rotate and zoom in to review scanned documents
5.1-25	Provide ability to archive electronically documents and badge records automatically on preset schedule following City data retention policies
5.1-26	Pro+A138:B143vide ability to institute City defined data retention policies on various levels (Company vs. Applicant level)
5.1.-27	Allow Trusted Agents 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 changes or deletes the note/comment
5.1-28	Allow the City to segregate duties based on Trusted Agent role through role-based access and management of identities and related access. Access rights can be instantaneously changed based on automated policies that govern user rights and related access across areas and zones (groups of areas)
5.1-29	Support a supervisory override function, with database documentation of the individual who overrode the transaction, when and reason for the override
5.1-30	Restrict Trusted Agent ability to change/delete comments to comments they entered
5.1-31	Provide a mechanism for identifying applicants and checking for undisclosed prior records such as badges previously/currently held that may have been unrecovered or were related to violations resulting in permanent suspension.
5.1-32	Support input of unlimited comments associated with persons, badges, and employers, each of which is automatically user/date/time stamped
5.1-33	Provide ability to make comments private based on user roles
5.11-34	Allow system workflows to be created and modified by the System Administrator
6.0 Computer Based Training	

6.1-1	Ability to configure business rules determining what CBT modules are required based on badge type, endorsements, time since last training, etc.
6.1-2	Track all CBT modules taken, date and pass/fail status - link those records with the appropriate badge and person
6.1-4	Integrate paperlessly with CBT to log pass/fail in badging system when applicant has successfully completed required CBT
6.1-5	Track required and delivered training for Trusted Agents and authorized signatories
6.1-6	Maintain training records for at least 180 days past the expiration of the person secure access privileges
6.1-7	Provide a drop down list by company that displays the DEN-approved City/Company trainer(s) configurable by the System Administrator.
6.1-8	Designate training classes as required for a given badge or credential type with applicable endorsements (icons) and the system shall deny the printing of a badge or credential for a person if the training requirements are not met
6.1-9	Provide ability to add/modify training and set expiration date of training
6.1-10	Provide capability to manually enter completion of non-CBT completed training
6.1-11	Provide ability for different user groups to add and amend training record for non CBT classes (e.g. DEN Operations instructors, driver training)
6.1-12	Provide capability to make certain training courses dependent on the other (for example Movement Area CBT training is dependent on Non-movement driver training)
6.1-13	Ability to track training events (security, non-movement & movement driving,) Badge status is conditional on successful training completion
6.1-14	Provide ability to identify whether a training event was conducted with translation assistance
7.0 Customs Seal	
7.1-1	Provide role for CBP user to manage CBP status. Investagate means to port CBP form into IDMS.
7.1-2	When a Customs seal is required, automatically create all appropriate workflow tasks
7.1-3	When a Customs seal is required, automatically require entry of all additional Customs seal application information
7.1-4	Incorporate business rules that ensure appropriate IDs are submitted with Customs seal application
7.1-5	Ability to generate all paper forms required for submission to CBP for Customs seals
7.1-6	Track submission, issuance and approval of Customs seal applications
7.1-7	On-line notification of suspension/termination of Customs seal
7.1-8	On-line fingerprint CHRC release form
7.1-9	On-line lost/stolen/damaged reporting
8.0 Enrollment	
8.1-1	Capture index finger minimum ANSI 378 biometrics using existing ATMEL FAP3010 or other recommended hardware with equal or greater capability
8.1-2	Provide biometric image quality score - solicit additional samples until acceptable quality is obtained
8.1-4	Capture compliant photograph of applicant using existing Canon camera or other recommended camera(s) with equal or greater capabilities and attach appropriate photo to appropriate record in the credentialing system; please indicate in comments the cameras you support

8.1-5	Option for Trusted Agent to re-capture badge photo if deemed necessary
8.1-6	Archive past photos from previous ID badges along with dates for which the photo was active on a badge, accessible through administration or log file view.
8.1-7	Record digital signature of enrollment data package from Trusted Agent, certifying data and establishing chain of trust
8.1-8	Print credential consistent with current DEN design
8.1-9	Provide ability to require new badge photo at user-defined intervals. Include a field that displays the date photo was taken. Prior photos should be archived and available for reference as needed
9.0 Access Control Management	
9.1-1	Mass editing - ability to add/remove individual doors to an entire company or department only via access profiles
9.1-2	Ability to associate Company/Department or Person with one or more MAXXNET (MAXXnet) access levels
9.1-3	Creation/management of business rule to default door matrix based on company/department/access level
9.1-4	Creation/management of business rules to prevent/allow assignment of ACS doors to badgeholders as appropriate
9.1-5	Ability to add individual doors to a badge in addition to the assigned door template(s)
9.1-6	No logical or general prohibitions on ability to utilize handheld devices to authenticate access credentials
9.1-7	Real time data transmission from IDMS to Access Control System for changes in badge activation status and door privileges
9.1-8	Track all changes made to badge access privileges
9.1-9	Ability to require approval from subset of trusted agent prior to processing requests for doors in addition to standard matrix
9.1-10	Provide capability to limit, which Access Codes can be used by a company or job title for specific badge types (prevents assignment of wrong Access Code)
9.1-11	Allow the System Administrator to define default access levels/clearance rights for each badge or credential type produced by company, department/division and access level (job title)
9.1-12	Ability to define CHRC and STA exemptions based on Company/Dept./Access Level
9.1-13	Support an unlimited number of access levels per badge or credential type
9.1-14	Aggregate PACS access definitions, providing a common assignment capability that is simultaneously compatible with multiple PACSs
9.1-15	Provide ability to assign individual access codes beyond defined/default Access Codes (temporary-auto expire capability or permanent)
9.1-16	Update PACS with badge holder data immediately. Update requests shall be queued for processing without delay
9.1-17	Have the capability of communicating with multiple physical access control systems simultaneously. May operate on "A" system while "B" is on old system
9.1-18	Integrate with CAISS (City legacy PACS, aka Maxxnet). Establish credentials in PACS from IDMS, exchange access definitions for assignment, synchronize badge information
9.1-19	Allow system to automatically grant and revoke access privileges in PACS, based on attribute changes, additions, deletions and trait expirations
9.1-20	Provide immediate notification if the IDMS connection to any PACS is lost

9.1-21	Support any permissions that the administrator sets. Example: User adds a new level of access permissions or adjusts an existing permission level
9.1-22	Provide ability to display doors/gates access that is associated with a specific Access Level

10.0 Badge Issue and Maintenance	
10.1-1	Ability to prepare and submit badge applications
10.1-2	Ability to issue multiple badges per employee - for different employers
10.1-3	Record unique card ID and/or card stock number and associate with badge record for use with ACS
10.1-4	Track available card stock at DEN
10.1-5	Show active badges at the top of the list on badge holder screen
10.1-6	Automatically purge badges not issued within a configurable number of days of the application date
10.1-7	Track badges revoked due to violations, link to violation record, and track violation type and date
10.1-8	Maintain history of badge holder and all badge transactions - including those spanning periods of non-continuous employment, employment by different companies, and employment at DEN
10.1-9	If previous badge was revoked due to a violation, require Security approval prior to issuing badge
10.1-10	Provide method for required forms to be read by the employee and accompany electronically captured signature
10.1-11	Capture electronic signature of applicant acknowledging badge issue and as otherwise required for payments and releases
10.1-12	Ability to provide applicant with hard copy or e-mailed version of electronically signed documents
10.1-13	Prevent issuance of replacement badges until existing badge is logged in the system as returned/lost/stolen/destroyed
10.1-14	Provide a warning to Trusted Agents if issuing a badge will exceed DEN's concession 25% Secured Area limit. Allow authorized users to override warning and issue badge. Track for audit purposes
10.1-15	Print badge for issuance to employee using Evolis Securion Badge Printers printers or other recommended printer with equal or greater capabilities.
10.1-16	Track lost/stolen/damaged badges including date reported, date deactivated
10.1-17	Ability to suspend a badge for a given date range and/or by time period (e.g., 1 week, 1 months, etc.)
10.1-18	Ability to specify a suspended badge to be automatically reinstated as of a certain date, or choose to require manual reinstatement
10.1-19	Archive/hide expired badge records to reduce screen clutter, allow access via interface when needed
10.1-20	Must be able to facilitate badge revalidation by specific populations, to include communication to Authorized Signatory, Badge tracking, and Badge termination.
10.1-21	Manage Badge Issuance (printing and inline encoding) of multi technology cards (smartcard and proximity) for different types of badge layouts defined for Secured, Sterile and Public Area access, including encoding iClass, MiFare, Desire, Dorado or Smart MX cards utilizing uninitialized media
10.1-22	Ensure the chip is encoded BEFORE printing a card. If encoding fails, functionality shall alert the operator and provide a method to quickly re-queue the encode/print request.

10.1-23	Scan and validate card encoding
10.1-24	Provide capability to create various types of cards. Examples include magnetic stripe, Smart Card, non-Smart Card badge, special event or special purposes credentials, such as a visitor badge or other generic badges that do not require access to PACS doors
10.1-25	Provide capability to limit badge types and icons by company/organization based on City-defined business rules (prevents issuance of the wrong badge type or endorsement Icon)
10.1-26	Support badge endorsements (icons) for Customs (FIS), Non-Movement Area Driver, Movement Area Driver and others as needed
10.1-27	Provide capability of reprinting a badge with the same badge number based on permission level
10.1-28	Be capable of changing the status of a company, department/division, or job title (business units). This shall cause all active badges assigned to that business unit to be placed into an "Invalid" status. That status change shall be sent to the PACS for all cards affected
10.1-29	Cause reactivation of a business unit and automatically reinstate all badges in that particular group of "Invalid" cards back to an active status in the IDMS database and the PACS
10.1-30	Allow an operator to make changes to multiple badges based on the cardholder's company, department/division, or job title
10.1-31	Allow modification to Company/Dept./Access Level (e.g. company name change) resulting in badge update upon renewal
10.1-32	Allow corporate name changes while retaining relation to the former corporate name, using internal generated Employer ID to maintain all relationship.
10.1-34	Provide ability to limit status changes based on business rules. For example, the system shall allow the System Administrator to configure badge statuses so that once a badge is stolen it can never be reactivated again
10.1-35	Provide ability to identify and archive/purge documents that no longer need to be retained as defined by the City
10.1-36	Provide mechanism to capture "signature" upon badge being released to a badge holder (signature pad or biometric authentication)
10.1-37	Provide the ability to issue a badge for each company the individual is employed and segregate privileges to individual badge. For example a Customs Seal or driver authorization icon would only be allowed on the company badge approved for these roles
10.1-38	Automatically invalidate renewed badge that does not have an updated CHRC at 46 days
10.1-39	Provide ability to pre-print badge when CHRC/STA are cleared or other wise approved, while applicant is undergoing training
11.0 Payments	
11.1-1	Ability to configure fee types and payment methods
11.1-2	Automate invoicing process
11.1-4	Prevent invoicing of any fees that have already been paid
11.1-5	Manage payments via manual updates of vendor solution
11.1-7	Ability to configure fee amount and payment method (invoice, cash, waived) by company and fee type
11.1-8	Vendor solution will record payments outstanding for, at a minimum, badge applications, fingerprints, lost badges, and violations
11.1-9	Track payer, date, amount, purpose and payment method

11.1-10	Link all payables to appropriate badge, permit, violation, person and/or company record
11.1-11	Vendor solution is able to accept manual entry of Cash, Credit Card, of Check payments made to POS and reflect that payment for associated badge, permit, violation, person and/or company records
11.1-12	Ability to override fees with reason code
11.1-13	Ability to override default "invoice" payment method to accept alternate payments
11.1-14	Record payment status changes (i.e., returned check and chargeback processing)
11.1-15	Enforce unique IDs across any elements to which payments might be linked to ensure referential integrity
11.1-16	Ability to configure receipt template with formatting, logo, etc. as appropriate to issuing location
11.1-17	Print receipt including item type, item fee, payment method - with ability to endorse the payment
11.1-18	Digitally track changes in badge and vetting dispositions, automatically generating invoice detail to be integrated with (or export to) financial software used by City Accounting.
11.1-19	Provide the capability to create, manage and track the fees/charges associated with badges, background investigations, and misc. items sold by the Security Badging Office
11.1-20	Allow for payment methods to be defined at individual company levels. For example, 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 cash or credit card at the time the service is rendered
11.1-21	Allow for credit card transactions separate from the IDMS. IDMS shall NOT process, transmit or store credit card data
11.1-22	Be capable of printing receipts to a standard printer supplied by the City, for each transaction that occurs
11.1-23	Be capable of printing reports that show all of the financial transactions related to a company over any period of time (a day, a week, a month, year-to-date, or since system inception)
11.1-24	Support user-defined badge billing rate classes by company and badge type, taking into account CHRC exemptions, external adjudication, and federal employee allowances
11.1-25	Have the ability to set customer billing rates for the following:
	a. New badges by type
	b. Differentiate new badge pricing for (1) individuals who are not fingerprinted by DEN, (2) individuals who are fingerprinted, but not adjudicated by DEN and (3) individuals who are fingerprinted by DEN and adjudicated by DEN
	c. Badge renewals by type
	d. CHRC pricing for renewal CHRCs
	e. Lost/Stolen replacements
	f. Badge reprinting
	h. Override for manager/supervisor to waive billing
	i. Other charges as required
	j. Provide ability to send receipt for payment direct to Authorized Signatory via email or to the AS Portal. (See Authorized Signatory Portal requirements)
12.0 Alerting	
12.1-1	Ability for Trusted Agents to log posted security and other advisories and display them at login

12.1-2	Ability for Trusted Agents to log messages to authorized signatories (e.g., reminder of bulk IDMS renewals)
12.1-3	Configurable alerts/emails to Trusted Agents, DEN, CBP, authorized signatories, applicants and other groups based on application statuses, pending expirations, badge returns, badge terminations, lost/stolen badges, overdue audits, or other events
12.1-4	Configurable notifications by Authorized Signatory: frequency (e.g., weekly, daily), status (awaiting FP, awaiting interview, awaiting pickup)
12.1-5	Management of undelivered e-mail via report, up to the point where email failed and did not reach the mail server
12.1-6	Provide notification to specified Security Badging Office user when the Communications Center changes the status of a badge
12.1-17	Provide notification to the Authorized Signatory when a badge status changes within the Authorized Signatory's company
12.1-18	Provide the System Administrator with notification template options and ability to modify templates
12.1-19	Automatically notify Authorized Signatories via email when their employee's background investigation status changes
12.1-20	Allow Authorized Signatories to select which notifications to receive from the IDMS. Allow the City to require certain emails that can't be amended by the Authorized Signatories
12.1-21	Email returned badge receipts to Authorized Signatories
12.1-22	Send notice to Authorized Signatory when a new applicant receives a badge and/or display in dashboard
12.1-23	Send notice to Authorized Signatory when a badge is renewed or otherwise changed
12.1-24	Send notice to Authorized Signatory when an applicant fails any training in the IDMS
12.1-25	Notification to Authorized Signatory when a CBP seal has been approved
12.1-26	Notification to Authorized Signatory 60 days before CBP seal expiration
12.1-27	Notification to Authorized Signatory 30 days prior to badge expiration
12.1-28	Notification to Authorized Signatory 30 days prior to training or documentation expiration
12.1-29	Provide a notification to the Authorized Signatory with new cipher code issuance
12.1-30	Provide notification to CBP when seal added/deleted from badge
12.1-31	Provide notification of the approved access privilege change to Authorized Signatory
13.0 Audits	
13.1-1	Automated annual 100% / bi-annual 10% badge auditing process
13.1-2	Ability to define badge statuses to include in audit - usually active and suspended
13.1-3	Ability to define business rules for audits - e.g., audit recipient based on contractor status, badge status to include in audits for various badge types
13.1-4	Ability to define fields to include in audit report - e.g., name, badge #, status, company, badge used in last 30 days, etc…)
13.1-5	Ability to require submission of proof of employment records in support of audit
13.1-6	Ability to select badges flagged by Authorized Signatories as terminated or on leave of absence for status update
13.1-7	Allow bulk suspension of companies who do not respond to audits by the deadline, and the ability to bulk reactivate once responded,

13.1-8	Audit lost/unaccounted for badge percentage (5%). This includes generating a report for lost badges and the percentage of Stop Listed badges against current active badges. The IDMS shall allow for this to be done for the entire cardholder population, for a specific company, or for a specific type of company (tenant, air carrier, City, contractor, vendor, etc.) or specific badge type
13.1-9	Provide automated Annual 100% audit of all active badges
13.1-10	Provide capability to schedule automated 10% audit of all active badges random checks every six (6) months
13.1-11	Provide automated Annual key audit electronically
13.1-12	Provide capability to automate the Tenant 25 % SIDA badge limitation audit
13.1-13	Provide a report for all concession tenants to determine the number of cardholders in this category with SIDA access. The number shall also be provided as a percentage of NON-SIDA badges in the same category
13.1-14	Provide capability for System Administrator to set up additional audits for badges, vehicle permits, keys, etc.
13.1-15	Provide an audit log that shows all updates made to badge records, company information and all other IDMS data entry components. Updates shall include what change was made, who made the change and when the change was made
13.1-16	Allow Authorized Signatories to audit companies they sponsor, but not have full access to individual badge information
13.1-17	Allow for the audit results to be viewed/sorted by exception based on changes made by the Authorized Signatories
14.0 Badge Expiration and Deactivation	
14.1-1	Default information from prior Temporary Visitor Passes
14.1-2	Ability to configure business rules ensuring that badge expiration dates to not exceed critical date drivers such as ID expiration, contract expiration, scheduled company termination, work authorization.
14.1-3	Manage badge revocations based on associated record statuses (e.g., contract expires, company retired, etc.)
14.1-4	Ability to automatically deactivate badge if last date worked or termination date is in the past
14.1-5	Automatically deactivate badge on the badge expiration date
14.1-6	Investigate with DEN the ability to to deactivate badges after configurable number of days of inactivity
14.1-7	Management of 30-day deactivation rule around badge status.
15.0 Temporary Visitor Passes	
15.1-2	Require that applicant pass DNI or Watch List prior to be issued a Temporary Visitor Passes
15.1-3	Ensure all Temporary Visitor Passes have an expiration date
15.1-4	Temporary visitor passes will clearly display the valid date range
15.1-5	Ability to generate Temporary Visitor Passes with photos
15.1-6	Prevent issuance of Temporary Visitor Passes to individuals with active Secured Area badges or who have exceeded the allowable Temporary Visitor Passes access as determined by DEN SOPs
15.1-7	Allow enrollment of visitors and comparison of biographic visitor information to the TSA Watch and No Fly Lists. DEN uses visitor management system to allow access to the SBO so must be able to compare to TSA Watch and No Fly lists.

