REQUEST FOR PROPOSAL

for

Identity Management System at Oakland International Airport

21-22/33

PORT OF OAKLAND

PURCHASING DEPARTMENT
530 WATER STREET
OAKLAND, CA 94607

PORT OF OAKLAND

REQUEST FOR PROPOSAL

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

The Port of Oakland (the "Port"), through its Purchasing Department, is hereby soliciting competitive proposals for the above-mentioned project. The successful Respondent will be required to furnish all labor, material, equipment, supplies, applicable taxes, insurance, bonding, and licenses to complete this project.

Proposal Information

Proposal Title	Identity Management System at Oakland International Airport
Proposal Type	Professional Services
Proposal Number	21-22/33
Proposal Issued	February 4, 2022
Department Requesting Services	Aviation Security
Pre-proposal Meeting	N/A
Scheduled Publication Date	February 4, 2022
Proposal Due Date	**March 17, 2022 until 11:00 a.m.**

Instructions for Submitting Proposals

Submittal Address	Port of Oakland Purchasing Department Attn: **Nickulaus Sioson** 530 Water Street Oakland, CA 94607
Submittal Copies	One (1) Original copy clearly marked "Original" and five (5) Copies marked "Copy". An electronic file of the Proposal shall be submitted as a single file in Adobe® portable document format (pdf) contained on a single USB flash drive.
Submittal Envelope Requirements	Proposal must be sealed and have the following information clearly marked and visible on the outside of the envelope: • Proposal Number • Name of Your Company • Address • Phone Number
Late Submittals	Proposals received after the time and date stated above shall be returned unopened to the Respondent.

How to Obtain Proposal Documents

Copies of the Proposal documents may be obtained at:

Location	Address
Website	http://www.portofoakland.com/business/bids-rfps/ Or navigate to the Port of Oakland's main website at: http://www.portofoakland.com/, then click on "Bids/RFPs" from the banner on the top of the page, and then scroll down to download the Bid.
Purchasing Department	Please call Nickulaus Sioson at (510) 627-1140 or email nsioson@portoakland.com for any issues downloading Bid document from Port website or to request an email copy.

Questions about the Proposal

Questions and/or Requests for Information (RFI) must be submitted in writing and can be submitted by email as follows:

Primary Contact	Nickulaus Sioson Email: nsioson@portoakland.com
Question/RFI Due Date	**February 18, 2022 until 4:00 p.m.** Please submit questions as soon as possible. No questions regarding the specifications will be responded to after the above date. All pertinent questions will be responded to and answered in writing no later than the Response Date listed below.
Response Date	**February 24, 2022** All pertinent questions will be responded to **via addendum** faxed (or emailed) to all prospective proposers and placed on the Port's website. Proposers who did not receive a copy of the addendum should download it from the Port's website. See the "How to Obtain Proposal Documents" section for our web address. All addenda must be acknowledged on the RFP Acknowledgement and Signature form.

Once the RFP is issued, and until a recommendation for award is made to the Board of Port Commissioners at a public Board of Port Commissioners meeting (or in cases where a recommendation for award does not require a public Board meeting, when Proposers are notified by Port staff of the recommendation for award), each Proposer and its representatives, agents, and affiliates, shall not contact members of the Evaluation Committee, Port staff or the Board of Port Commissioners to discuss or ask questions about the contents of this RFP or the selection process. All questions shall be submitted in writing as described in this RFP. Any inappropriate contact by a Proposer, its representatives, agents, and/or affiliates may result in the Proposers' proposal being disqualified.

Full Opportunity

The Port's policy prohibits discrimination or preferential treatment because of race, color, religion, sex, national origin, ancestry, age (over 40), physical or mental disability, cancer-related medical condition, a known genetic pre-disposition to a disease or disorder, veteran status, marital status, or sexual orientation. It is the policy of the Port of Oakland to encourage and facilitate full and equitable opportunities for small

local businesses to participate in its contracts for the provision of goods and services. It is further the Port's policy that no discrimination shall be permitted in small local business participation in Port contracts or in the subcontracting of Port contracts. The successful Respondent shall comply with the Port's non-discrimination policy.