15.1-8	Allow a visitor badge to be printed with an expiration date on regular badge stock (no DEN badge number assigned), or a simple printer with paper badges
15.1-9	Clearly articulate how visitor badges are issued outside regular badge numbers
15.1-10	Track number of times a specific individual is issued a Visitor Badge and send notification to designated Trusted Agent when a specific number is reached
15.1-11	Require an approver or escort be attached to the record. System shall allow additional escort to be added if the escort changes in situations where an escort is required
15.1-12	Print Visitor badges on other types of printers and not using HID badge stock if desired by the City
15.1-13	Provide a flat rate cost for this module not based on number of identities
16.0 Vehicle Permits	
16.1-1	On-line submittal and processing of vehicle permits via Authorized Signatory portal
16.1-2	Track all information currently tracked in Permit
16.1-3	Ability to link scanned/photographed documents to vehicle permit and Temporary Vehicle Tags applications
16.1-4	Prevent issuance of vehicle permits for companies who cannot supply proof of minimum insurance
16.1-5	Ability for contract security and DEN Communication Center personnel to access permit expiration date to verify permits are active before allowing entry
16.1-6	Ability to generate annual/semi annual renewal reminders to permit holding companies
16.1-7	On-line submittal and processing of Temporary Vehicle Tags via Authorized Signatory Portal
17.0 Safety and Security Violations	
17.1-1	Has portal to allow entry of violation response information by Authorized Signatory
17.1-2	Track all information current tracked in safety and security violations database
17.1-3	Track lost badge, safety and security violations; violation types; and severity
17.1-4	Link violation records to badge, badge holder and/or sponsoring company
17.1-5	Ability to configure and manage a variety of safety and security violations with a variety of fees, consequences and timeframes
17.1-6	Ability to send notifications to violating company and/or individual
17.1-7	Ability to reduce or override violation fees and/or consequences with a reason code
17.1-8	Ability to collect payment of cash, credit card or money order and credit amount of citation fee
17.1-9	Track payment of badge violations - any dollar amount, loss of badge
17.1-10	Ability to process payments in point of sale module, have payment reflected on violation record, and automatically update violation status as appropriate
17.1-11	Ability to record a change in the disposition of a citation and associated charges
17.1-12	Ability to invoice company bi-annually for outstanding violations
17.1-13	Ability to list all badges and access information for an employee receiving a violation
17.1-14	If a badged employee has exceeded the allowed number or severity of violations, ability to deactivate all associated badges unless one or all badge deactivations overridden by an Security supervisor
17.1-15	Track hearing results for all steps in the violation hearings process
17.1-16	Allow users with appropriate permissions to add new types of violations
17.1-17	Allow an unlimited number of violation types to be added while insuring reference to original violation type
17.1-18	Manage a central record of employee's violations at DEN
17.1-19	Record and track DEN violations in each identity profile, safety and security violations, etc

17.1-20	Record and track repeated violations (including driving violations), which may warrant re-training of the employee
17.1-21	Allow City to determine if a badge should be suspended, but should not occur automatically unless defined by the System Administrator
17.1-22	Track penalties relating to a suspension
17.1-23	Track fulfillment of any necessary corrective actions relating to penalty, suspension, training, etc.
17.1-24	Provide ability to enforce business rules to manage employee violations, suspensions, training, etc.
17.1-25	Provide ability to search existing or historical records of violations by multiple fields such as name, company, badge number, ticket number, plate number, etc.
17.1-26	Provide ability to define and limit users access. Data entry, read-only, etc.
17.1-27	Send violation notices out via email automatically to the Authorized Signatory
18.0 Company Management	
18.1-1	Manage companies and departments including contractor/subcontractor relationship, company name, alias, start date, end date, sponsoring company, etc.
18.1-2	Allow bulk deactivation of contracts, sub-contracts, subcontractor companies, and badges if the last remaining parent company or primary contract is to be deactivated
18.1-3	Ability to allow authorized signatories to create/discontinue sponsorships for companies
18.1-4	Require on-line request for new company including reason for access, area of access, primary and secondary contact information
18.1-5	Require Trusted Agent approval for all new and discontinued companies
18.1-6	Vendor to train DEN Trusted Agents to operationally prevent and manage Company record duplicates.
18.1-7	Ability for Trusted Agent to merge multiple company records to correct duplicates or accommodate company mergers
18.1-8	Ability to revise company name, track prior company names with effective dates, and have company name queries check current and previous name(s)
18.1-9	Ability to assign billing account number to each new company and/or division (as defined by business rules) to ensure unique link to invoices and payments
18.1-10	Restrict company types to a validated, configurable lookup list
18.1-11	Track both Corporate Name (e.g., franchise or parent company name) and Doing Business As (customer facing name e.g., Starbucks)
18.1-12	Track both invoice address and local address
18.1-13	Ability to prevent deactivation of companies or contracts having active contracts, sub-contracts, subcontractor companies, or badged employees
18.1-14	Prevent badge expiration dates that are later than company/contract expiration dates. If contract expiration dates are moved up, prompt trusted agent to change expiration dates of associated badges.
18.1-15	Require proof of insurance if company employees need to operate vehicles or motorized equipment in the movement or non-movement areas - including key insurance information, expiration date, and scanned copy of insurance certificate
18.1-16	Allow scanned documents or digital photos of documents to be linked to request for new and/or discontinued company
18.1-17	Prevent setting company status to "Active" until all required forms and approvals have been submitted

18.1-18	Provide option to allow companies to update their information via the Authorized Signatory portal
18.1-19	Ability to bulk manage perimter gate access privileges for drivers of companies whose insurance has expired
18.1-20	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 of time that exceeds parameters set by the System Administrator. A supervisor must be able to override this function if it is not applicable to the company
18.1-21	Store the company type. This shall be a drop down list which would include entries such as "Contractor," "Tenant", "Concession Tenant" (TSA 25% Rule tracking), "City," "Air Carrier," "Vendor," "Federal Government," etc. The IDMS shall allow the System Administrator privileges to add new company types
18.1-22	Store multiple addresses, phone numbers and contacts for each company
18.1-23	Provide capability to link all vendor companies to sponsoring companies. Sponsoring companies require company name, Authorized Signatory contact info and number of active badges by badge type
19.0 Authorized Signatory Management	
19.1-1	Ability for Trusted Agent to reinstate Authorized Signatory privileges after badge and training are made current
19.1-2	Require Authorized Signatories to have an active Secured, Sterile or Public Area badge.
19.1-3	Require Authorized Signatories to indicate in their on-line badge application that they are Authorized Signatories - default from existing Authorized Signatory list. Must be approved by another Authorized Signatory unless there is only one.
19.1-4	Require recurrent Authorized Signatory training and track training expiration dates in the badging system
19.1-5	Ability to deliver on-line Authorized Signatory Training via the ASP and track dates of successful completion
19.1-6	Ability to associate an Authorized Signatory with more than one company such that employees associated with that company are automatically associated with the appropriate Authorized Signatory(ies)
19.1-7	Track authorized signatories for companies along with e-mail address, active service dates, and current expiration date
19.1-8	Upon approval as an Authorized Signatory, issue a user ID and password to allow access to Authorized Signatory portal
19.1-9	Ability for Authorized Signatory to reset their own password after answering security questions to verify their identity
19.1-10	Ability for an Authorized Signatory to request removal of signatory privileges for signatories within their own company
19.1-11	Ability for Trusted Agents to approve and execute removal of Authorized Signatory privileges
19.1-12	Ability for Trusted Agents to control Authorized Signatory access privileges (badge applications, vehicle permits, etc.)
19.1-13	Automatic suspension of Authorized Signatory privileges if last active badge or authorized signatory training expires
20.0 Badge Design	
20.1-1	Ability to easily configure badge design (fonts, sizes, locations of elements, artwork, images, colors, orientation, etc.) per badge type and support double sided badge printing
20.1-2	Ability to manage badge designs via intuitive names reflecting badge type, background, etc.
20.1-3	Ability to add different custom seals to the badge design with associated business rules

20.1-4	Maintain badge design history (e.g. past card designs and effective dates)
21.0 Scheduling	
21.1-1	On-line scheduling for CBT, FP, Authorized Signatory Training and other appointments
21.1-2	Ability to configure available hours and capacity and prevent users from scheduling beyond available capacity
22.0 Form Design/Revision	
22.1-1	Ability for designated system administrators to add user-defined fields and constraints to tables and screens without requiring code modifications or programming
22.1-2	Ability to rearrange fields on data entry forms
22.1-3	Ensure that all user-defined fields are available for query, report and dashboard operations
23.0 Data Quality Assurance	
23.1-1	Includes preconfigured business rules necessary to enforce compliance with TSA 49 CFR Part 1542 all other applicable regulatory requirements
23.1-2	Ability to define business rules to drive visible fields, required fields, single field validation parameters (e.g., min, max, lookup), and composite field validation parameters (e.g., if applicant requires driving privileges, valid driver's license is required)
23.1-3	Business rule maintenance - rules and sub rules, start/end dates for rules, audit trail tracking
23.1-4	Ability to define tasks and task statuses; establish workflows and task/status dependencies (e.g., terminated may not be reinstated) based on badge type, etc.; and specify who has privileges to create/update each task
23.1-5	Data validation upon entry rather than when saving the record
23.1-6	Assign each applicant a unique DEN Airport ID to identify that person during their career at DEN and act as the link to badge records. This ID may not be based on the persons' name, SSN or alien ID
23.1-7	If a person has not previously worked at DEN, assign a unique person ID at the time the application is submitted
23.1-8	If a person was previously or is currently employed at DEN, link any new applications and badges to the existing unique person ID
23.1-9	Ability to prevent duplicate badge holders in system by defining set of key fields that, if a subset match an existing record, the user will be prompted to select from potential matching person records or initiate a new person record
23.1-10	Ability for designated system administrators to implement changes to business rules and field validations without code modifications or programming
23.1-11	Limit free form text fields for use only when necessary
23.1-12	Provide code tables for any fields that can be codified, require validation of field contents against lookup table
23.1-13	Codes sort alphanumerically
23.1-14	Ability to deactivate lookup table codes (by effective data range) so that they do not appear on pull-down lists but are available for reporting as appropriate
23.1-15	Business rule governing application questions - i.e., can only ask Air Carrier employees if they were arrested/convicted of a disqualifying felony, can ask non-Air Carrier employees if they were arrested/convicted of ANY felony. Questions differentiated by company type.
23.1-16	Automatically determine if person was previously employed at DEN - auto-populate appropriate application fields
23.1-17	Ability to require that the Airport Security Coordinator (ASC) approve badge applications
23.1-18	Support the creation of new business policies/rules regarding how and when a badge or credential shall be issued without any modifications to code

	24.0 Data Quality Control
24.1-1	Produce reports highlighting any records violating referential integrity constraints (e.g. invalid codes, orphan records)
24.1-2	Ability for Trusted Agent to merge multiple person records to correct duplicates
	25.0 Document Management
25.1-1	Ability to scan/photograph documents (IDs, letters, releases, etc.), and easily link to badge, person, violation, permit and/or company record
25.1-2	Require that all scanned documents be assigned a document type and linked to at least one record in the database
25.1-3	Require entry of key fields from certain document types (e.g., IDs)
25.1-4	Ability to link and an unlimited number of documents to a record
25.1-5	Manage scanned documents to ensure that the correct documents get to the correct third party (DEN, CBP, etc.) based on document type and associated record
25.1-6	Ability to scan later version of a particular ID and not overwrite the previous version (e.g., new license after old one expires)
25.1-7	Ability to search for a record and securely transmit that records with all associated scanned documents and data to an approved recipient
25.1-8	Provide for applicant photo capture, cropping, and digital enhancing from within the client application
25.1-9	Provide ability to for Security Badging Offices and Authorized Signatory 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
25.1-10	Provide ability to scan and store documents and mark private based on user roles. Restricts viewing by unauthorized users
	26.0 Query and Reporting
26.1-1	Inclusion/recreation of existing BadgEze, safety and security violation, POS and Crystal queries and reports deemed necessary by Project Team
26.1-2	Badge retrieval by scanning badge rather than typing in badge number
26.1-3	Ad-hoc query and reporting with user friendly query/report builder including customizable report formatting including element placement, font, grouping, aggregation, header/footer, titles, etc.
26.1-4	Intuitively organized standard query/report library interface allowing for robust searching and with the ability to add ad-hoc queries and reports
26.1-5	Ability to develop multi-table queries and filters
26.1-6	Metrics - throughput (e.g., badge issued, fingerprints taken, etc.), status wait times, and data QC; for a user-defined date range - with ability to group/aggregate by Security personnel
26.1-7	Ability to query by, sort by, group by and report on user-defined fields
26.1-8	Ability to query records using partial information (wildcards)
26.1-9	Ability to search both name and alias using a single name search
26.1-10	TSA-required reports including new/amended reports as required by evolving TSA regulations and directives
26.1-11	Provide "badge viewer" page with limited field availability for City law enforcement review of badge holders of any status . (basic demographics, badge detail and photo)
26.1-13	Name searches must be broad/smart enough to account for hyphens, apostrophes, multiple last names, etc.
26.1-14	Metrics - personnel quality reports - voided billing items, voided/misprinted cards or other corrections required to Security staff activity

26.1-15	Ability to further refine searches by specifying filters on additional fields
26.1-16	Ability to utilize Boolean logic (e.g., And, Or), mathematical (greater than, equal to, between), and text comparison (e.g., contains, starts with, ends with) functions for record searches and report building
26.1-17	Ability to name and save a query for future querying and/or as the basis for reports
26.1-18	Ability to view query and report results on screen and sort based on one or more columns by clicking on column header
26.1-19	Ability to scroll through results to select the desired record
26.1-20	Ability to parameterize reports and have user enter parameter (e.g., start date, badge status, badge type, etc.) at run time
26.1-21	Inclusion of query/report logic, including user-entered parameters, in query/report header
26.1-22	Ability to create and schedule automatically generated reports (e.g., weekly, monthly), filter report content based on intended audience, and automatically e-mail results to intended audience
26.1-23	Ability to generate letters and forms automatically based on trigger events(s) and/or by applying the results of a query for bulk generation
26.1-24	Ability to create template letter (e.g.,. reminder letters) and forms (e.g., CBP forms) using system data
26.1-25	Ability to define report templates to drive headers, footers, fonts, logos and other formatting
26.1-26	Ability to export all reports and query results to standard formats such as CSV, Excel, PDF, and XML
26.1-27	Allow Trusted Agents to see information for all badge holders in reports and provide option to filter and/or group by one or more companies
26.1-28	Ability to filter all reports by company
26.1-29	Limit reports run by Authorized Signatories to information on only the badge holders assigned to that Signatory
26.1-30	Provide pre-defined reports, in a variety of formats that allow the user to select or specify the grouping and/or sorting criteria
	a· Active Badge Report (Company Group)
	b· Driver Endorsement Report
	c· Audit Report
	d· Background Status Report
	e· Badge Color
	f· Badge Expiration By Company & Date
	g· Badge Expiration By Date
	h· Badges Issued on a Day (delineating between new and renewals)
	i· Cardholder Record
	j· Company Count Total Badges
	k· User Activity Report
	l· Terminated Over 180 Days
	m· Physical access history granted to an individual (In all integrated PACS)
	n· Pending Approvals
	o· Shows the status of various personnel and physical access activities
	p· Operator Comments
	q· Listing of Companies
	r· Listing of Companies Sorted by Code

		s· Master Badge List group by badge
		t· Master Key Active List
		u· Master Key Active List Grouped by Company
		v· Mailing Labels to Companies of Expired Badges
		w· New Badges Created on a Date
		x· Authorized Signatory Labels
		y· Endorsements
		z· Returned Badges in a Date Range
		aa· Revalidation List
		bb· Badges by classification
		cc· Status Report
		dd· Stop List
		ee· Violations Report
		ff· Cardholder Search
		gg· Authorized Signatories by Company
		hh· Approvals and Rejections: Shows requests for which approval activity has occurred
		ii· IDMS Audit Events: Shows audit records of user actions and an audit of all system actions
		jj· Six Pack (Law enforcement lineup)
		kk· Active Customs Seals
		ll· Active Customs Seal expiration dates by badge holder
		mm· Ad Hoc report to see expiration dates of Authorized Signatories
		nn· Badge holders by each type of endorsement
26.1-31		Easily generate ad-hoc reports or queries without specialized skills (most easily via filtering, sorting, grouping)
26.1-32		Allow reports to be exportable at a minimum into .csv, .pdf and .xlsx formats
26.1-33		Provide ability for a system user to create new reports as well as modify existing reports
26.1-34		Provide an intuitively organized library of standard reports, which may be configured at run time via the use of parameters (e.g., date ranges). Reports must limit information based on user privileges (e.g., Authorized Signatories may only see information pertaining to the badge holders assigned to them). Standard reports must support at a minimum: badge status monitoring, financial reporting, data quality control, audit trail reporting, and regulatory compliance. Vendor shall generate the following pre-defined reports for the initial standard reports library:
26.1-35		Provision to ensure Authorized Signatory records are maintained for 24 months after invalidation of Authorized Signatory privileges
27.0 Dashboarding		
27.1-1		Ability for Trusted Agents to see dashboard contents for all badge holders or limit by company
27.1-2		Ability to click on top level graphic (count, %, odometer showing status with regard to threshold, etc.) and drill down for detailed report
27.1-3		Automatically filter dashboard contents by badge holders assigned to logged in Authorized Signatory
27.1-4		Dashboards for various stakeholders - applications awaiting their action
27.1-5		Authorized Signatory/Trusted Agent - applications awaiting CHRC and/or STA
27.1-6		Trusted Agent - status of 5% unrecovered badges by badge type (Sterile Area Only, Secured and Sterile, etc…)
27.1-7		Authorized Signatory/Trusted Agent - awaiting badge pick up

27.1-8	Authorized Signatory/Trusted Agent - awaiting CBP interview
27.1-9	Authorized Signatory/Trusted Agent - awaiting CBT completion
27.1-10	Authorized Signatory/Trusted Agent - awaiting Customs seal
27.1-11	Authorized Signatory/Trusted Agent - awaiting deactivation or suspension by Trusted Agent
27.1-12	Authorized Signatory/Trusted Agent - suspended badges
27.1-13	Authorized Signatory/Trusted Agent - awaiting fingerprinting
27.1-14	Authorized Signatory/Trusted Agent - awaiting initial CBP visit (new employees only)
27.1-15	Authorized Signatory/Trusted Agent - awaiting DEN CHRC adjudication
27.1-16	Authorized Signatory/Trusted Agent - badges deactivated but not yet returned to Trusted Agent
27.1-17	Authorized Signatory/Trusted Agent - lost badges
27.1-18	Authorized Signatory/Trusted Agent - pending expirations
27.1-19	Authorized Signatory/Trusted Agent - status of 25% rule by company
27.1-20	Provide on dashboard those CHRC results that have not been returned in 40 days. (To meet TSA 45-day requirement)
27.1-21	Have different page/module colors to facilitate quick action reference
27.1-22	Easily indicate active badges versus returned and invalid badges
27.1-23	Provide indication of invalid or non conforming record entries
27.1-24	Indicate expired documents when record is opened by Authorized Signatory or Trusted Agents
28.0 Paperless Hardware/Software Integration	
28.1-1	ATMEL FAP3010 fingerprinting system (Dorado card encoder) - including all necessary application information
28.1-2	Crossmatch Guardian Fingerprint Scanner, not to include any costs from Crossmatch for software/personnel for their responsibilities in this integration.
28.1-3	DAC (Telos ID) - for execution of STAs, CHRCs and (if possible) CBP background checks; bi-directional, real time and bundled with demographic data, not to include any costs from Telos for software/personnel for their responsibilities in this integration.
28.1-4	DAC (Telos ID)- to reconcile active badges in IDMS with active badges managed by Telos ID
28.1-5	DAC (Telos ID)- submit required monthly upload of all active/revoked badges
28.1-6	Customs and Border Protection - grant role for CBP to manually manage their part of the Customs Seal Application
28.1-7	Credential verification system- to import information extracted from breeder documents
28.1-9	Electronic signature capture
28.1-10	Compatible badge photo cameras
28.1-11	Evolis Securion badge printers (or other recommended printer with equal or greater capabilities)
28.1-12	Ability to to capture MAXXNET biometric enrollment and transmit to IDMS
28.1-14	AAAE IET CBT - to update badge application record with successfully completed training requirements
29.0 Regulatory and Standards Compliance	
29.1-1	Complies with TSA 49 CFR Part 1542
29.1-2	TSA Security Directive 1542-04-08K, with the understanding that vendor solution is not certified compliant by TSA, and configuration must be evaluated by DEN for compliance with its FSD/TSA

30.0 Platform	
30.1-1	SQLServer 2008 SP2 or later database
30.1-2	Windows Server 2008 R2 or later
30.1-3	Windows 7 workstations
30.1-4	McAfee 8.5 antivirus or later on all servers and workstations
30.1-5	McAfee Data Loss Prevention (DLP) and McAfee Host-Intrusion Protection (HIPS) on all workstations
30.1-6	Architecturally accomodate primary vendor solution database use by DEN and City users only.
30.1-7	Architecturally accomodate secondary vendor solution database which will be public-facing, populated with limited-datasets by the primary vendor solution database.
30.1-8	All software and licenses that vendor requires to implement and run the vendor's system on City provided hardware. DEN will secure licenses for all DEN-contracted vendors such as TelosID, Crossmatch, etc..
30.1-9	Provide an application architecture that is based on industry standard practices and non-proprietary tools
30.1-10	Provide a non-Security Sensitive description of database and network architecture that supports their application in a currently live environment, including storage, computing, and throughput requirements
30.1-11	Passport/ID read/authentication full page reader - TBD
30.1-12	High-speed, duplex, multi-page document scanner - TBD
30.1-13	High-speed flatbed scanner - TBD
30.1-14	Backlit signature pad - TBD. Vendor shall provide ability to store signatures of the Authorizing Signatories from each company. Signature must be captured via the signature pad or via scanning the Authorizing Signatory signature(s) from a paper document using a document scanner. Must be able to store applicant's signature with applicant's record
30.1-15	Reference Biometric Enrollment Reader - Integrate reference biometric capture to the current Cyber Country biometric reader selected for the PACS to limit the number of biometric enrollments required
30.1-16	Provide a software driver support for camera and encoding badge printer and biometric reader peripherals to integrate with vendor solution
30.1-17	DEN will provide required storage, backup, and network hardware
30.1-18	Provide a standardized API for use by City developers to integrate or interface third-party systems and custom solutions
30.1-19	Integrate with a TSA certified DAC (the current City DAC is Telos) for processing of STA's and CHRC's. Automate submission of applicant demographics and biometrics to the DAC and return of vetted results directly into individual records
30.1-20	Biographical information sent to Telos must be able to indicate exempt status for FAA/TSA and others so Trusted Agent doesn't have to enter it separately
30.1-21	Integrate with Livescan Type 14 system (Cross Match) used for capture of applicant fingerprints during CHRC enrollment. Exchange applicant demographic and EFT submission status. Vendor is not laible for cost of Crossmathc licenses.
30.1-22	Integrate with IDS RFID Vehicle Permit system
30.1-23	Integrate with the CBP e-Badge program when it is available, at additional chargeges from vendor.
30.1-24	Solution must be able to differentiate between records that require STAs and those that are exempt

30.1-25	Provide compatibility and integration with the computer based training platforms AAAE's Interactive Employee Training (IET)
30.1-26	List all certified integrations with Enterprise Resource Planning / Financial systems (e.g. Peoplesoft, AMS Advantage, SAP, etc.)
30.1-27	Provide a flexible and extensible design to incorporate additional features or modules
30.1-28	Provide a proposed logical architecture delineating the recommended separation of solution components by network segment (e.g. DMZ, internal employee LAN, segmented server LAN, etc.) based on industry expertise, SSI requirements, and product logical architecture
30.1-19	Coordinate IP addressing and routing with City network communications staff
30.1-30	Run system in a VMware virtual environment
31.0 Security	
31.1-1	Integration between IDMS on secure ACS network, including authorized signatory portal, CBT, etc., via secure DEN-approved protocol
31.1-2	Support of secure client environment to house badging and ACS - zero to limited internet access, USB ports, discs, etc.
31.1-3	Encrypt all data being transferred between the secure badging/ACS network and external data sources/repositories
31.1-4	E-mailing of reports, not to contain containing SSI or PII must information
31.1-5	Need 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
31.1-6	Maintain records in an encrypted format
31.1-7	Require unique ID for all users with access to badging system and/or authorized signatory portal
31.1-8	Interface to manage all secure user logins (trusted agents, authorized signatories, etc.)
31.1-9	Disallow use of vendor supplied password defaults for system passwords
31.1-9	Prevent passwords that are derivatives of the username
31.1-10	Enforce DEN password and account lockout policy
31.1-11	Investigate multi-part authentication methods for Trusted Agents.
31.1-12	Require user to reset password after a set period (configurable)
31.1-13	Times out after an administrator-configured period of idle time; saves work prior to time-out
31.1-14	Ability to establish multiple user groups with varying IDMS access limits and to map all system users to user groups with only the system permissions necessary to accomplish their jobs
31.1-15	Log unauthorized or invalid attempts to access privileged services or functions
31.1-16	Limit to system administrators the ability to change user privileges
31.1-17	Allow system administrators to set user roles and privileges governing access to data, functions and modules
31.1-19	Mask display of PII or sensitive data fields after initial input unless user has privileges to and has selected the option to modify them
31.1-20	Limit browser-based modules to accept only HTTPS connections for authentication purposes
31.1-21	Automatic audit trail logging of all configuration updates made by any user - business rules, validation, required fields, lookup tables, etc.
31.1-22	Automatic audit trail logging for all queries and reports run - query/report name or SQL code, date/time, user
31.1-23	Automatic audit trail logging data viewed by any user - record or file, date/time, user

31.1-24	Automatic audit trail logging data updated by any user - table, field, old value, new value, user ID, date/time
31.1-25	Ability to control how to share and/or segregate employee, badge and code table data for DEN
31.1-26	Ensure that no single Trusted Agent can perform all tasks in a given badging operation
31.1-27	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).
31.1-28	Provide method(s) for the System Administrator to view and maintain user profiles such as: add new users, modify and delete user profiles
31.1-29	Have the ability to encrypt sensitive and personally identifiable information (PII) at rest and in transit
31.1-30	Provide and describe mechanisms to incorporate 2-factor authentication for the Authorizing Signatory Portal, to include, without limitation, authentication codes via text or email
31.1-31	Provide an a detailed list of all authentication capabilities for application access and Authorizing Signatory Portals
31.1-32	System provides automated means for user password resets with authentication
31.1-33	Provide vendor cyber security program information (number of personnel, staffed by a dedicated team, how long established), as it relates to the IDMS proposal
31.1-34	Provide detail in how cybersecurity is part of the product development process, including new vulnerability notification procedure
31.1-25	Provide details for any penetration testing, proprietary or 3rd-party, conducted by the vendor
31.1-26	Provide details of a data breach Recovery Plan, including liability matrix
31.1-27	Manage concurrent user sessions on a single shared credentialing workstation while accurately identifying the user making the change for audit purposes
31.1-28	Employ record locking mechanisms to ensure data integrity
32.0 Performance	
32.1-1	IDMS designated as a critical business system with 24/7 availability and appropriate redundancy for immediate recovery
32.1-2	Collaborate with DEN to IT to architect and implement for an uptime goal of 99.9%
32.1-3	Collaborate with DEN to IT to architect and implement for a sub 3-second reponse time to return any individual screen
32.1-4	Ability to store an unlimited number of scanned documents so long as there is sufficient disk space
32.1-5	Archive badge records and tasks after a pre-configured period of time. Exclude from standard queries but allow for report-only retrieval when necessary
32.1-6	Be available at all times to business operations. Provide details of U.S. Mountain Standard Time hours) telephone or email customer support services. Provide access for DEN 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
32.1-7	Provide details of vendors change management program (system changes, roll-back plan, etc.) and provide examples of change management documentation that is currently used
32.1-8	Vendor shall explain active data storage and archiving methodologies
32.1-9	Vendor shall support the utilization of backup and recovery management software that will allow for a Recovery Point Objective of no greater than 4 hours

32.1-10	Provide ability to monitor and automatically report system health, notifying support staff using standard technologies such as SMS and SNMP
33.0 Historical Data Conversion	
33.1-1	All data fields utilized in BadgEze database will be converted to and managed by IDMS
33.1-2	Utilize existing badges with new system
33.1-3	Maintains same unique badge IDs
33.1-4	Generate a unique person ID or use existing unique DEN Airport ID for all converted badge holder records
33.1-5	Collaborate with DEN to ensure that all BadgEze business rules are functional in the new IDMS.
33.1-6	Has scripts to convert existing tables/fields to product database tables/fields
33.1-7	Has secure server on which to test data translation involving SSI
33.1-8	Merge multiple records for the same person
33.1-9	Identify all data to be migrated into the IDMS in a Transition Plan, which must include a data migration validation
33.1-10	Vendor shall include a backout plan for all data and processes in the event the go-live event does not execute as planned
33.1-11	Identify all data to be migrated into the IDMS in a Transition Plan, which must include a data migration validation
33.1-12	Coordinate scheduling and deliverables to achieve agreed upon project schedule taking into account other City work activities
33.1-13	Provide Acceptance Test Plan for individual units and the system as a whole, and will work with the City to conduct and review the test results and obtain approval for final System Acceptance
33.1-14	Provide software integration to a badging workstation with peripherals in the existing IT test lab that connects to the test/development environment
33.1-15	Provide system testing sufficient to verify proper operation of all system components, system interfaces, and end-to-end system activities to the satisfaction of the City project team
33.1-16	Have at least one individual onsite for 5 business days during the transition from the test environment to a live environment
33.1-17	Provide sample test scripts that will be used during all phases of UAT
34.0 Documentation and Training	
34.1-1	Provide an electronic training platform (recorded and live) for DEN Authorized Signatory population
34.1-2	Business processes must be documented and included as part of the training manual
34.1-3	Provide supporting documentation about IDMS for DEN dissemination users and stakeholders
34.1-4	Includes end user training for trusted agents and authorized signatories prior to roll-out
34.1-5	On-line user documentation illustrating how to use software
34.1-6	Provide accurate, meaningful, configurable on-screen instructions.
34.1-7	Provide training plan schedule 90 days prior to training event. Submit training plans, objectives, curriculum, and sample materials for City project team final review, at least two weeks in advance of scheduled training

34.1-8	Provide training for all system users, System Administrators, and support personnel at the City's facilities prior to system implementation that includes classroom training, tutorials, and/or self-study materials. Provide digital copy of training materials. Locally hosted training videos are desired *by activity* for Authorized Signatory reference
34.1-9	Provide training and certification of Vendor's product for customer support staff
34.1-10	Supply DEN-specific SOP's no later than six weeks prior to "Go live" date
34.1-11	Provide System documentation, such as user and System Administrator manuals, system reference guides, quick reference cards, etc.
34.1-12	Provide API documentation
34.1-13	Provide System and component configuration documents
34.1-14	Provide data file formats and structure; data architecture drawings and data flows
34.1.15	Provide System manuals
34.1-16	Provide published API documentation
34.1-17	Provide physical and logical as-built server and application architecture, along with step by step deployment actions
34.1-19	Provide vendor solution training for DEN user community (excluding Authorized Signatories)
34.1-20	Provide a detailed schedule including specific deliverables and dates
35.0 Warranty	
35.1-1	Warrantied until 36th month from contract execution date, after formal written acceptance of production system. Customer Care (Support & Maintenance) includes all product releases to support new Federally issued SD's (1542-04-08K); labor, version upgrades, upgrades to remain compliant with regulatory changes, support, and preventive maintenance typically included in annual maintenance
35.1-2	Includes all updates to remain compliant with TSA 49 CFR Part 1542 and other applicable regulatory requirements, subject to agreement within the vendor solution Aviation Community Forum. Variations may be chargeable as enhancements.
35.1-3	New required fields created to comply with TSA SDs or other reasons must be prepopulated to prevent null values
35.1-4	Includes all regular version upgrades
35.1-5	24/7 on-call support via phone or web with one hour maximum initial response time
35.1-6	Live phone support Monday-Friday 6:30am-6:30pm EST
35.1-7	Respond within one (1) hour of vendor application outage
35.1-8	Includes keeping integrations current with new releases of vendor business-partner integrated products at no extra cost. Non-vendor business partner integration upkeep may require extra costs.
36.0 Standard Maintenance	
36.1-1	Provide vendor solution updates and bug fixes to the system at no additional charge during the term of any maintenance/service agreements. All system changes will be conducted after hours in coordination with DEN staff.
36.1-2	Provide during the warranty period and any period thereafter where the IDMS is covered by an annual maintenance agreement, no-charge Released Updates to comply with TSA Security Directives. Custom updates may require additional costs to DEN.
36.1-3	Include an explanation of the system's warranty coverage, and also includes optional extended maintenance agreement/warranty options. All non-emergency system maintenance will be completed after hours

36.1-4	Provide an annual onsite system review with DEN staff. System performance will be reviewed and discussed as well as vendor insight provided to future software and other changes and/or upgrades
36.1-5	Provide support that must be available from the Vendor via toll free phone support 24/7
36.1-6	Provide software license agreement is not dependent on the maintenance agreement
36.1-7	Provide all software upgrades in the first year warranty and included in subsequent years as part of any maintenance agreement
37.0 Physical Key Tracking	
37.1-1	Assign metal keys to cardholders and automatically require the return or reassignment of those keys when a badge or credential expires or otherwise loses active status
37.1-2	Track key information and status, such as serial number, date key entered in system, and date key issued, date key lost, fee for lost key, fee payment date, fee receipt number, or indication if fee is waived
37.1-3	Provide a means whereby keys can be transferred from one cardholder to another active cardholder in the same company
37.1-4	Allow Authorized Signatories to reassign Administrative keys to cardholders within their company
37.1-5	Send automated notification, such as notifying a City manager, or Authorized Signatories, Locksmith, etc. who may be assigned the next action to review, approve, adjudicate and allow access or obtain keys
37.1-6	Allow System Administrator the ability to assign a Trusted Agent, Comm Center, Locksmith, etc. to a pre-defined workgroup when a new person is assigned to that workgroup, they shall automatically receive all permissions associated with that workgroup definition

Exhibit A, Attachment A-2

Invoice #	Milestone	Task Deliverables	Software Installation	Professional Services	Support and Maintenance	Invoice Due	Retainage	Retainage Returned	Invoice Paid	Complete by Month	Running Total
			$1,125,000.00	$503,000.00	$200,000.00						
1	Functional specification signoff	1.1, 1.2, 1.3, 1.4, 1.5	$112,500.00	$100,600.00		$213,100.00	$21,310.00		$191,790.00	6	$191,790.00
2	Technical specification - review and signoff	1.6, 1.7	$112,500.00	$25,150.00		$137,650.00	$13,765.00		$123,885.00	8	$315,675.00
3	Test plan - review and signoff	1.8, 1.9a, 1.9b	$112,500.00	$25,150.00		$137,650.00	$13,765.00		$123,885.00	8	$439,560.00
4	**Development Environment** - SAFE Core 5.0 + modules - Testing	2a, 3a, 5a	$112,500.00	$62,300.00		$174,800.00	$17,480.00		$157,320.00	7	**$439,560.00**
5	**QA Environment** - User Acceptance Test signoff	2b, 3b, 4, 5b	$225,000.00	$100,600.00		$325,600.00	$32,560.00		$293,040.00	12	**$889,920.00**
6	**Production Environment** - SAFE Core 5.0 + modules - Testing plus User Acceptance Test signoff	1.10, 1.11, 6	$450,000.00	$201,200.00		$651,200.00	$65,120.00		$586,080.00	16	$1,476,000.00
7	**Production Environment** - SAFE Solution - **GO LIVE** and Punch-List Completion	7			$200,000.00	$200,000.00	$20,000.00		$180,000.00	18	$1,656,000.00
	Retainage Subtotal						$184,000.00				
8	Retainage Returned	Paid following Invoice #8					$184,000.00	$184,000.00	$184,000.00	19	$1,840,000.00
9	Post-Contract Date of Execution Licensing/Support/Maintenance for Year 4	7			$175,320.00	$175,320.00	$0.00		$175,320.00	37	$2,015,320.00
10	Post-Contract Date of Execution Licensing/Support/Maintenance for Year 5	7			$175,320.00	$175,320.00	$0.00		$175,320.00	49	$2,190,640.00
11	Post-Contract Date of Execution Licensing/Support/Maintenance for Year 6 (at DEN discretion)	7			$175,320.00	$175,320.00	$0.00		$175,320.00	61	$2,365,960.00
12	Post-Contract Date of Execution Licensing/Support/Maintenance for Year 7 (at DEN discretion)	7			$175,320.00	$175,320.00	$0.00		$175,320.00	73	$2,541,280.00
	Total		$1,125,000.00	$515,000.00	$901,280.00	$2,541,280.00			$2,541,280.00		$2,541,280.00

Software Support Agreement (SSA)

Quantum Secure offers standard software system support coverage for all their products. This Agreement sets forth the terms and conditions under which Quantum Secure shall maintain its Software Products which have been properly purchased, licensed or sub-licensed to the Customer.

1.0 Maintenance of Software

Beginning on the day of the execution of this agreement, Quantum Secure shall provide the following error-correction, bug fixing and software support services:

(a) Telephonic support during the defined days and hours of business operation as per below. Such support shall include consultation on the operation and utilization of the Software.

(b) Software error / bug correction services, consisting of Quantum Secure's using all reasonable efforts to design, code and implement programming changes to the Software, and modifications to the documentation, to correct reproducible errors therein so that the Software is brought into substantial conformance with the Specification.

(c) Copyrighted software patches, updates, new releases and new versions of the Software, including the PACS agents deployed along with other generally available technical material. Under this agreement, Quantum Secure will release the new PACS agent for the newer release of the PACS (Physical Access Control Systems) software within six months of the new version of that PACS being commercially available in the market by the PACS manufacturer.

The Licensee must inform Quantum Secure at least 90 days before any scheduled upgrades to the SAFE connected systems, such as PACS, IDMS, etc. for receiving appropriate software upgrade. In case Quantum Secure cannot get hold of the newer version of the PACS or any other software from the market / from the original manufacturers, then Quantum Secure will be allowed to develop the upgrade of its software against the copy of the new version of the PACS or any other software belonging to the Licensee.

In order to provide timely support under this support agreement, the Licensee must provide a convenient remote access authorization to Quantum Secure support team to the servers where Quantum Secure products are installed. Without an uninterrupted access to these servers, the support process may be delayed and could lead to longer time for problem diagnostics and resolution.

2.0 Exceptions

Quantum Secure Software Support Agreement does not cover operating systems, backup and/or restoration of the Quantum Secure SOFTWARE and/or associated data, reinstallation of the SOFTWARE on a different or repaired computer, SOFTWARE tampering in any form, accounting issues, Database issues, Internet connection issues, viruses, spy ware, networking issues, hardware or any other third party software or device issues. While we will do our best to help, support of these uncovered issues may incur additional charges on a per incident basis. Software updates does not cover any required data conversion; operating systems, hardware, additional training, government initiated changes which require software programming changes, pre-printed form layouts or the conversion and/or adaptation of any Licensee requested modifications or reports.

3.0 Term

This SSA will be for a period of one year from the first day of the following month the software installation at the Licensee's site begins or the 90 days from the shipment date, whichever comes first and shall be automatically renewed for additional one year terms. Licensee may terminate this SSA at any time without penalty upon sixty (60) days prior written notice to Quantum Secure. This SSA may also be terminated by Quantum Secure if the Customer defaults in the payment of any monies due under this SSA and fails to remedy the default within 15 days after written notice or in the event of a breach by Licensee of any other provision of this SSA.

4.0 *Intentionally Deleted.*

5.0 Fees & Payments

The support fees will be invoiced annually up to 30 days in advance of the renewal date and invoices are payable 30 days after receipt of invoice by the Customer. In the event that the agreement is not terminated at the end of a running one year term, the Customer is responsible for ensuring that the appropriate customer purchase order is sent to Quantum Secure, if your company requires a PO to pay the invoice.