Title VI Solicitation Notice: The Port of Oakland, in accordance with the provisions of Title VI of the Civil Rights Act of 1964 (78 Stat. 252, 42 U.S.C. §§ 2000d to 2000d-4) and the Regulations, hereby notifies all bidders that it will affirmatively ensure that any contract entered into pursuant to this advertisement, disadvantaged business enterprises will be afforded full and fair opportunity to submit bids in response to this invitation and will not be discriminated against on the grounds of race, color, or national origin in consideration for an award.

The Port reserves the right to reject any or all proposals, to waive any irregularities or informalities not affected by law, to evaluate the proposals submitted, and to award the contract according to the proposal which best serves the interests of the Port.

John Banisadr,
Port Purchasing Manager

Table of Contents

Attachments:

Title		Must Be Returned with Proposal
1	Non-Collusion Declaration	Yes
2	Statement of Equal Employment Opportunity	Yes
3	RFP Acknowledgement and Signature Form	Yes
4	Proposal Worksheet	(See attachment 13)
5	Port of Oakland Non-Discrimination and Small Local Business Utilization Policy A. Chart for Submitting Data for Calculation of Preference Points B. Local Participation Questionnaire C. Monthly Utilization of Local and Small Business Enterprises D. Final Utilization of Local and Small Business Enterprises	Yes Attachment 5-A and 5-B are required with the Proposal. (Note: If you are submitting a new Certification Application for preference points, then your completed application is due 7 business days prior to the proposal due date.) Attachments 5-C and –D are required after contract award final completion of the project.
6	Non-Discrimination and Small Local Business Utilization Policy Program Affidavit	Yes
7	City of Oakland City Charter §728 Living Wage Information A. Employer Self-Evaluation for Port of Oakland Living Wage B. Certificate of Compliance—Living Wage	No (Attachment 7-A and 7-B are required after contract award.)

Title		Must Be Returned with Proposal
8	Statement of Living Wage Requirements	Yes
9	Supplier Insurance Requirements	No
10	Insurance Acknowledgement Statement	Yes
11	Standard Professional Services Agreement	No (Note: If awarded the contract, the successful Respondent will execute a revised version of the Port's standard Professional Services Agreement, which will be consistent with the provisions of this RFP.)
12-1	IdMS Citation Requirements	No
12-2	OAK Existing Business Process	No
12-3	OAK IdMS Specifications and Technical Specifications Compliance Matrix	Yes
13	OAK IdMS Pricing Sheet	Yes
14	OAK ID Badging Office Acceptable Document List	No

I. Project Overview

The Port of Oakland (Port) is soliciting proposals from qualified firms for a comprehensive and automated Identity Management System (IdMS) at the Oakland International Airport (Airport). The main functions of the system will be to issue Airport Identification (ID) badges and manage vehicle permits, keys, and citations. The primary objectives of the IdMS are to enforce business rules for badge issuance; maintain compliance with the Transportation Security Administration's (TSA) regulations and Security Directives (SD); reduce repetitive, manual, time consuming, error prone data entry into multiple standalone systems; improve customer service; and achieve a paperless records management process. For reference, please see **Attachment 12-2**: OAK Existing Business Process, and **Attachment 12-3:** OAK IdMS Specification and Technical Specifications Requirements Compliance Matrix. The Port plans to award a contract for up to 7 years comprised of:

- 2-year Implementation Period for IdMS implementation;
- 2-year Maintenance and Support Period, which includes the 1-year Warranty (Warranty to commence after System acceptance by the Port); and
- Three (3) additional one-year extensions of the Maintenance and Support Period, to be exercised at the Port's sole option.