Late payment of undisputed invoices after the due date on the invoice or after the start date of the new term may be subject to 1.5% per month late charges. The Support services and benefits are suspended

upon the expiration of the current Software Support Agreement term if the payment is not received by that time.

Standard (Silver) Service is our standard support coverage option. It provides telephone support and assistance from our Licensee Support Center during normal support hours (Mon – Fri, 9:00 a.m. – 5:00 p.m. PST) as well as software upgrades if and when available.

24/7 (Gold) Service is our premium support coverage option. It provides telephone support and assistance from our Licensee Support Center on a 24/7 basis as well as software upgrades if and when available.

Responses to the Licensee's support issues require the Licensee to provide adequate information and documentation to enable Quantum Secure to recreate the problem. Quantum may notify the Licensee that the problem could not be recreated, located or identified, if such is the case. If the reported problem is unrelated to Quantum Secure's installed products, Quantum Secure may notify Licensee that the problem will not be resolved and the reason for this decision. Notwithstanding the provisions of this section, Quantum Secure makes no warranties that the Support Services provided hereunder will be successful in resolving all difficulties or problems or in diagnosing all faults.

Licensee must maintain a functional Internet connection and dial-in (or log in via VPN) capabilities during business hours for any on-line support. Licensee must make sufficient daily, weekly and monthly backups.

NOTE: It is our policy to support the current version of each software product and one full version back. All support calls for products not under Warranty or SSA are subject to T &M charges or will be directed to purchase a SSA.

More details on our support process is available via Quantum Secure published Customer Care documentation which is included (and is downloadable from your customer care site) with the shipment of your products.

The Licensee's Role

The provision of the error correction and support services described above shall be expressly contingent upon the Licensee's reasonable cooperation in providing all relevant information about the errors, promptly reporting any errors in the Software or related documentation to the Quantum Secure's Support Department, providing adequate remote access and not modifying the Software without the written consent from Quantum Secure.

6.0 Limitation of Liability

QUANTUM SECURE AND ITS SUPPLIERS, EMPLOYEES, AGENTS, RESELLERS, OEM PARTNERS, DEALERS AND FRANCISEES WILL IN NO EVENT OTHER THAN QUANTUM SECURE'S GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, **LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION OR THE LIKE, DAMAGES FOR THE INABILITY TO USE EQUIPMENT OR ACCESS DATA**) SUFFERED BY LICENSEE, ANY OF ITS EMPLOYEES OR AGENTS OR ANY OTHER PERSON ARISING OUT OF OR IN CONNECTION WITH THE USE OR INABILITY TO USE THE SOFTWARE OR THE DOCUMENTATION, OR THE MAINTENANCE OR SUPPORT THEREOF **AND BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF QUANTUM SECURE OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.**

Quantum Secure neither assumes nor authorizes any employee, agent, dealer or franchisee to assume for Quantum Secure any other liability in connection with the license, use of performance of the Software or Documentation.

Quantum Secure will undertake all reasonable efforts to provide technical assistance under this SSA and to rectify or provide solutions to problems where the Software does not function as described in the Software documentation, but Quantum Secure does not guarantee that the problems will be solved or that any item will be error-free. This SSA is only applicable to Quantum Secure's Software running under the certified environments specified in the release notes for that product.

7.0 Software System Support

Standard Software Support Agreement (SSA) coverage, as listed, is in force for the customer after the initial warranty period. In addition, systems integrators opting to purchase support services on an "as needed" basis only, may do so at prevailing **Time and Materials Rates (T&M).** Quantum Secure requires a signed Purchase Order prior to providing T & M support services. If the end user requires on-site

installation of the software upgrades from Quantum Secure, then the end-user may do so at the prevailing time and material rates from Quantum Secure. Licensee will reimburse Quantum Secure for the actual cost of reasonable, documented travel and living expenses of the support representative, and pre-approved by Licensee for on-site activity outside of normal support.

8.0 Telephone Technical Support

During the Agreement, Quantum Secure will only accept service calls from the end –user or the employees of the Systems Integrator of Record for the specific installation to which the support inquiry relates. The standard technical support telephone number is (800) 776-3414. The preferred way to report issues is through our web site: http://support.quantumsecure.com/Login.asp

This SSA may be modified only in writing by authorized representatives of Quantum Secure, Inc. and the Customer.

NOTE: Quantum Secure does not guarantee defects will be fixed in any specific time duration due to the nature of software operating in a multi-vendor environment. It is the goal of Quantum Secure to deliver our best effort to satisfactorily resolve each incident using the best judgment under each circumstance.

Exhibit B

PROFESSIONAL SERVICES

SCHEDULING, PROGRESS REPORTING, INVOICING AND CORRESPONDENCE CONTROL

Revised: December 2014

City and County of Denver

Contents

I.   PURPOSE

The purpose of this Exhibit B is to provide consultants with specific guidelines and instructions for preparing and submitting invoices. These guidelines are not meant to be all inclusive or apply in all instances. Flexibility shall be allowed at the discretion of the project manager. Consultants shall **reference the appropriate section** as determined by the Project Manager or other authorized designee and will be maintained through the entire term of the agreement.

II.   STANDARD CONTRACTS

1.   Introduction

This Exhibit B describes the Consultant's obligations to prepare and submit schedules and progress reports, control its budget and submit invoices. The Consultant shall prepare invoices which are based on its progress toward completing the Consultant's Project. In the "payment for progress" concept described herein, the Consultant schedules the work and identifies the resources (costs and man-hours) which will be required to complete each scheduled phase. Those resources are totaled for each phase. A lump sum cost has been developed for each phase and is described in the Agreement. Progress payment measurement alternatives which the Consultant may propose for written approval for each phase are described in Section 3.below.

2.   Work Schedule

2.1   Consultant shall provide the city a preliminary Final Project Work Schedule in a format approved by the Project Manager within 45 days after receiving the *Notification to begin work*. This schedule shall follow the Work Breakdown Structure (WBS) template provided by the Project Manager, and The City may require this schedule be cost and resource loaded.

2.2   The schedule shall identify completion dates for tasks and submittals shown in the Consultant's Scope of Work.

2.3   The City will provide its comments to the Consultant within seven days after the preliminary Final Work Schedule is submitted. The Consultant shall incorporate the City's comments in the Final Work Schedule.

2.4   No later than 75 days after the Notification to begin work, the Consultant shall submit to the Project Manager the Final Work Schedule. The approved Final Work Schedule, will provide the baseline for determining monthly progress for the work and preparing invoices after it has been submitted and approved.

2.5   **Three - Week Schedule** Immediately following the Notification to begin work and throughout the Project, the Consultant shall submit to the Project Manager a rolling three-week, look-ahead schedule by every other Friday for the following three week's work. The schedule shall be time scaled in bar chart format, and shall include all tasks identified in the Final Work Schedule for each Project.

3.   Progress Payment Measurement Alternatives

The Consultant may propose for approval one of the following measurement alternatives for each scheduled task or Project for the purpose of calculating progress payments and reporting schedule status to the Project Manager. The Consultant shall use the alternative as approved in the work Authorization.

3.1   **Submittal Status** - Progress payments will be made after the submittals described in the scope of work have been delivered and approved by the Project Manager. A portion of the Fee will be allocated to each submittal.

3.2   **In Progress Status** - Progress payments will be based on the percentage of drawings, specifications, reports or other documents which have been prepared, submitted, and reviewed or completed. This alternative is acceptable for phases which have a long duration and several months may elapse between submittal dates. The Consultant shall prepare a detailed worksheet for each task

showing a schedule of proposed billing points and the number of drawings, specifications, reports and reviews that establish each point.

3.3   Completion - Payments will be made for completed phases whose total duration is less than one month, if applicable. A finish credit of 95% of the portion of the Fee allocated to a task will be given when a task has been completed and approved.

3.4   Level of Effort - Progress payments will be based on the actual number of man-hours utilized to perform the task. The Consultant shall use the above alternatives to the maximum extent possible to measure activities such as progress for management, administration, and quality control, but in situations where such tasks do not fit within the first three alternatives, the level of effort alternative maybe used. This alternative may be used for Construction Phase Services.

The Consultant may be paid on its progress toward completing each task shown on its work schedule. Submittal of time sheets may be required concurrent with the submittal of each invoice. Payments for each task will be calculated by multiplying the task completion percentage by the portion of the lump sum fee allocated to that task.

Time sheet and expense records shall be maintained by the Consultant for all work performed under the Contract. Time sheets shall be organized and tracked separately for this Project or Additional Services Authorization in separate sets of files, maintained in three ring binder(s). The City and the FAA shall have a right to examine and audit these during regular business hours.

Note: Approvals by the City of submittals do not waive any obligation by the Consultant to provide complete work that has been authorized. Authorized payments on previous invoicing may be reduced on subsequent invoicing in the event work submitted is found to be in non-compliance with scope requirements.

4.   Invoices and Progress Payments

4.1   The City will provide the Consultant access to Unifier (the approved Project Management tool) to submit their monthly progress invoice. Each Project shall be measured per discipline (including reimbursable costs) and per design phase.

4.2   Each month in which an invoice is submitted the Consultant shall invoice the City for its achieved progress on each phase during the previous month based on the method of measurement alternative selected for each phase. The invoice shall be in a form acceptable to the City. The worksheets which the Consultant uses to calculate progress for each task must be included with each copy of the invoice. (The Project Manager must provide written approval of the format for these worksheets before they may be used.)   One (1) electronic copy of both the invoice and the Consultant's worksheet(s) shall be submitted each month to the DIA Business Management Services Contract Administrator via email ContractAdminInvoices@flydenver.com. If Textura® is to be utilized please see Section 4.7.

4.3   The Consultant shall submit with each invoice signed Partial Releases from each subconsultant which states the amount of payment received for services performed during the prior billing period.

4.4   If applicable, five percent (5%) of the total amount of each invoice shall be withheld from each progress payment. The amount withheld shall be paid to the Consultant after the Consultant completes all submittals required, submittals have been approved, and the Consultant has provided all lien releases for that Project.

4.5   The Project Manager will review all invoices and in the event the Project Manager disagrees with the invoiced progress, he will notify the Consultant. The Consultant and Project Manager will meet to discuss the reasons for the disagreement and whether a portion of the payment for the task should be deferred. The Deputy Manager shall have the authority in his sole and absolute discretion to withhold portions of any progress payment request if he determines that the progress claimed for any task in the invoice has not been achieved.

4.6 In accordance with requirements set forth in this Agreement, the Consultant must have provided the City with the documentation found in Section 8 before any payments will be made to the Consultant.

4.7 Textura®**:** The consultant recognizes and agrees that it may be required to use the Textura® Construction Payment Management System (CPM System) for this Project. Proposers are urged, when preparing a proposal, to contact the Textura® Corporation at 866-TEXTURA (866-839-8872) for pricing schedule and fees, as all fees associated with the CPM System are to be paid by the consultant and subconsultant for billings for work performed.

5. Monthly Progress Report Development

5.1 The Consultant shall submit to the Project Manager two (2) copies of the Monthly Progress Report with its invoice. The report shall be in letter size format, 3 hole punched, and shall be bound by temporary aluminum screw post This Report shall contain the following sections:

Summary
- Executive Summary
- Work Schedule
- Cost Status
- Cash Flow Requirements
- Manpower and Task Completion Variance Analysis, Achieved vs. Planned, and any Planned or Proposed Schedule or Budget Revisions or other Remedial Actions
- Subcontract and Affirmative Action Goals Status

Status of Project
- Drawing/Document Schedule and Status
- Project Schedule and Manpower Status
- Task Activities Planned for Next Month
- Monthly Task Activity and Accomplishments
- Identification and Analysis, of any Scheduling, Coordination or Other Problem Areas.
- Copies of Incoming and Outgoing Correspondence Logs

5.2 The exact format and detail level required for The Monthly Progress Report will be established jointly by the Project Manager and the Consultant within fourteen (14) days after Notification to begin work based on a proposed format prepared by the Consultant. The Report shall describe task completion status in terms of original plan, actual, a forecast of time to complete tasks and any expected task budget or schedule completion variances. The "Status of Each Project" report shall be bound (stapled) separately for each project or task.

5.3 The Consultant shall be available, when requested, to meet with City representatives to discuss the current Monthly Progress Report.

6. Schedule Changes and Increases In Project Amount

Any requests for schedule changes or increases in an agreed Amount shall be submitted to the City in writing and shall include an explanation and justification for the proposed schedule change or increases. All Schedule changes or increases in compensation shall be approved in advance and in writing by the City.

7. Allowable General and Administrative Overhead (Indirect Costs)

7.0 All Allowable General and Administrative Overhead expenses are incorporated in the Labor Rates and Classifications Exhibit; Overhead / Multiplier Factor Calculation – Professional Services

Agreements, and paid through the application of the Overhead Multiplier Factor against core staff wage reimbursements.

7.1 Indirect costs are the general administrative overhead costs that benefit more than one project; costs that cannot be directly identified with a single specific task objective of the project. Department of Aviation policy is to allow overhead costs in the following manner as part of the negotiated multiplier as calculated in the Labor Rates and Classifications Exhibit:

7.1.1 **Office Provisions:** Utilities, communications systems, rent, depreciation allowances, furniture, fixed equipment, etc.

7.1.2 **Supplies, Equipment & Vehicles:** For office, drafting, engineering copying, postage, freight, surveying vehicles, computer drafting and graphics, computers, software, etc.

7.1.3 **Maintenance and Repair:** On office equipment, survey & testing equipment, buildings, vehicles, etc.

7.1.4 **Insurance:** Professional liability, errors and omissions liability, vehicles, facilities, etc.

7.1.5 **Taxes:** Personal property, state & local taxes, real estate, (state and federal income taxes excluded), etc.

7.1.6 **Marketing Fees & Publications:** Licenses, dues, subscriptions, trade shows, staff support, etc.

7.1.7 **Admin & Clerical Office Staff:** All administrative, clerical & management support staff not directly involved in the specific project or task.

7.1.8 **Other Indirect Costs:** Training, technical seminars, library, financial & legal costs, employment fees & recruiting costs, etc.

7.2 **Non-Allowable** Overhead: Including but not limited to: Advertising, bad debts, bank fees, bonuses, contingencies, distribution of profits, donations, gifts, & charitable contributions, employee stock ownership plans, entertainment & social functions, state and federal income taxes, fines & penalties, goodwill, interest expense, lobbying costs, overtime premium, unallowable relocation costs pursuant to Federal Acquisition Regulations (FAR 31.205-35), etc.. If an expense is not explicitly included in this Agreement as an allowable expense, it is not an allowable expense.

8. Allowable (Non-Salary) Expenses

8.0 **Expenses Reimbursed at Cost:** All Allowable (Non-Salary) expenses are reimbursed at cost.

8.1 **Receipts Required:** All direct expenses submitted for reimbursement must be evidenced by a submitted receipt.

8.2 **Expenses Greater Than $500:** All direct expenses greater than $500 must be pre-approved by the Project Manager or his/her designee (*Attachment B2*). Any asset purchased by DIA must be surrendered to DIA at the end of the project or task. The consultant shall be charged replacement value for any asset purchased by DIA that is not accounted for at the end of the project or task.

8.3 **Mileage Outside Of The Denver Metro Area:** Mileage reimbursement will be provided only for travel outside the Denver Metropolitan area that has been pre-approved by the Manager or his/her designee (*Attachment B3*). The reimbursement will be at the current rate established for reimbursement by the United States Internal Revenue Service (www.irs.gov). Denver metropolitan area mileage for employees assigned to the project and employees not assigned to the project will not be reimbursed. Tolls will not be reimbursed.

8.4   Travel and Airfare: All travel must be pre-approved on the DIA Advance Travel Authorization Form (Attachment B4) and signed by the Project Manager or his/her designee. Travel shall be done using the most reasonable cost and means under the circumstances. Travel expenses are reasonable, appropriate, and necessary travel and business related expenses(s) that are incurred while carrying out official City business as it relates to the consultant's contractual obligations and scope of work. The determination of reasonableness of cost and of the means of travel shall be at the discretion of the Project Manager or his/her designee, who shall consider economic factors and circumstances, including but not limited to number of days of travel, advance notice, possibility of trip cancellation, distance of travel, travel alternatives, and hours of arrival or departure.

Airfare will be reimbursed for Economy/Coach class travel only, including luggage check-in fees. Convenience expenses such as seat upgrades, in-flight meals and refreshments, entertainment, etc. will <u>not</u> be reimbursed.

8.5   Rental Car: At cost for standard class or smaller and when required for out-of-town personnel or out-of-town travel.

8.6   Lodging Rate / Night: A maximum of the Lodging per diem for the Denver metropolitan area as published by the U.S. General Services Administration website www.gsa.gov plus taxes per night, unless approved in advance in writing by the Project Manager or his/her designee.

8.7   Meals: The City shall reimburse the Traveler for reasonable meals expenses at the meal and incidental expense (M&IE) rates established through federal guidelines and IRS regulations, or at actual cost. The Agency/Department will decide on the reimbursement method. Only one method of reimbursement may be used per trip. The per diem rate includes breakfast, lunch, and dinner. Reimbursements will be made per individual Traveler conducting official City business as it relates to the consultant's contractual obligations and scope of work.

Alcohol will not be reimbursed. Meal reimbursements are not allowed for consultant employees located in the Denver Metropolitan Area.

8.8   Special: Including printing, equipment, express courier, delivery, rentals, etc., that is not already included in O.H. and is for the specific project or a task related to the Agreement. All expenditures in section 8.8 submitted for reimbursement must be pre-approved by the Project Manager or his/her designee.

8.9   Specialty Consulting: Including geotechnical testing, surveying, legal, real estate, computer, financial, renderings, animations, modeling, etc. must be pre-approved by the Project Manager or his/her designee.

8.10   Relocation Expenses For Key Personnel: All relocations intended to be submitted for reimbursement must be allowed by the contract terms and pre-approved by the Project Manager or his/her designee prior to incurring the expense. Unallowable relocation costs pursuant to Federal Acquisition Regulations (FAR 31.205-35) will not be reimbursed. DIA will reimburse only for actual relocation expenses evidenced by receipts. Reimbursement of relocations will be based on the approved receipts submitted up to a maximum of $20,000.00 for each relocation. Only relocations to the Denver metropolitan area will be considered for reimbursement. Any individual relocated must work on the related Denver International Airport project for at least six (6) months after the relocation or the reimbursement of the relocation will be refunded back to the City.

8.11   Project Field Office & Equipment: Including utilities, rent, communications systems, furniture, fixed equipment, etc.

8.12   Project Field Supplies, Equipment & Vehicles: For field office, engineering copying, postage, freight, field vehicles, computer drafting and graphics, computers, all software / license fees, etc.

8.13   <u>Non-Allowable</u> Expenses: Including but not limited to: valet parking, alcohol, tolls, laundry and dry cleaning, flight upgrades, flight change fees (unless flight changes resulted from action(s)

caused by Denver International Airport), entertainment & social functions (corporate and civic), overtime premium, fines & penalties, items included in section 7.2 above, etc. If an expense is not explicitly included in this Agreement as an allowable expense, it is <u>not</u> an allowable expense.

8.14   Preparation Of Proposals: Costs for proposal preparation and negotiation will <u>not</u> be reimbursable.

9.   Correspondence Control

All correspondence, including transmittals, between the Consultant and the City, subconsultants, contractors, subcontractors, major permanent material vendors, and other entities with participation in the design or construction of the Project(s) shall be serialized. The Consultant shall maintain individual incoming and outgoing correspondence logs for each entity. The Consultant may not correspond with Construction Contractors or Subcontractors or Suppliers without prior written approval by the Project Manager for each correspondence. The Consultant shall provide, at the request of the Project Manager, copies of all correspondence related to its work under the Agreement.