About the Port of Oakland
The Port of Oakland was established in 1927 and oversees the Oakland seaport, Oakland International Airport, Commercial Real Estate, and 20 miles of waterfront. The Oakland seaport is one of the top ten busiest container ports in the U.S.; Oakland International Airport is the second largest San Francisco Bay Area airport offering over 300 daily passenger and cargo flights; and the Port's real estate includes commercial developments such as Jack London Square and hundreds of acres of public parks and conservation areas. Together, through Port operations and those of its tenants and users, the Port supports nearly 73,000 jobs in the region and over 827,000 jobs across the United States. The Port is an independent department of the City of Oakland.

II. Scope of Services

The Port is seeking a comprehensive and automated Identity Management System (IdMS) for issuing Airport Identification badges with access to Sterile, Secured, and Security Identification Display Area (SIDA) areas; and keys with access to restricted areas of the Oakland International Airport (OAK). The Aviation Security Department (AVSEC) is sponsoring this solicitation. The ID Badging Office, part of AVSEC, currently manages approximately 6,500 active badges. Badge holders include employees of the Port, airlines, tenants, contractors, concessionaires, consultants, and government (local, State, and Federal) agencies. The ID Badging Office handles approximately 75-80 transactions per day. These transactions include processing new and renewal badge applicants and issuing replacement badges, cyber and metal keys, and ramp permits.

ID Badging Office staff will be the primary users and administrators of the IdMS. Authorized Signers will be another key user group. The Airport has approximately 425 Authorized Signers (AS) who act as a tenant's or agency's representative(s) and have the authority to make decisions on behalf of their company's or agency's sponsored badge holders. A company's AS is also the main point of contact for the ID Badging Office. One main function of the AS is to work with badging applicants to complete the badging process. The current badging process involves paper application form(s) to be filled out by the employee / badge applicant, and reviewed and signed by the AS. The application is then entered by the ID Badging Office staff in multiple standalone systems that provide specific functions: background checks, training, financial (Point of Sale (PoS) and receipt printer) and access control. Excel logs are used for tracking and managing ramp permits and keys.

To ensure a smooth transition between existing and future operations, the IdMS will need to integrate, at a minimum, with the existing Crossmatch fingerprint systems (we are open to other technology), TSA Designated Aviation Channeling (DAC) service provider (Telos ID), Learning Management system (SSi), access control system (C•CURE 9000), and cyber keys (Videx CyberLock). The Port is seeking a single

IdMS contractor to provide all software, software customization, training, badging hardware, and related maintenance services necessary for an IdMS.

The primary objectives of the IdMS are:

1. Enforce business rules for badge issuance.
2. Comply with the Transportation Security Administration (TSA) regulations and Security Directives (SD), FAA Safety Training requirements (Part 139).
3. Improve data integrity by reducing manual, time consuming, error prone and duplicate data entry in multiple standalone systems.
4. Improve financial tracking of badge and permit fees.
5. Provide online browser-based interface for Authorized Signatories and applicants to submit badge applications.
6. Improve customer service (e.g., reduced wait times in the ID Badging Office, increase appointment volume).
7. Achieve a paperless process.

To meet the objectives listed above, the Port has developed a "Concept of Operations" described below. The Concept of Operations provides a general description of the overall concept for the IdMS and articulates some of the Port's expectations for how the IdMS will operate at the Airport, how it should benefit the Airport (Changes to Existing Roles, Systems and Process), the architectural components of the system, the functional characteristics of the system, and operating procedures and implementation approach. The successful Respondent should achieve and address the expectations described below, including those described in all Attachments, which contain more specific features of the IdMS.