Upon Notification to begin work, the Consultant shall submit to the Project Manager a list of key personnel and their e-mail addresses for use in the DIA correspondence control system, Primavera Unifier. The Consultant will need to have sufficient software licenses to manage the Project which it shall immediately institute upon receipt of written approval from the Project Manager.

III.   TASK ORDER-BASED CONTRACTS (Airport Infrastructure Management)

1.   Introduction

1.1   This Exhibit B describes the Consultant's obligations to prepare and submit schedules, budgets, invoices, and progress reports, and to control correspondence. The Consultant shall prepare invoices that are based on its progress toward completing the Consultant's Task Order. The Consultant schedules the work and identifies the resources (costs and man-hours), which will be required to complete each scheduled phase of a Task Order. Those resources are totaled for each phase of the Task Order. The Consultant then measures monthly progress and prepares invoices on the basis of payment alternatives, which the Consultant must submit written approval for each Task Order as described in Section Three (3) of this Exhibit B. **Billing shall be at one task per invoice.**

1.2   The Consultant shall be paid on its progress toward completing a task shown on its work schedule for that Task Order. Submittal of time sheets is required concurrent with the submittal of each invoice. Payments for each Task Order will be calculated in accordance with the payment method set forth in each Task Order pursuant to Section three (3) of this Exhibit B, and shall not exceed the Not-to-Exceed amount allocated to that Task Order unless modified by a revised Task Order/Change Order.

1.3   The City shall have the right to audit all payments made to the Consultant under this Agreement. Any payments to the Consultant which exceed the amount to which the Consultant is entitled under the terms of this Agreement will be subject to set-off (what does the term set-off mean?) and not approved for payment.

1.4   The Consultant will keep and retain records relating to this Agreement and will make such records available upon request to representatives of the City, at reasonable times during the performance of this Agreement and for at least six (6) years after termination of this Agreement for purposes of audit, inspection, copying, transcribing and abstracting.

1.5   The Consultant will furnish, or cause to be furnished to the Chief Executive Officer (CEO), such information as may be requested relative to the progress, execution, and cost of individual Task Orders. The Consultant will maintain, or cause to be maintained, records showing actual time devoted and costs incurred. The Consultant will maintain, or cause to be maintained, its books, records, documents, and other evidence, and adopt, or cause to be adopted, accounting procedures and practices sufficient to reflect properly all costs of whatever nature, claimed to have been incurred and anticipated to be incurred for or in connection with the Project for six (6) years after termination of this Agreement. This system of accounting will be in accordance with generally accepted accounting principles and practices, consistently applied throughout and in accordance with instructions from the City.

1.6   In the event of the failure by the Consultant to provide records when requested, then and in that event, the Consultant will pay to the City reasonable damages the City may sustain by reason thereof.

1.7   No provision in the Agreement granting the City a right of access to records is intended to impair, limit or affect any right of access to such records, which the City would have had, in the absence of such provision.

2.   Work Schedule

2.1   The Consultant, working jointly with DIA, will develop scheduling and management procedures which allow for seamless communications of its requirements for managing Task Orders and the City's information requirements to monitor the Consultant's activities. Task Order schedules shall include all of the activities that the Consultant must perform to complete the

Consultant's Task Order Scope of Work. It shall also identify activities or actions that must be performed by the City and third parties, which would affect the Consultant's Work.

2.2 The City will provide its comments to the Consultant within five (5) working days after the Task Order Schedule is submitted. The Consultant shall incorporate the City's comments into the Task Order Schedules.

2.3 Immediately following the Notice to Proceed and throughout the Task Order, the Consultant shall submit to the Project Manager, a rolling three-week, look-ahead schedule, for the following three week's work.

3. Progress Payment Measurement Alternatives

3.1 DIA will propose and the consultant may offer alternatives, one of the following measurement alternatives for each Task Order or the overall Program for calculating progress payments and reporting schedule status to the City. The City shall make the final determination and the Consultant shall use the alternative as approved for the scope of work described in the Task Order.

    3.1.1 Submittal Status: Progress payments will be made after the submittals described in a Task Order have been delivered and approved by the City. A portion of the Fee will be allocated to each submittal as defined in the Task Order scope.

    3.1.2 In Progress Status: Progress payments will be based on the percentage of designs submittals, drawings, specifications, reports or other documents, which have been prepared, submitted, and reviewed or completed. This alternative is acceptable for Task Orders, which have a long duration, and several months may elapse between submittal dates. The Consultant shall prepare a detailed worksheet for each Task Order showing a schedule of proposed billing points and the number of design submittals, drawings, specifications, reports and reviews that establish each point.

    3.1.3 Completion: Payments will be made for completed Task Orders. This method may be used for Task Orders whose total duration is less than one month, if applicable.

    3.1.4 Level of Effort: Progress payments will be based on the actual number of man-hours utilized to perform a Task Order. Progress payments (less the appropriate retainage) will be based on the actual number of direct labor-hours expended for the period invoiced to perform a Task Order. Progress payments will not be made for amounts above the Not-to-Exceed (NTE) amount (if applicable).

3.2 Note: Approvals by the City of submittals do not waive any obligation by the Consultant to provide complete work that has been authorized. Authorized payments on previous invoicing may be set-off on subsequent invoicing in the event work submitted is found to be in non-compliance with the scope of work requirements.

4. Invoices and Progress Payments

4.0 Task orders are issued for projects with a pre-defined maximum value known as the Not-to-Exceed amount. The Not-to-Exceed is <u>not</u> a guaranteed amount to the Consultant. It is the maximum amount allowed to be paid out for the Task Order, plus or minus any pre-authorized changes. The Project Manager will determine when the Task Order deliverables have been met.

4.1 The City will provide the Consultant with the format required to process the payment through Primavera Unifier. The Consultant shall provide to the City a completed invoice format for review and approval no later than fourteen (14) days after the Issuance of task order. This format will identify the measurement alternatives, which will be used to measure progress for an individual task.

4.2   The Project Manager and the Consultant shall agree on the day of the month the Consultant's invoices shall be submitted. By the day of the month agreed to for submitting invoices, the Consultant shall invoice the City for its achieved progress on each task during the previous 30 day period. The worksheet(s) which the Consultant used to calculate progress for the Task Order must be submitted with the copy of the invoice. (The Project Manager must provide written approval of the format for these worksheets before they may be used. One (1) electronic copy of both the invoice and the Consultant's worksheet(s) shall be submitted each month to the DIA Business Management Services Contract Administrator via email ContractAdminInvoices@flydenver.com. If Textura® is to be utilized please see Section 4.11.

4.3   The Consultant shall submit with each invoice signed Partial Releases from each subconsultant which states the amount of payment(s) received and/or amount(s) invoiced but unpaid for services performed through the prior billing period. If Textura® is to be utilized please see Section 4.11.

4.4   The employee labor data (company name, employee name, hourly rate, and number of hours) on each invoice shall be submitted in Unifier.

4.5   Payment for invoices received after the day of the month agreed to for submitting invoices may be delayed. Accordingly, timely submission of invoices is required.

4.6   If applicable, five percent (5%) of the total amount of each invoice may be withheld per contract or the Bond Ordinance as it may apply, from each progress payment regardless of the measurement alternative selected in section 3 above. The amount withheld (retainage) shall be paid to the Consultant after the Consultant's completion and approval of all submittals as detailed in the CPM schedule and Submittal Log in Primavera Unifier, required by the Task Order, submittals of all lien releases, and submittal of a final close out invoice. Within six (6) months of the Substantial Completion of a Task Order, the Consultant will forfeit all retainage if Consultant fails to complete all submittals required by the Task Order.

4.7   The Project Manager will review all invoices and, in the event, the Project Manager disagrees with the invoiced progress, he will notify the Consultant. The Consultant and Project Manager will meet within fifteen (15) days of the receipt of the invoice to discuss the reasons for the disagreement and whether a portion of the payment for the task should be deferred. The Manager or his/her designee shall have the authority in his/her sole and absolute discretion to withhold portions of any progress payment request if he/she determines that the progress claimed for any task in the invoice has not been achieved.

4.8   In accordance with requirements set forth in this Agreement, the Consultant must have provided the City with the following documentation before any payments will be made to the Consultant:
- A current Certificate of Insurance providing the levels of protection required per Prime Agreement
- Signed Subconsultant Agreement(s) on: Initial Subconsultants and as new Subconsultants are acquired.
- Final Organizational Chart (Updated with new Subconsultants as they are acquired)
- Name and Title for Authorized Signatures. The table shall also include the type(s) of documents which can be signed, any dollar threshold limitations, and a facsimile of the employee's signature.

4.9   Monthly Invoice Checklist - Professional Services Agreements (*Attachment B1*): The Monthly Invoice Checklist must be submitted to the project manager with each invoice. Failure to submit the Monthly Invoice Checklist and all requirements of Exhibit B will be cause for rejection of the invoice until such time that all requirements are fulfilled.

4.10   Final Close Out Invoice: By submitting a final close out invoice, Consultant agrees that in consideration of the prior and final payments made and all payments made for authorized changes, the Consultant agrees to release and forever discharge the Owner from any and all obligations, liens, claims, security interests, encumbrances and/or liabilities arising by virtue of the contract and authorized changes between the parties, either verbal or in writing. Consultant agrees

that this release is in full settlement of any and all claims, causes of action, and liability of any nature whatsoever which Consultant, any of its subconsultants, suppliers, or the employees of each of them may now have or may assert in the future against the City of Denver, its elected and appointed officials, and its officers, employees and agents arising out of or associated with the design of the above-referenced project. It is understood and agreed that this release extends to all claims of every nature and kind whatsoever, known or unknown, suspected or unsuspected.

4.11 Textura®**:** The consultant recognizes and agrees that it may be required to use the Textura® Construction Payment Management System (CPM System) for this Project. Proposers are urged, when preparing a proposal, to contact the Textura® Corporation at 866-TEXTURA (866-839-8872) for pricing schedule and fees, as all fees associated with the CPM System are to be paid by the consultant and subconsultant for billings for work performed.

5. Monthly Progress Report Development

5.1 Invoice Report: The Consultant shall submit to the Project Manager an electronic submittal of the Monthly Progress Report with its invoice. This Report shall contain the following sections:

- a.) Executive Summary
- b.) Work Schedule (per Primavera Unifier)
- c.) Cost Status
- d.) Cash Flow Requirements
- e.) Subcontract and Minority/Women/Small/Disadvantaged Business Enterprise (M/W/S/DBE) Goals and Status
- f.) Status of Task Order
- g.) Drawing/Document Schedule and Status
- h.) Task/Project Schedule and Manpower Status
- i.) Task/Project Activities Planned for Next Month
- j.) Monthly Task/Project Activity and Accomplishments
- k.) Identification and Analysis, of any Scheduling, Coordination, or Other Problem Areas.
- l.) Change Order Log – Approved and Pending

5.2 The exact format and detail level required for The Monthly Progress Report will be established jointly by the Project Manager and the Consultant within seven (7) days after Issuance of task order based on a proposed format prepared by the Consultant. The Report shall describe Task Order(s) completion status in terms of original plan, actual, a forecast of time to complete the Task Order(s) and any expected Task Order budget or schedule completion variances. The "Status of Task Order" report shall be formatted separately for each Task Order Scope of Work.

5.3 The Consultant shall be available, when requested, to meet with City representatives to discuss the Monthly Progress Report.

6. Schedule Changes and Increase in Project Amount

6.1 Any requests for schedule changes or increases in a Task Order amount shall be submitted to the City in writing and shall include an explanation and justification for the proposed schedule change or increases.

7. Allowable General and Administrative Overhead (Indirect Costs)

7.0 All Allowable General and Administrative Overhead expenses are incorporated in the Labor Rates and Classifications Exhibit; Overhead / Multiplier Factor Calculation – Professional Services Agreements, and paid through the application of the Overhead Multiplier Factor against core staff wage reimbursements.

7.1 Indirect costs are the general administrative overhead costs that benefit more than one project; costs that cannot be directly identified with a single specific task objective of the project.

Department of Aviation policy is to allow overhead costs in the following manner as part of the negotiated multiplier as calculated in the Labor Rates and Classifications Exhibit:

7.1.1   Office Provisions: Utilities, communications systems, rent, depreciation allowances, furniture, fixed equipment, etc.

7.1.2   Supplies, Equipment & Vehicles: For office, drafting, engineering copying, postage, freight, surveying vehicles, computer drafting and graphics, computers, software, etc.

7.1.3   Maintenance and Repair: On office equipment, survey & testing equipment, buildings, vehicles, etc.

7.1.4   Insurance: Professional liability, errors and omissions liability, vehicles, facilities, etc.

7.1.5   Taxes: Personal property, state & local taxes, real estate, (state and federal income taxes excluded), etc.

7.1.6   Marketing Fees & Publications: Licenses, dues, subscriptions, trade shows, staff support, etc.

7.1.7   Admin & Clerical Office Staff: All administrative, clerical & management support staff not directly involved in the specific project or task.

7.1.8   Other Indirect Costs: Training, technical seminars, library, financial & legal costs, employment fees & recruiting costs, etc.

7.2   Non-Allowable Overhead: Including but not limited to: Advertising, bad debts, bank fees, bonuses, contingencies, distribution of profits, donations, gifts, & charitable contributions, employee stock ownership plans, entertainment & social functions, state and federal income taxes, fines & penalties, goodwill, interest expense, lobbying costs, overtime premium, unallowable relocation costs pursuant to Federal Acquisition Regulations (FAR 31.205-35), etc.. If an expense is not explicitly included in this Agreement as an allowable expense, it is not an allowable expense.

8.   Allowable (Non-Salary) Expenses

8.0   Expenses Reimbursed at Cost: All Allowable (Non-Salary) expenses are reimbursed at cost.

8.1   Receipts Required: All direct expenses submitted for reimbursement must be evidenced by a submitted receipt.

8.2   Expenses Greater Than $500: All direct expenses greater than $500 must be pre-approved by the Project Manager or his/her designee (*Attachment B2*). Any asset purchased by DIA must be surrendered to DIA at the end of the project or task. The consultant shall be charged replacement value for any asset purchased by DIA that is not accounted for at the end of the project or task.

8.3   Mileage Outside Of The Denver Metro Area: Mileage reimbursement will be provided only for travel outside the Denver Metropolitan area that has been pre-approved by the Manager or his/her designee (*Attachment B3*). The reimbursement will be at the current rate established for reimbursement by the United States Internal Revenue Service (www.irs.gov).   Denver metropolitan area mileage for employees assigned to the project and employees not assigned to the project will not be reimbursed. Tolls will not be reimbursed.

8.4   Travel and Airfare: All travel must be pre-approved on the DIA Advance Travel Authorization Form (Attachment B4) and signed by the Project Manager or his/her designee. Travel shall be done using the most reasonable cost and means under the circumstances. Travel expenses are reasonable, appropriate, and necessary travel and business related expenses(s) that

are incurred while carrying out official City business as it relates to the consultant's contractual obligations and scope of work. The determination of reasonableness of cost and of the means of travel shall be at the discretion of the Project Manager or his/her designee, who shall consider economic factors and circumstances, including but not limited to number of days of travel, advance notice, possibility of trip cancellation, distance of travel, travel alternatives, and hours of arrival or departure.

Airfare will be reimbursed for Economy/Coach class travel only, including luggage check-in fees. Convenience expenses such as seat upgrades, in-flight meals and refreshments, entertainment, etc. will not be reimbursed.

8.5   Rental Car: At cost for standard class or smaller and when required for out-of-town personnel or out-of-town travel.

8.6   Lodging Rate / Night: A maximum of the Lodging per diem for the Denver metropolitan area as published by the U.S. General Services Administration website www.gsa.gov plus taxes per night, unless approved in advance in writing by the Project Manager or his/her designee.

8.7   Meals: The City shall reimburse the Traveler for reasonable meals expenses at the meal and incidental expense (M&IE) rates established through federal guidelines and IRS regulations, or at actual cost. The Agency/Department will decide on the reimbursement method. Only one method of reimbursement may be used per trip. The per diem rate includes breakfast, lunch, and dinner. Reimbursements will be made per individual Traveler conducting official City business as it relates to the consultant's contractual obligations and scope of work.

Alcohol will not be reimbursed. Meal reimbursements are not allowed for consultant employees located in the Denver Metropolitan Area.

8.8   Special: Including printing, equipment, express courier, delivery, rentals, etc., that is not already included in O.H. and is for the specific project or a task related to the Agreement. All expenditures in section 8.8 submitted for reimbursement must be pre-approved by the Project Manager or his/her designee.

8.9   Specialty Consulting: Including geotechnical testing, surveying, legal, real estate, computer, financial, renderings, animations, modeling, etc. must be pre-approved by the Project Manager or his/her designee.

8.10   Relocation Expenses For Key Personnel: All relocations intended to be submitted for reimbursement must be allowed by the contract terms and pre-approved by the Project Manager or his/her designee prior to incurring the expense.   Unallowable relocation costs pursuant to Federal Acquisition Regulations (FAR 31.205-35) will not be reimbursed. DIA will reimburse only for actual relocation expenses evidenced by receipts. Reimbursement of relocations will be based on the approved receipts submitted up to a maximum of $20,000.00 for each relocation. Only relocations to the Denver metropolitan area will be considered for reimbursement. Any individual relocated must work on the related Denver International Airport project for at least six (6) months after the relocation or the reimbursement of the relocation will be refunded back to the City.

8.11   Project Field Office & Equipment: Including utilities, rent, communications systems, furniture, fixed equipment, etc.

8.12   Project Field Supplies, Equipment & Vehicles: For field office, engineering copying, postage, freight, field vehicles, computer drafting and graphics, computers, all software / license fees, etc.

8.13   Non-Allowable Expenses: Including but not limited to: valet parking, alcohol, tolls, laundry and dry cleaning, flight upgrades, flight change fees (unless flight changes resulted from action(s) caused by Denver International Airport), entertainment & social functions (corporate and civic), overtime premium, fines & penalties, items included in section 7.2 above, etc. If an expense is not explicitly included in this Agreement as an allowable expense, it is not an allowable expense.

8.14   Preparation Of Proposals: Costs for proposal preparation and negotiation will <u>not</u> be reimbursable.

9.   Summary of Contract Task Order Control

9.1   Prior To Commencement Of Work – Submittals Required

9.1.1   Signed Subconsultant Agreement(s) with an Exhibit listing the subconsultant's core staff rates and calculated Labor Rates and Classifications.

9.1.3   List of the names and titles of Authorized Signers, which document(s) they can sign, and a facsimile of the employee's signature.

9.1.3   Work Schedule and Task List formatting

9.2   Within 3 Days After Issuance of Task Order – Submittals Required

9.2.1   The Consultant shall meet with the Project Manager for a Pre-Work Meeting.

9.2.2   Current Certificate of Insurance reflecting the Mandatory Coverage in Exhibit D.

9.2.3   Final Organizational Chart of the Prime Contractor and all Subconsultants.

9.3   Within 7 Days After Issuance of Task Order

9.3.1   Correspondence Control Methods and Progress Report Format

9.3.2   Invoice and Progress Payment Format

9.3.3   The Consultant shall submit their proposed Monthly Progress Report Format

9.4   Bi-Weekly Submittal

9.4.1   The Consultant shall submit a detailed two-week look-ahead schedule of activities for the Task Order.

9.5   Monthly Submittals

9.5.1   The Consultant shall submit the Monthly Progress Report.

9.5.2   The Consultant shall submit invoicing by the day of the month referenced in section 4.2.

9.6   Within 7 Days After Request For Proposal For Task Order – Submittals Required

9.6.1   Scope Definitions and Detailed Cost Estimate per task and per sub-consultant, List of Submittals or Deliverables, Drawing and Specification.

9.6.2   Work Schedule per task and overall Task Order schedule showing appropriate milestones.

9.6.3   The Consultant shall submit the *Exhibit Task Order Fee Proposal* template detailing the costs of the project.

10.   Information Management Format and Electronic-Mail Protocols

10.1   All information between the Consultant and the City, and other entities with participation in the services as stated in the development of the Task Order shall be handled using Primavera Unifier.

10.2   Within 3 days following the Issuance of task order, the Consultant shall meet with the City to review the City's proposed method of correspondence, email, & submittal communication control. Within 7 days following this review, the Consultant shall institute its control procedures for the Program.

10.2.1   General: Procedures for professional services agreements require the serialization of all correspondence between the City, consultants, subconsultants, and all project entities.   All Consultants, Subconsultants, that communicate via e-mail must be managed through the Primavera Unifier system. Web-based programs or other methods of tracking electronic communications may be proposed. However, those systems must be compatible with DIA records management data system. The Consultant shall review its system with the Records Management group to determine its compatibility with DIA procedures, processes and systems.

IV.   TASK ORDER-BASED CONTRACTS (Technologies Division)

1.   Introduction

1.1   This Exhibit B describes the Consultant's obligations to prepare and submit schedules, budgets, invoices, and progress reports, and to control correspondence. The Consultant shall prepare invoices that are based on its progress toward completing the Consultant's Task Order. The Consultant schedules the work and identifies the resources (costs and man-hours), which will be required to complete each scheduled phase of a Task Order. Those resources are totaled for each phase of the Task Order. The Consultant then measures monthly progress and prepares invoices on the basis of payment alternatives, which the Consultant must propose for written approval for each Task Order as described in Section Three (3) of this Exhibit B. **Billing shall be at one task per invoice.**

1.2   The Consultant shall be paid on its progress toward completing a task shown on its work schedule for that Task Order. Submittal of time sheets is required concurrent with the submittal of each invoice. Payments for each Task Order will be calculated in accordance with the payment method set forth in each Task Order pursuant to Section three (3) of this Exhibit B, and shall not exceed the Not-to-Exceed amount allocated to that Task Order unless modified by a revised Task Order/Change Order.

1.3   The City shall have the right to audit all payments made to the Consultant under this Agreement. Any payments to the Consultant which exceed the amount to which the Consultant is entitled under the terms of this Agreement will be subject to set-off and not approved for payment.

1.4   The Consultant will keep and retain records relating to this Agreement and will make such records available upon request to representatives of the City, at reasonable times during the performance of this Agreement and for at least six (6) years after termination of this Agreement for purposes of audit, inspection, copying, transcribing and abstracting.

1.5   The Consultant will furnish, or cause to be furnished to the Chief Executive Officer (CEO), such information as may be requested relative to the progress, execution, and cost of individual Task Orders. The Consultant will maintain, or cause to be maintained, records showing actual time devoted and costs incurred. The Consultant will maintain, or cause to be maintained, its books, records, documents, and other evidence, and adopt, or cause to be adopted, accounting procedures and practices sufficient to reflect properly all costs of whatever nature, claimed to have been incurred and anticipated to be incurred for or in connection with the Project for six (6) years after termination of this Agreement. This system of accounting will be in accordance with generally accepted accounting principles and practices, consistently applied throughout and in accordance with instructions from the City.

1.6   In the event of the failure by the Consultant to provide records when requested, then and in that event, the Consultant will pay to the City reasonable damages the City may sustain by reason thereof.

1.7   No provision in the Agreement granting the City a right of access to records is intended to impair, limit or affect any right of access to such records, which the City would have had, in the absence of such provision.

2.   Work Schedule

2.1   The Consultant, working jointly with DIA's assigned Project Manager, will develop scheduling and management procedures which allow for seamless communications of its requirements for managing Task Orders and the City's information requirements to monitor the Consultant's activities. Task Order schedules shall include all of the activities that the Consultant must perform to complete the Consultant's Task Order Scope of Work. It shall also identify activities or actions that must be performed by the City and third parties, which would affect the Consultant's Work.

2.2 The City will provide its comments to the Consultant within five (5) working days after the Task Order Schedule is submitted. The Consultant shall incorporate the City's comments into the Task Order Schedules.

2.3 Immediately following the Issuance of task order and throughout the Task Order, the Consultant shall submit to the Project Manager, a rolling three-week, look-ahead schedule, for the following three week's work.

3. Progress Payment Measurement Alternatives

3.1 DIA will propose and the consultant may offer alternatives, one of the following measurement alternatives for each Task Order or the overall Program for calculating progress payments and reporting schedule status to the City. The City shall make the final determination and the Consultant shall use the alternative as approved for the scope of work described in the Task Order.

3.1.1   Submittal Status: Progress payments will be made after the submittals described in a Task Order have been delivered and approved by the City. A portion of the Fee will be allocated to each submittal as defined in the Task Order scope.

3.1.2   In Progress Status: Progress payments will be based on the percentage of designs submittals, drawings, specifications, reports or other documents, which have been prepared, submitted, and reviewed or completed. This alternative is acceptable for Task Orders, which have a long duration, and several months may elapse between submittal dates. The Consultant shall prepare a detailed worksheet for each Task Order showing a schedule of proposed billing points and the number of design submittals, drawings, specifications, reports and reviews that establish each point.

3.1.3   Completion: Payments will be made for completed Task Orders. This method may be used for Task Orders whose total duration is less than one month, if applicable.

3.1.4   Level of Effort: Progress payments will be based on the actual number of man-hours utilized to perform a Task Order. Progress payments (less the appropriate retainage) will be based on the actual number of direct labor-hours expended for the period invoiced to perform a Task Order. Progress payments will not be made for amounts above the Not-to-Exceed (NTE) amount (if applicable).

3.2   Note: Approvals by the City of submittals do not waive any obligation by the Consultant to provide complete work that has been authorized. Authorized payments on previous invoicing may be set-off on subsequent invoicing in the event work submitted is found to be in non-compliance with the scope of work requirements.

4. Invoices and Progress Payments

4.0 Task orders are issued for projects with a pre-defined maximum value known as the Not-to-Exceed amount. The Not-to-Exceed is not a guaranteed amount to the Consultant. It is the maximum amount allowed to be paid out for the Task Order, plus or minus any pre-authorized changes. The Project Manager will determine when the Task Order deliverables have been met.

4.1 The City will provide the Consultant with the format required to process the payment through Textura may be applicable. The Consultant shall provide to the City a completed invoice format for review and approval no later than fourteen (14) days after the Issuance of task order. This format will identify the measurement alternatives, which will be used to measure progress for an individual task.

4.2 The Project Manager and the Consultant shall agree on the day of the month the Consultant's invoices shall be submitted. By the day of the month agreed to for submitting invoices, the Consultant shall invoice the City for its achieved progress on each task during the previous 30 day period. The worksheet(s) which the Consultant used to calculate progress for the Task Order

must be submitted with the copy of the invoice. (The Project Manager must provide written approval of the format for these worksheets before they may be used. One (1) electronic copy of both the invoice and the Consultant's worksheet(s) shall be submitted each month to the DIA Business Management Services Contract Administrator via email ContractAdminInvoices@flydenver.com. If Textura® is to be utilized please see Section 4.11.

4.3 The Consultant shall submit with each invoice signed Partial Releases from each subconsultant which states the amount of payment(s) received and/or amount(s) invoiced but unpaid for services performed through the prior billing period. If Textura® is to be utilized please see Section 4.11.

4.4 The employee labor data (company name, employee name, hourly rate, and number of hours) on each invoice shall be submitted in Unifier.

4.5 Payment for invoices received after the day of the month agreed to for submitting invoices may be delayed. Accordingly, timely submission of invoices is required.

4.6 If applicable, five percent (5%) of the total amount of each invoice may be withheld per contract or the Bond Ordinance as it may apply, from each progress payment regardless of the measurement alternative selected in section 3 above. The amount withheld (retainage) shall be paid to the Consultant after the Consultant's completion and approval of all submittals as detailed in the CPM schedule and Submittal Log in Primavera Unifier, required by the Task Order, submittals of all lien releases, and submittal of a final close out invoice. Within six (6) months of the Substantial Completion of a Task Order, the Consultant will forfeit all retainage if Consultant fails to complete all submittals required by the Task Order.

4.7 The Project Manager will review all invoices and, in the event, the Project Manager disagrees with the invoiced progress, he will notify the Consultant. The Consultant and Project Manager will meet within fifteen (15) days of the receipt of the invoice to discuss the reasons for the disagreement and whether a portion of the payment for the task should be deferred. The Manager or his/her designee shall have the authority in his/her sole and absolute discretion to withhold portions of any progress payment request if he/she determines that the progress claimed for any task in the invoice has not been achieved.

4.8 In accordance with requirements set forth in this Agreement, the Consultant must have provided the City with the following documentation before any payments will be made to the Consultant:
- A current Certificate of Insurance providing the levels of protection required per Prime Agreement
- Signed Subconsultant Agreement(s) on: Initial Subconsultants and as new Subconsultants are acquired.
- Name and Title for Authorized Signatures. The table shall also include the type(s) of documents which can be signed, any dollar threshold limitations, and a facsimile of the employee's signature.

4.9 **Monthly Invoice Checklist - Professional Services Agreements (*Attachment B1*):** The Monthly Invoice Checklist must be submitted to the project manager with each invoice. Failure to submit the Monthly Invoice Checklist and all requirements of Exhibit B will be cause for rejection of the invoice until such time that all requirements are fulfilled.

4.10 **Final Close Out Invoice:** By submitting a final close out invoice, Consultant agrees that in consideration of the prior and final payments made and all payments made for authorized changes, the Consultant agrees to release and forever discharge the Owner from any and all obligations, liens, claims, security interests, encumbrances and/or liabilities arising by virtue of the contract and authorized changes between the parties, either verbal or in writing. Consultant agrees that this release is in full settlement of any and all claims, causes of action, and liability of any nature whatsoever which Consultant, any of its subconsultants, suppliers, or the employees of each of them may now have or may assert in the future against the City of Denver, its elected and appointed officials, and its officers, employees and agents arising out of or associated with the

design of the above-referenced project. It is understood and agreed that this release extends to all claims of every nature and kind whatsoever, known or unknown, suspected or unsuspected.

4.11 Textura®**:** The consultant recognizes and agrees that it may be required to use the Textura® Construction Payment Management System (CPM System) for this Project. Proposers are urged, when preparing a proposal, to contact the Textura® Corporation at 866-TEXTURA (866-839-8872) for pricing schedule and fees, as all fees associated with the CPM System are to be paid by the consultant and subconsultant for billings for work performed.

5.   Monthly Progress Report Development

5.1   Invoice Report: The Consultant shall submit to the Project Manager an electronic submittal of the Monthly Progress Report with its invoice. This Report shall contain the following sections:

      m.)   Executive Summary
      n.)   Work Schedule (per Primavera Unifier)
      o.)   Cost Status
      p.)   Cash Flow Requirements
      q.)   Subcontract and Minority/Women/Small/Disadvantaged Business Enterprise (M/W/S/DBE) Goals and Status
      r.)   Status of Task Order
      s.)   Drawing/Document Schedule and Status
      t.)   Task/Project Schedule and Manpower Status
      u.)   Task/Project Activities Planned for Next Month
      v.)   Monthly Task/Project Activity and Accomplishments
      w.)   Identification and Analysis, of any Scheduling, Coordination, or Other Problem Areas.
      x.)   Change Order Log – Approved and Pending

5.2 The exact format and detail level required for The Monthly Progress Report will be established jointly by the Project Manager and the Consultant within seven (7) days after Issuance of task order based on a proposed format prepared by the Consultant. The Report shall describe Task Order(s) completion status in terms of original plan, actual, a forecast of time to complete the Task Order(s) and any expected Task Order budget or schedule completion variances. The "Status of Task Order" report shall be formatted separately for each Task Order Scope of Work.

5.3 The Consultant shall be available, when requested, to meet with City representatives to discuss the Monthly Progress Report.

6.   Schedule Changes and Increase in Project Amount

6.1 Any requests for schedule changes or increases in a Task Order amount shall be submitted to the City in writing and shall include an explanation and justification for the proposed schedule change or increases.

7.   Allowable General and Administrative Overhead (Indirect Costs)

7.0 All Allowable General and Administrative Overhead expenses are incorporated in the Labor Rates and Classifications Exhibit; Overhead / Multiplier Factor Calculation – Professional Services Agreements, and paid through the application of the Overhead Multiplier Factor against core staff wage reimbursements.

7.1 Indirect costs are the general administrative overhead costs that benefit more than one project; costs that cannot be directly identified with a single specific task objective of the project. Department of Aviation policy is to allow overhead costs in the following manner as part of the negotiated multiplier as calculated in the Labor Rates and Classifications Exhibit:

7.1.1 Office Provisions: Utilities, communications systems, rent, depreciation allowances, furniture, fixed equipment, etc.

7.1.2 Supplies, Equipment & Vehicles: For office, drafting, engineering copying, postage, freight, surveying vehicles, computer drafting and graphics, computers, software, etc.

7.1.3 Maintenance and Repair: On office equipment, survey & testing equipment, buildings, vehicles, etc.

7.1.4 Insurance: Professional liability, errors and omissions liability, vehicles, facilities, etc.

7.1.5 Taxes: Personal property, state & local taxes, real estate, (state and federal income taxes excluded), etc.

7.1.6 Marketing Fees & Publications: Licenses, dues, subscriptions, trade shows, staff support, etc.

7.1.7 Admin & Clerical Office Staff: All administrative, clerical & management support staff not directly involved in the specific project or task.

7.1.8 Other Indirect Costs: Training, technical seminars, library, financial & legal costs, employment fees & recruiting costs, etc.

7.2 Non-Allowable Overhead: Including but not limited to: Advertising, bad debts, bank fees, bonuses, contingencies, distribution of profits, donations, gifts, & charitable contributions, employee stock ownership plans, entertainment & social functions, state and federal income taxes, fines & penalties, goodwill, interest expense, lobbying costs, overtime premium, unallowable relocation costs pursuant to Federal Acquisition Regulations (FAR 31.205-35), etc.. If an expense is not explicitly included in this Agreement as an allowable expense, it is not an allowable expense.

8. Allowable (Non-Salary) Expenses

8.0 Expenses Reimbursed at Cost: All Allowable (Non-Salary) expenses are reimbursed at cost.

8.1 Receipts Required: All direct expenses submitted for reimbursement must be evidenced by a submitted receipt.

8.2 Expenses Greater Than $500: All direct expenses greater than $500 must be pre-approved by the Project Manager or his/her designee (*Attachment B2*). Any asset purchased by DIA must be surrendered to DIA at the end of the project or task. The consultant shall be charged replacement value for any asset purchased by DIA that is not accounted for at the end of the project or task.

8.3 Mileage Outside Of The Denver Metro Area: Mileage reimbursement will be provided only for travel outside the Denver Metropolitan area that has been pre-approved by the Manager or his/her designee (*Attachment B3*). The reimbursement will be at the current rate established for reimbursement by the United States Internal Revenue Service (www.irs.gov). Denver metropolitan area mileage for employees assigned to the project and employees not assigned to the project will not be reimbursed. Tolls will not be reimbursed.

8.4 Travel and Airfare: All travel must be pre-approved on the DIA Advance Travel Authorization Form (Attachment B4) and signed by the Project Manager or his/her designee. Travel shall be done using the most reasonable cost and means under the circumstances. Travel expenses are reasonable, appropriate, and necessary travel and business related expenses(s) that are incurred while carrying out official City business as it relates to the consultant's contractual obligations and scope of work. The determination of reasonableness of cost and of the means of travel shall be at the discretion of the Project Manager or his/her designee, who shall consider

economic factors and circumstances, including but not limited to number of days of travel, advance notice, possibility of trip cancellation, distance of travel, travel alternatives, and hours of arrival or departure.

Airfare will be reimbursed for Economy/Coach class travel only, including luggage check-in fees. Convenience expenses such as seat upgrades, in-flight meals and refreshments, entertainment, etc. will not be reimbursed.

8.5   Rental Car: At cost for standard class or smaller and when required for out-of-town personnel or out-of-town travel.

8.6   Lodging Rate / Night: A maximum of the Lodging per diem for the Denver metropolitan area as published by the U.S. General Services Administration website www.gsa.gov plus taxes per night, unless approved in advance in writing by the Project Manager or his/her designee.

8.7   Meals: The City shall reimburse the Traveler for reasonable meals expenses at the meal and incidental expense (M&IE) rates established through federal guidelines and IRS regulations, or at actual cost. The Agency/Department will decide on the reimbursement method. Only one method of reimbursement may be used per trip. The per diem rate includes breakfast, lunch, and dinner. Reimbursements will be made per individual Traveler conducting official City business as it relates to the consultant's contractual obligations and scope of work.

Alcohol will not be reimbursed. Meal reimbursements are not allowed for consultant employees located in the Denver Metropolitan Area.

8.8   Special: Including printing, equipment, express courier, delivery, rentals, etc., that is not already included in O.H. and is for the specific project or a task related to the Agreement. All expenditures in section 8.8 submitted for reimbursement must be pre-approved by the Project Manager or his/her designee.

8.9   Specialty Consulting: Including geotechnical testing, surveying, legal, real estate, computer, financial, renderings, animations, modeling, etc. must be pre-approved by the Project Manager or his/her designee.

8.10   Relocation Expenses For Key Personnel: All relocations intended to be submitted for reimbursement must be allowed by the contract terms and pre-approved by the Project Manager or his/her designee prior to incurring the expense. Unallowable relocation costs pursuant to Federal Acquisition Regulations (FAR 31.205-35) will not be reimbursed. DIA will reimburse only for actual relocation expenses evidenced by receipts. Reimbursement of relocations will be based on the approved receipts submitted up to a maximum of $20,000.00 for each relocation. Only relocations to the Denver metropolitan area will be considered for reimbursement. Any individual relocated must work on the related Denver International Airport project for at least six (6) months after the relocation or the reimbursement of the relocation will be refunded back to the City.

8.11   Project Field Office & Equipment: Including utilities, rent, communications systems, furniture, fixed equipment, etc.

8.12   Project Field Supplies, Equipment & Vehicles: For field office, engineering copying, postage, freight, field vehicles, computer drafting and graphics, computers, all software / license fees, etc.

8.13   Non-Allowable Expenses: Including but not limited to: valet parking, alcohol, tolls, laundry and dry cleaning, flight upgrades, flight change fees (unless flight changes resulted from action(s) caused by Denver International Airport), entertainment & social functions (corporate and civic), overtime premium, fines & penalties, items included in section 7.2 above, etc. If an expense is not explicitly included in this Agreement as an allowable expense, it is not an allowable expense.

8.14   Preparation Of Proposals: Costs for proposal preparation and negotiation will not be reimbursable.

9. Summary of Contract Task Order Control

9.1 Prior To Commencement Of Work – Submittals Required

9.1.1 Signed Subconsultant Agreement(s) with an Exhibit listing the subconsultant's core staff rates and calculated Labor Rates and Classifications.

9.1.2 List of the names and titles of Authorized Signers, which document(s) they can sign, and a facsimile of the employee's signature.

9.1.3 Work Schedule and Task List formatting

9.2 Within 3 Days After Issuance of Task Order – Submittals Required

9.2.1 The Consultant shall meet with the Project Manager for a Pre-Work Meeting.

9.2.2 Current Certificate of Insurance reflecting the Mandatory Coverage in Exhibit D.

9.2.3 Final Organizational Chart of the Prime Contractor and all Subconsultants.

9.3 Within 7 Days After Issuance of Task Order

9.3.1 Correspondence Control Methods and Progress Report Format

9.3.2 Invoice and Progress Payment Format

9.3.3 The Consultant shall submit their proposed Monthly Progress Report Format

9.4 Bi-Weekly Submittal

9.4.1 The Consultant shall submit a detailed two-week look-ahead schedule of activities for the Task Order.

9.5 Monthly Submittals

9.5.1 The Consultant shall submit the Monthly Progress Report.

9.5.2 The Consultant shall submit invoicing by the day of the month referenced in section 4.2.

9.6 Within 7 Days After Request For Proposal For Task Order – Submittals Required

9.6.1 Scope Definitions and Detailed Cost Estimate per task and per sub-consultant, List of Submittals or Deliverables, Drawing and Specification.

9.6.2 Work Schedule per task and overall Task Order schedule showing appropriate milestones.

9.6.3 The Consultant shall submit the *Exhibit Task Order Fee Proposal* template detailing the costs of the project.

10. Information Management Format and Electronic-Mail Protocols

10.1 All information between the Consultant and the City, and other entities with participation in the services as stated in the development of the Task Order shall be handled using Primavera Unifier.

10.2 Within 3 days following the Issuance of task order, the Consultant shall meet with the City to review the City's proposed method of correspondence, email, & submittal communication control. Within 7 days following this review, the Consultant shall institute its control procedures for the Program.

10.2.1 General: Procedures for professional services agreements require the serialization of all correspondence between the City, consultants, subconsultants, and all project entities. All Consultants or Subconsultants that communicate via e-mail must be managed through the Primavera Unifier system. Web-based programs or other methods of tracking electronic communications may be proposed. However, those systems must be compatible with DIA records management data system. The Consultant shall review its system with the Records Management group to determine its compatibility with DIA procedures, processes and systems.

Attachment B1 – Monthly Invoice Checklist

Professional Services Agreements

Date: _____   **Invoice Number:** _____

Contract Number: _____

Contract Name: _____

Consultant: _____
<div align="center">(Name)</div>

_____
<div align="center">(Address)</div>

Monthly Progress Payment Invoice and Exhibit B Progress Requirements Checklist:
(Place a check in the box to indicate that the item was supplied in accordance with Exhibit B requirements)

- ☐ Three Week Schedules for period covered by this invoice (Section 2.4)
- ☐ Originals of Sub-Consultant Partial Releases (Section 4.3)
- ☐ Invoice Report (Section 5.1)
    - ☐ Executive Summary
    - ☐ Work Schedule(s)
    - ☐ Cost Status
    - ☐ Cash Flow Requirements
    - ☐ Manpower and Task Completion Variance Analysis, Achieved vs. Planned, and any Planned or Proposed Schedule or Budget Revisions or other Remedial Actions
    - ☐ Subcontract and Minority/Women/Small/Disadvantaged Business Enterprise (M/W/S/DBE) Goals and Status
    - ☐ Status of Task Order
    - ☐ Drawing / Document Schedule and Status
    - ☐ Task/Project Schedule and Manpower Status
    - ☐ Task/Project Activities Planned for Next Month
    - ☐ Monthly Task/Project Activity and Accomplishments
    - ☐ Identification and Analysis, of any Scheduling, Coordination, or Other problem Areas
    - ☐ Change Order Log – Approved and Pending

The preceding and noted reports, schedules and logs have been submitted at the appropriate intervals and in accordance with the requirements of Exhibit B. The Consultant acknowledges that failure to submit the required items will result in the rejection of the Monthly Progress Payment Invoice until such time that all requirements are fulfilled.

_____
Signature   Date

_____
Type Name and Title

Attachment B2 – Expense Greater than $500 Approval Form

Date: _____

Contract Name: _____

Contract Number: _____ **Task Number(s) (if applicable):** _____

Company Name: _____

Employee Name: _____

Estimated Total Cost: $_____

Reason for Expense: _____

_____

_____

_____

_____

_____

To be completed by DIA personnel:

Capital Assets   Y / N
(Including but not limited to: computer equipment, copiers, furniture, vehicles, etc.)

Note: Any assets purchased by DIA must be returned to DIA at the end of the project. The Consultant will be charged replacement value for any assets purchased by DIA that are unaccounted for at the end of the project.

The above described expense has been approved.

_____
Signature   Date

_____
Type Name and Title

cc: Finance if asset purchase

December 2014

Attachment B3 – Mileage Reimbursement Form

Date:_____

Contract Name: _____

Contract Number: _____**Task Number(s):** _____

Company Name: _____

Employee Name: _____

Travel From: _____

Travel To: _____

Estimated Total Miles: _____

Estimated Total Cost: $_____

Reason for Travel: _____

_____

_____

_____

_____

Travel for the above named individual and purpose is approved.

_____
Signature   Date

_____

Attachment B4 – Advance Travel Authorization Form

Contract No.:_____ **Date:**_____

Traveler's Name: _____ **Authorization No.:**_____

Traveler's Employer: _____

Destination: _____

Duration: From _____ **To** _____

Purpose of Trip: _____

Approximate Travel Costs: $_____

Reviewed by: _____
Project Manager   Date

Approved by: _____
Section Manager   Date

Approved by: _____
Deputy Manager   Date

cc: BMS Contract Administrator

Attachment B5 – Technologies Work Order Form

CONTRACTOR WORK ORDER

1. Vendor Name: _____   Contract No: 201XXXXXX

2. Start Date: XX/XX/XXXX   End Date: XX/XX/XXXX

3. Contracted   Employee's   Name:

   _____

4. Bill Rate: $XX.XX   per hour (estimated at 40 hours per week)

5. Title: _____

6. *Overtime Rate: $XX.XX   per hour (for hours worked in excess of 40 hours per week)
   *Client approval required for overtime.

7. Training Expenses: DIA will not pay for training or for hours spent in training for consultants or contractors.

8. Expense Reimbursements: DIA will not reimburse for any expenses incurred by consultant.

9. Service Sites: Unless otherwise specified in writing, the services to be performed by Consultant shall be performed at the Client location specified above.

10. Time Tracking: All work performed by consultant shall be tracked accurately and consultant shall submit a weekly timecard to Client for approval.

11. Written Approval: All overtime (hours worked in excess of 40 hours per week) and work performed off-site shall be approved by Client in writing prior to the work being performed.

12. Early Termination: Client reserves the right to terminate this Work Order at any time and for any reason prior to the end date specified in this work order.

13. Mandatory Furlough: In the case where the City & County of Denver mandates furlough days for its personnel, Consultant agrees to match the required furlough days for its employees and not bill DIA for the furlough days taken by the contractor.

Employee Name: _____
Vendor Name: _____
Contract No. <u>201XXXXXX</u>

14. Responsibilities:

- Manage Information Security's service ticket queue. Perform service ticket resolution or escalation in a timely fashion while meeting SLA response time.

- Create change requests and perform modifications to Information Security systems, such as firewalls, VPN systems, access control systems, AAA systems, web proxies, logging environment, and other Information Security systems.

- Participate in all phases of the SDLC as it relates to new Information Security initiatives and projects. This includes design, testing and modifying new systems, and assisting with enterprise deployments.

- Creation of formal documentation and diagrams for systems administration, operations, and maintenance

- Analyze system and network data from sources such enterprise SIEM, data feeds of alerts and logs from firewalls, routers, and other network devices or hosts, network IPS/IDS systems, other host and network-based signature and heuristics based systems, AAA systems, and other information sources. This serves to ensure the safety of DIA's digital assets and to protect systems from intentional or inadvertent access, prevent security violations, system intrusions, data breaches, and system destruction.

- Prepares reports on an as needed basis for compliance, change management, systems monitoring, and intrusion analysis.

- Performs Information Security Incident Response and investigation activities and maintains logs to record and report incidents.

- Proactively monitor critical Information Security infrastructure for operating errors or other risks to system availability as the Information Security liaison to the DIA Technologies' Enterprise Service and Monitoring Center (ESMC) team. This may require after-hours work to support enterprise wide upgrades or deployments that interact with Information Security systems.

- Assist in bringing new systems into Information Security's monitoring and policy enforcement platforms. This includes the integration of system, network, event, and user access logs into the SIEM platform. It also includes integration into our vulnerability, compliance, inspection, and data scanning systems.

- Consultant will provide General Project Management services in support of the Technologies Project Management Office (PMO).

- Consultant presents regular status reports to supervisor and other key stakeholders; presents required project information at project gate reviews; submits project status reports.

- Consultant acts in an ethical and respectful manner at all times. Consultant acts in accordance with DIA standards of professional conduct & integrity.

- Consultant performs other duties as assigned or requested.

Employee Name: _____
Vendor Name: _____
Contract No. <u>201XXXXXX</u>

14.   Performance Criteria and Deliverables: Consultant's performance will be evaluated by Client on at least a
        bi-annual basis, using the following criteria:

- Professional Conduct:
  Consultant acts in an ethical and respectful manner at all times. Consultant acts in accordance with DIA
  standards of professional conduct & integrity.

- SLA achievement:
  Ticket resolution is achieved within SLA parameters

- Change requests:
  Volume and quality of change requests

- Documentation:
  Volume and quality of documentation produced

- Incident Monitoring and ESMC participation:
  Actively participates in the DIA monitoring center (ESMC), and regularly tracks and investigates security
  related incidents (by volume and thoroughness of investigation

If any conflict should arise between this work order and the Contract, the contract overrides this work order and its
content.

Vendor Representative: **Denver International Airport**

By: _____

Title: _____

Date: _____   Title: Budget and Procurement Supervisor, Technologies

Funding Approval: Fund 81 – 6027 / Program 14

EXHIBIT C

Quantum Secure, Inc.: End-User License Agreement

This END-USER LICENSE AGREEMENT ("Agreement") is entered into by and between Quantum Secure, Inc., a California Corporation with offices located at 100 Century Center Court, Suite 800, San Jose, CA 95112 (as referred to herein as "Licensor" or "Quantum Secure") and the City and County of Denver, a Municipal Corporation (as referred to herein as "You" or "Licensee"). This Agreement is effective upon the date of full execution of the Agreement (the "Effective Date").

THIS AGREEMENT CONSTITUTES THE COMPLETE AGREEMENT BETWEEN YOU AND QUANTUM SECURE.

1. **OWNERSHIP AND ADMINISTRATION OF SOFTWARE**

1.1 **Ownership and Title.** As between the parties, Quantum Secure, and its licensors, own and shall retain all right, title, and interest in and to: (i) the Software including all intellectual property rights embodied therein; (ii) all of the service marks, trademarks, trade names, or any other designations associated with the Software; and (iii) all copyrights, patent rights, trade secret rights, and other proprietary rights relating to the Software. (iv) all "Derivative Work" described as work that is based upon or derived (whether directly or indirectly, or in whole or in substantial part) from product implementation or a copyrighted work, such as a revision, modification, enhancement, translation, portation, abridgment, correction, condensation, addition or expansion of or to the copyrighted work, or any form in which the copyrighted work may be recast, transformed or adapted, which represents an original work of authorship and, if prepared other than in accordance with an express license grant in this Agreement and other express terms of this Agreement, would constitute copyright infringement without limitation, all deliverables, computer programs (source, object and custom code), programming aids and tools, documentation, reports, data provided by Quantum, designs, concepts, know-how, and other information provided by Quantum, whether copyrightable / patentable or not.

1.2 **Administration of Software.** Quantum Secure may include on the media with the Software additional computer programs which are not currently licensed for use by Licensee. Inclusion of such additional computer programs in no way implies a license from Quantum Secure and access or use of such programs is strictly prohibited unless Licensee procures the right to use any such program and the applicable Enabler Code is provided thereto.

2. **LICENSE GRANT**

2.1 **Grant.** Quantum Secure grants to Licensee a nonexclusive, nontransferable, non sub-licensable, perpetual, unless terminated in accordance with the provisions of this Agreement, license (the "License") to (i) use the Software installed in accordance with the Documentation and only on the licensed computer solely for its own internal operations; and (ii) move the Software temporarily in case of computer system malfunction. The License granted under

EXHIBIT C

this Agreement does not constitute a sale of the Software or any portion or copy of it. Licensee may not use the Software on more than one computer system unless otherwise specifically authorized by an explicit Software product, or additional licenses for additional computers are purchased. Rights not expressly granted are reserved by Quantum Secure.

2.2 **Copies.** Licensee may make copies of the Software provided that any such copy is: (i) created as an essential step in utilization of the Software according to this Agreement and is used in no other manner; or (ii) used for archival purposes to back up the licensed computers. All trademark and copyright notices must be reproduced and included on such copies. Licensee may not make any other copies of the Software.

2.3 **Restrictions on use.** Licensee shall not, and shall not aid, abet, or permit any third party to: (i) decompile, disassemble, or otherwise reverse engineer or attempt to reconstruct or discover any source code or underlying ideas or algorithms of the Software by any means whatsoever; (ii) remove any identification, copyright, or other notices from the Software; (iii) provide, lease, lend, use for timesharing or service bureau purposes; (iv) create a derivative work of any part of the Software; or (v) develop methods to enable unauthorized parties to use the Software. If EC law is applicable, the restrictions in Section 3.3 (i) are limited so that they prohibit such activity only to the maximum extent such activity may be prohibited without violating the EC Directive on the legal protection of computer programs. Notwithstanding the foregoing, prior to decompiling, disassembling, or otherwise reverse engineering any of the Software, Licensee shall request Quantum Secure in writing, to provide Licensee with such information or assistance and Licensee shall refrain from decompiling, disassembling, or otherwise reverse engineering any of the Software unless Quantum Secure cannot or has not complied with such request in a commercially reasonable amount of time.

Licensee will not sell, assign or sub-license this license or sell or otherwise transfer the Software or Documentation (or any portion thereof) to any other party except to an affiliate of the Licensee and except with the written consent of Quantum Secure. Licensee will maintain the Software and Documentation ("Confidential Information") in confidence and not disclose any data or other information contained in the Software or Documentation to any party, except for Licensee's employees and agents who require access to the Software for the purposes of Licensee's internal business and only for use in accordance with the terms of this License Agreement. Customer will not use the Software for the provision of time-sharing services to others.

 2.4 **OEM License.** Quantum Secure may OEM or Resell certain software products from third party manufacturers and all such products are subject to strictly this license agreement.

2.5 **Non Disclosure.** Each party will implement appropriate measures, within each party's reasonable discretion, to satisfy its obligation hereunder and, generally, will treat confidential information, including, but not limited to Software and Documentation, with the same degree of care and confidentiality which the recipient party of the confidential information provides for its own confidential information. Since unauthorized transfer, use or disclosure of the Software and Documentation and other confidential information would

EXHIBIT C

diminish their value to Quantum Secure and its suppliers or Licensee, as appropriate, who, may have no adequate remedy at law in the event the recipient of the confidential information materially breaches its obligations under this Agreement, the disclosing party may be entitled to seek injunctive relief, in addition to such other remedies and relief that would be available to them in the event of such a breach. Confidentiality requirements shall not apply to Confidential Information:

a. Already known by the recipient party without an obligation of confidentiality,

b. Publicly known or becomes publicly known through no unauthorized act of the recipient party,

c. Rightfully received from a third party without obligation of confidentiality,

d. Independently developed by the recipient party without use of the other party's Confidential Information,

e. Disclosed without similar restrictions by the owner of the Confidential Information to a third party (other than an affiliate or customer of the party owning the Confidential Information),

f. Approved by the party owning the Confidential Information, in writing, for disclosure, or

g. Required to be disclosed pursuant to a requirement of a governmental agency or law so long as the recipient party provides the other party with timely prior written notice of such requirement.

2.6 **Purchase Orders**. Nothing contained in any purchase order, acknowledgment, or invoice shall in any way modify the terms or add any additional terms or conditions to this Agreement.

2.7 **Updates**. This section applies if the Software acquired is an update to the original Software (the "**Update**"). An Update does not constitute a legally licensed copy of the Software unless purchased as an Update to a previous version of the same Software. The Update may only be used in accordance with the provisions of this Agreement. The Update, together with the original Software, constitutes one (1) legally licensed copy of the Software.

3. SALES, MAINTENANCE AND SUPPORT

3.1 Attached Exhibit 1 describes the maintenance and support policies of Quantum Secure under this contract.

3.2 Attached Exhibit 2 describes the sales terms of Quantum Secure under this contract.

EXHIBIT C

4. **LIMITED WARRANTY**

4.1 **Media and Documentation.** Quantum Secure warrants that if the media or documentations are damaged or physically defective at the time of delivery of the first copy of the Software to Licensee and if defective or damaged product is returned to Quantum Secure within ninety (90) days thereafter, then Quantum Secure will provide Licensee with replacements at no cost.

4.2 **Limited Software Warranty.** Subject to the conditions and limitations of liability stated herein, Quantum Secure warrants for a period of ninety (90) days from the delivery of the first copy of the Software to Licensee that the Software, as delivered, will materially conform to Quantum Secure's then current published Documentation for the Software. This warranty covers only problems reported to Quantum Secure during the warranty period. For customers outside of the United States, this Limited Software Warranty shall be construed to limit the warranty to the minimum warranty required by law. Quantum Secure makes no representations or warranties with respect to third party software and shall not be responsible for any loss of data or other errors resulting from the software's failure to perform.

4.3 **Remedies.** The remedies available to Licensee hereunder for any such Software which does not perform as set out herein shall be either repair or replacement, or, if such remedy is not practicable in Quantum Secure's opinion, refund of the license fees paid by Licensee upon a return of all copies of the Software to Quantum Secure. In the event of a refund this Agreement shall terminate immediately without notice.

4.4 **Virus or Malicious Code.** Quantum Secure warrants that it has exercised commercially reasonable measures to ensure Software does not harm, through virus or other malicious code, Licensee technology or network.

4.5 **Non-infringement.** Quantum Secure warrants that Software does not infringe on any third party intellectual property right and that Quatum Secure has title and authority to license the Software.

EXCEPT AS SET FORTH IN THIS SECTION 4, QUANTUM SECURE DISCLAIMS ANY WARRANTY, EXPRESS OR IMPLIED WITH RESPECT TO THE SOFTWARE OR THE DOCUMENTATION OR THEIR OPERATION OR USE PROVIDED IN CONNECTION THEREWITH WILL BE UNINTERRUPTED OR IS ERROR FREE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE OR USE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTEIS, SO THE ABOVE EXCLUSION DOES NOT APPLY IN SUCH STATES. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE.

5. **LIMITATION OF LIABILITY**

5.1 **Limited Liability.** QUANTUM SECURE AND ITS SUPPLIERS, EMPLOYEES, AGENTS, RESELLERS, OEM PARTNERS, DEALERS AND FRANCISEES WILL IN NO EVENT OTHER THAN GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, OR OTHER DIRECT OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION OR THE LIKE, DAMAGES FOR THE INABILITY TO USE EQUIPMENT OR ACCESS DATA) SUFFERED BY LICENSEE, ANY OF ITS EMPLOYEES OR AGENTS OR ANY OTHER PERSON ARISING OUT OF OR IN CONNECTION WITH THE USE OR INABILITY TO USE THE SOFTWARE OR THE

EXHIBIT C

DOCUMENTATION, OR THE MAINTENANCE OR SUPPORT THEREOF AND BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF QUANTUM SECURE OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

Quantum Secure neither assumes nor authorizes any employee, agent, dealer or franchisee to assume for Quantum Secure any other liability in connection with the license, use of performance of the Software or Documentation.

Licensee is solely responsible for the selection of the Software to achieve Licensee's intended results, for the conformity of the computer on which the Software is run to Quantum Secure's specifications or requirements and for the maintenance of such computer in good working order and repair.

THE FOREGOING LIMITATIONS ON LIABILITY ARE INTENDED TO APPLY TO THE WARRANTIES AND DISCLAIMERS ABOVE AND ALL OTHER ASPECTS OF THIS EULA.

5. **TERM AND TERMINATION**

5.1 **Term**. The term of this Agreement is perpetual unless terminated in accordance with its provisions.

5.2 **Termination**. Either party may terminate this Agreement upon thirty (30) days written notice in the event of the breaching party's failure to cure breach within twenty (20) days of receipt of notice of breach from the non-breaching party.

5.3 **Termination for Convenience.** Licensee may terminate this Agreement and the SSA attached as Exhibit "A", without cause and without penalty, at any time upon the provision of sixty (60) days prior written notice to Quantum Secure of intent to terminate.

5.4 **Effect of Termination**. Upon termination of this Agreement, Licensee agrees to cease all use of the Software and to return to Quantum Secure or destroy the Software and all Documentation and related materials in Licensee's possession, and so certify to Quantum Secure. Except for the License granted herein and as expressly provided herein, the terms of this Agreement shall survive termination.

6. **PAYMENT; TAXES**

6.1 **Payment.** All undisputed amounts payable hereunder are due at net thirty (net 30) term, unless otherwise specified herein. Quantum Secure reserves the

EXHIBIT C

right to charge 1.5% / month late fee on any unpaid balance not reasonably disputed by Licensee.

6.2 **Increases**. Unless otherwise specified in this agreement, Quantum Secure's fees for maintenance services may be increased on each annual anniversary of the Effective Date provided that the fees after any such increase shall not exceed the lesser of: (i) five percent (5%) over the amounts charged in the preceding year, or (ii) United States CPI Index for the previous year.

6.3 **Taxes**. Licensee agrees to pay all taxes levied upon the Software and any services based upon their use hereunder, exclusive, however, of taxes based on Quantum Secure's income, which taxes shall be paid by Quantum Secure.

7. **U.S. GOVERNMENT RIGHTS**

7.1 **Restricted Rights**. The Software and Documentation are provided with restricted rights. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraphs (b)(3)(ii) and (c)(1)(ii) of the Rights in Technical Data and Computer Software Clause of Department of Defense Federal Acquisition Supplement (DFARS) 252.227-7013 or in subparagraph (g)(3)(i) of Federal Acquisition Regulations (FAR) 52.227-14, Alternate III as applicable.

8. **MISCELLANEOUS**

8.1 **Governing Law**. This Agreement shall be governed by the laws of the State of Colorado, without regard to the principles of conflict of laws or the United Nations Convention on Contracts for the International Sale of Goods.

8.2 **Export and Import Controls**. Regardless of any disclosure made by Licensee to Quantum Secure of an ultimate destination of the Products, Licensee will not directly or indirectly export or transfer any portion of the Software, or any system containing a portion of the Software, to anyone outside the United States (including further export if Licensee took delivery outside the U.S.) without first complying with any export or import controls that may be imposed on the Software by the U.S. Government or any country or organization of nations within whose jurisdiction Licensee operates or does business. Licensee shall at all times strictly comply with all such laws, regulations, and orders, and agrees to commit no act which, directly or indirectly, would violate any such law, regulation or order.

8.3 **Software Delivery:** Quantum Secure delivers all software and documentation via electronic FTP download.

8.4 **Assignment**. Quantum Secure may assign or otherwise transfer any or all of its rights and obligations under this Agreement upon notice to Licensee in an event of change of control.

8.5 **Sole Remedy and Allocation of Risk**. Licensee's sole and exclusive remedies are set forth in this Agreement. This Agreement defines a mutually agreed-upon allocation of risk, and the License price reflects such allocation of risk.

8.6 **Equitable Relief**. The parties agree that a breach of this Agreement adversely affecting Quantum Secure's intellectual property rights in the Software may cause irreparable injury to Quantum Secure for which monetary damages may not be an adequate remedy and Quantum Secure shall be entitled to equitable relief in addition to any remedies it may have hereunder or at law.

EXHIBIT C

8.7 **No Waiver**. Failure by either party to enforce any provision of this Agreement will not be deemed a waiver of future enforcement of that or any other provision, nor will any single or partial exercise of any right or power hereunder preclude further exercise of any other right hereunder.

8.8 **Severability**. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or portion thereof, to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.

8.9 **Audit Rights**. Quantum Secure shall have the right to periodically audit at times and in manners agreed to by Licensee (or to request a report from the Licensee which report will be due fifteen days from the written (letter or email) request from Quantum Secure) the total number of active identities (employees, contractors and physical access cardholders) managed by Quantum Secure software in the records of the Licensee during normal business hours and upon reasonable notice to the Licensee, to verify compliance with the licensing and payment provisions of this Agreement. Licensee shall not unreasonable deny Quantum Secure an opportunity to audit hereunder.

8.10 **Publicity / News**. Intentionally Deleted.

9. **ENTIRE AGREEMENT**

9.1 This Agreement sets forth the entire understanding and agreement between the parties and may be amended only in a writing signed by authorized representatives of both parties. No vendor, distributor, dealer, retailer, sales person, or other person is authorized by Quantum Secure to modify this Agreement or to make any warranty, representation, or promise which is different than, or in addition to, the warranties, representations, or promises made in this Agreement. No prior agreements, terms or preprinted purchase orders shall in any way modify, replace, or supersede the terms of this Agreement.

EXHIBIT C

Exhibit 1

Software Support Agreements (SSA) and Software Maintenance

Quantum Secure offers standard software system support coverage for all their products. This Agreement sets forth the terms and conditions under which Quantum Secure shall maintain its Software Products which have been properly purchased, licensed or sub-licensed to the Customer.

1.0 Maintenance of Software
Beginning on the day of the execution of this agreement, Quantum Secure shall provide the following error-correction, bug fixing and software support services:

(a) telephonic support during the defined days and hours of business operation as per below. Such support shall include consultation on the operation and utilization of the Software.

(b) software error / bug correction services, consisting of Quantum Secure's using all reasonable efforts to design, code and implement programming changes to the Software, and modifications to the documentation, to correct reproducible errors therein so that the Software is brought into substantial conformance with the Specification.

(c) copyrighted software patches, updates, new releases and new versions of the Software, including the PACS agents deployed along with other generally available technical material. Under this agreement, Quantum Secure will release the new PACS agent for the newer release of the PACS (Physical Access Control Systems) software within six months of the new version of that PACS being commercially available in the market by the PACS manufacturer.

The Licensee must inform Quantum Secure at least 90 days before any scheduled upgrades to the SAFE connected systems, such as PACS, IDMS, etc. for receiving appropriate software upgrade. In case Quantum Secure cannot get hold of the newer version of the PACS or any other software from the market / from the original manufacturers, then Quantum Secure will be allowed to develop the upgrade of its software against the copy of the new version of the PACS or any other software belonging to the Licensee.

In order to provide timely support under this support agreement, the Licensee must provide a convenient remote access authorization to Quantum Secure support team to the servers where Quantum Secure products are installed. Without an uninterrupted access to these servers, the support process may be delayed and could lead to longer time for problem diagnostics and resolution.

2.0 Exceptions
Quantum Secure Software Support Agreement does not cover operating systems, backup and/or restoration of the Quantum Secure SOFTWARE and/or associated data, reinstallation of the SOFTWARE on a different or repaired computer, SOFTWARE tampering in any form, accounting issues, Database issues, Internet connection issues, viruses, spy ware, networking issues, hardware or any other third party software or device issues. While we will do our best to help, support of these uncovered issues may incur additional charges on a per incident basis. Software updates does not cover any required data conversion; operating systems, hardware, additional training, government initiated changes which require software programming changes, pre-printed form layouts or the conversion and/or adaptation of any Licensee requested modifications or reports

EXHIBIT C

3.0 Term
This SSA shall be coterminous with the Agreement between the parties, City
and County of Denver Contract Number PLANE201523684. Licensee may terminate
this SSA at
any time without penalty upon sixty (60) days prior written notice to Quantum
Secure. This SSA may also be terminated by Quantum Secure if the Customer
defaults in the payment of any monies due under this SSA and fails to remedy
the default within 15 days after written notice or in the event of a breach
by Licensee of any other provision of this SSA.

4.0 Intentionally Deleted.

5.0 Fees & Payments
The support fees will be invoiced annually up to 30 days in advance of the
renewal date and invoices are payable 30 days after receipt of invoice by the
Customer. In the event that the agreement is not terminated at the end of a
running one year term, the Customer is responsible for ensuring that the
appropriate customer purchase order is sent to Quantum Secure, if your
company requires a PO to pay the invoice.

Late payment of undisputed invoices after the due date on the invoice or
after the start date of the new term may be subject to 1.5% per month late
charges. The Support services and benefits are suspended upon the expiration
of the current Software Support Agreement term if the payment is not received
by that time.

Standard Service is our standard support coverage option. It provides
telephone support and assistance from our Licensee Support Center during
normal support hours (Mon – Fri, 9:00 a.m. – 5:00 p.m. PST) as well as
software upgrades if and when available.

Responses to the Licensee's support issues require the Licensee to provide
adequate information and documentation to enable Quantum Secure to recreate
the problem. Quantum may notify the Licensee that the problem could not be
recreated, located or identified, if such is the case. If the reported
problem is unrelated to Quantum Secure's installed products, Quantum Secure
may notify Licensee that the problem will not be resolved and the reason for
this decision. Notwithstanding the provisions of this section, Quantum Secure
makes no warranties that the Support Services provided hereunder will be
successful in resolving all difficulties or problems or in diagnosing all
faults.

Licensee must maintain a functional Internet connection and dial-in (or log
in via VPN) capabilities during business hours for any on-line support.
Licensee must make sufficient daily, weekly and monthly backups.

NOTE: It is our policy to support the current version of each software
product and one full version back. All support calls for products not under
Warranty or SSA are subject to T &M charges or will be directed to purchase a
SSA.

More details on our support process is available via Quantum Secure published
Customer Care documentation which is included (and is downloadable from your
customer care site) with the shipment of your products.

The Licensee's Role
The provision of the error correction and support services described above
shall be expressly contingent upon the Licensee's reasonable cooperation in

EXHIBIT C

providing all relevant information about the errors, promptly reporting any errors in the Software or related documentation to the Quantum Secure's Support Department, providing adequate remote access and not modifying the Software without the written consent from Quantum Secure.

6.0 Limitation of Liability

QUANTUM SECURE AND ITS SUPPLIERS, EMPLOYEES, AGENTS, RESELLERS, OEM PARTNERS, DEALERS AND FRANCISEES WILL IN NO EVENT OTHER THAN QUANTUM SECURE'S GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION OR THE LIKE, DAMAGES FOR THE INABILITY TO USE EQUIPMENT OR ACCESS DATA) SUFFERED BY LICENSEE, ANY OF ITS EMPLOYEES OR AGENTS OR ANY OTHER PERSON ARISING OUT OF OR IN CONNECTION WITH THE USE OR INABILITY TO USE THE SOFTWARE OR THE DOCUMENTATION, OR THE MAINTENANCE OR SUPPORT THEREOF AND BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF QUANTUM SECURE OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

Quantum Secure neither assumes nor authorizes any employee, agent, dealer or franchisee to assume for Quantum Secure any other liability in connection with the license, use of performance of the Software or Documentation.

Quantum Secure will undertake all reasonable efforts to provide technical assistance under this SSA and to rectify or provide solutions to problems where the Software does not function as described in the Software documentation, but Quantum Secure does not guarantee that the problems will be solved or that any item will be error-free. This SSA is only applicable to Quantum Secure's Software running under the certified environments specified in the release notes for that product.

Software Support Agreements

Services	Standard
Telephone Support Silver Level Mon – Fri, 9:00 a.m. – 5:00 p.m. (PST) Gold Level 24x7	**X**
If & when available, Software Maintenance and/or Enhancement Release Updates (Software Upgrades)	**X**

7.0 Software System Support

Standard Software Support Agreement (SSA) coverage, as listed, is in force for the customer after the initial warranty period. In addition, systems integrators opting to purchase support services on an "as needed" basis only, may do so at prevailing **Time and Materials Rates (T&M).** Quantum Secure requires a signed Purchase Order prior to providing T & M support services. If the end user requires on-site installation of the software upgrades from Quantum Secure, then the end-user may do so at the prevailing time and material rates from Quantum Secure. Licensee will reimburse Quantum Secure for the actual cost of reasonable, documented travel and living expenses of the support representative, and pre-approved by Licensee for on-site activity

EXHIBIT C

outside of normal support.

8.0 Telephone Technical Support
During the Agreement, Quantum Secure will only accept service calls from the
end –user or the employees of the Systems Integrator of Record for the
specific installation to which the support inquiry relates. The standard
technical support telephone number is (800) 776-3414. The preferred way to
report issues is through our web site:
http://support.quantumsecure.com/Login.asp

This SSA may be modified only in writing by authorized representatives of
Quantum Secure, Inc. and the Customer.

NOTE: Quantum Secure does not guarantee defects will be fixed in any specific
time duration due to the nature of software operating in a multi-vendor
environment. It is the goal of Quantum Secure to deliver our best effort to
satisfactorily resolve each incident using the best judgment under each
circumstance.

EXHIBIT C

Exhibit 2

Sales Terms

All Terms are subject to this entire License Agreement.

CITY AND COUNTY OF DENVER
INSURANCE REQUIREMENTS FOR THE DEPARTMENT OF AVIATION

Certificate Holder Information:

CITY AND COUNTY OF DENVER
Attn: Risk Management, Suite 8810
Manager of Aviation
Denver International Airport
8500 Peña Boulevard, Room 8810
Denver CO 80249

CONTRACT NAME & NUMBER TO WHICH THIS INSURANCE APPLIES: 201523684 – Identity Management – BadgeEze Replacement

I.   MANDATORY COVERAGE

Colorado Workers' Compensation and Employer Liability Coverage

Coverage: COLORADO Workers' Compensation

Minimum Limits of Liability (In Thousands)

WC Limits: $100, $500, $100

And Employer's Liability Limits:

Any Policy issued under this section must contain, include or provide for the following:
1. All States Coverage or Colorado listed as a covered state for the Workers' Compensation
2. Waiver of Subrogation and Rights of Recovery against the City and County of Denver (the "City"), its officers, officials and employees.
3. State Of Colorado law states that if a contractor is a sole proprietor, they are not required to have Workers Compensation coverage.

Commercial General Liability Coverage

Coverage: Commercial General Liability (coverage at least as broad as that provided by ISO form CG0001 or equivalent)

Minimum Limits of Liability (In Thousands):

Each Occurrence: $1,000
General Aggregate Limit: $2,000
Products-Completed Operations Aggregate Limit: $2,000
Personal & Advertising Injury: $1,000

Any Policy issued under this section must contain, include or provide for the following:
1. City, its officers, officials and employees as additional insureds, per ISO form CG2010 and CG 2037 or equivalents.
2. Coverage for defense costs of additional insureds outside the limits of insurance, per CG0001.
3. Liability assumed under an Insured Contract (Contractual Liability).
4. The full limits of coverage must be dedicated to apply to this project/location, per ISO form CG2503 or equivalent.
5. Waiver of Subrogation and Rights of Recovery, per ISO form CG2404 or equivalent.
6. Separation of Insureds Provision required
7. General Aggregate Limit Applies Per: Policy ___Project ____Location_____, if applicable

Business Automobile Liability Coverage

Coverage: Business Automobile Liability (coverage at least as broad as ISO form CA0001)

Minimum Limits of Liability (In Thousands):   Combined Single Limit $1,000

> **Any Policy issued under this section must contain, include or provide for the following:**
> 1. Symbol 1, coverage for any auto. If no autos are owned, Symbols 8 & 9, (Hired and Non-owned) auto liability.
> 2. If this contract involves the transport of hazardous cargo such as fuel, solvents or other hazardous materials may occur, then Broadened Pollution Endorsement, per ISO form CA 9948 or equivalent and MCS 90 are required.

II. ADDITIONAL COVERAGE

Umbrella Liability

Coverage:

Umbrella Liability, Non Restricted Area
Minimum Limits of Liability (In Thousands)

Umbrella Liability Controlled Area	Each Occurrence and aggregate	$9,000
Umbrella Liability Non-Controlled Area	Each Occurrence and aggregate	$1,000

> **Any Policy issued under this section must contain, include or provide for the following:**
> 1. City, its officers, officials and employees as additional insureds.
> 2. Coverage in excess of, and at least as broad as, the primary policies in sections WC-1, CGL-1, and BAL-1.
> 3. **If operations include unescorted airside access at DIA, then a $9 million Umbrella Limit is required.**

Professional Liability Information Technology Contracts

Coverage: Professional Liability including Cyber Liability for Errors and Omissions
(If contract involves software development, computer consulting, website design/programming, multi-media designers, integrated computer system design, data management, and other computer service providers.)

Minimum Limits of Liability (In Thousands)   Per Claim $1,000

> **Any Policy issued under this section must contain, include or provide for the following:**
>
> 1.   The insurance shall provide coverage for the following risks:
>
>   a. Liability arising from theft, dissemination and / or use of confidential information (a defined term including but not limited to bank account, credit card account, personal information such as name, address, social security numbers, etc. information) stored or transmitted in electronic form
>
>   b. Network Security Liability arising from the unauthorized access to, use of or tampering with computer systems including hacker attacks, inability of an authorized third party, to gain access to your services including denial of service, unless caused by a mechanical or electrical failure
>
>   c. Liability arising from the introduction of a computer virus into, or otherwise causing damage to, a customer's or third person's computer, computer system, network or similar computer related property and the data, software, and programs thereon.
>
> 2.   Policies written on a claims-made basis must remain in full force and effect in accordance with CRS 13-80-104. The Insured warrants that any retroactive date under the policy shall precede the effective date of this Contract; and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of two (2) years beginning at the time work under the Contract is completed.
>
> 3   Any cancellation notice required herein may be provided by either certified or regular mail.
>
> 4.   The policy shall be endorsed to include the City, its elected officials, officers and employees as additional insureds with respect to liability arising out of the activities performed by, or on behalf of the Insured
>
> 5.   Coverage must include advertising injury, personal injury (including invasion of privacy) and intellectual property offenses related to internet.

III. ADDITIONAL CONDITIONS

It is understood and agreed, for the benefit of the City, that the following additional conditions shall apply to all coverage specified herein

- All coverage provided herein shall be primary and any insurance maintained by the City shall be considered excess.
- With the exception of professional liability and auto liability, a Waiver of Subrogation and Rights of Recovery against the City, its officers, officials and employees is required for each coverage period.
- The City shall have the right to verify or confirm, at any time, all coverage, information or representations contained herein, and the insured and its undersigned agent shall promptly and fully cooperate in any such audit the City may elect to undertake.
- Advice of renewal is required.
- With the exception of Workers Compensation, all insurance companies issuing policies hereunder must carry at least an A -VI rating from A.M. Best Company or obtain a written waiver of this requirement from the City's Risk Administrator.
- Compliance with coverage requirement by equivalent herein must be approved in writing by the City's Risk Administrator prior to contract execution.
- No changes, modifications or interlineations on this document shall be allowed without the review and approval of the Risk Administrator prior to contract execution.

NOTICE OF CANCELLATION

It is understood and agreed that should any Policy issued hereunder be cancelled or non-renewed before the expiration date thereof, or sustain a material change in coverage adverse to the City, the issuing company or its authorized Agent shall give notice to the Department of Aviation in accordance with policy provisions.