IdMS CONCEPT OF OPERATIONS

1. IdMS System Architecture

1.1 High-Level System Architecture

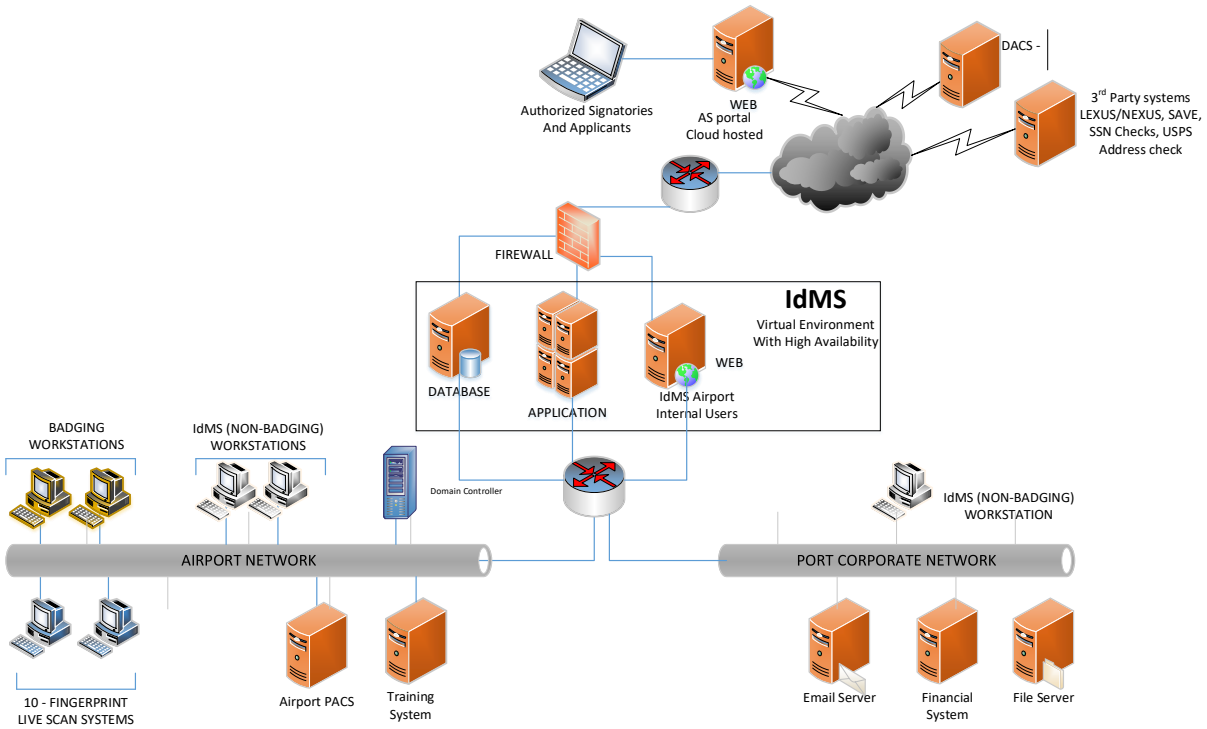


Figure 1: Proposed IdMS System Architecture

Figure 1 above generally displays the type of system architecture and connections OAK expects from an IdMS. Figure 1 represents an IdMS in a virtual environment that consists of an application, database, and web servers allowing for high availability. The application, database, and web servers are scaled according to the performance, transactions / throughput in the ID Badging Office, and concurrent logged-in users. The user groups that access the IdMS can be categorized into internal users (ID Badging Office, AVSEC, operations, admin, IT staff) and external users (Authorized Signer, applicants, U.S. Customs and Border Protection ("CBP")).

Most of the application systems used – such as the physical access control systems, LiveScan systems, file servers and badging workstations – will operate over the Airport network. The Port enterprise systems, such as email servers, operate over the Port's Corporate IT network. Figure 1 also indicates the connection points from IdMS to internal systems (e.g., PACS, financial) and external systems (e.g., DAC, training).

1.2 Badging Workstation Layout

In addition to the server and network system level components in Figure 1 above, the other critical components for the IdMS is the badging workstation and peripherals. These peripherals allow the Trusted Agent to capture information from Driver License and Passport documents, capture fingerprints for background checks, etc. Figure 2 depicts the required components and connections of the badging workstation layout. The Port will provide existing hardware for each badging workstation, which the successful Respondent will fully maintain, upgrade (as necessary), and utilize for the IdMS.

Figure 2: New IdMS Badging Workstation

The ID Badging Office will require seven (7) fully equipped badging workstation setups, one (1) additional setup for testing purposes. Equipment required for each work station:

a. Badge Printer (Networked)	Quantity 5
b. LiveScan	Quantity 7
c. Camera	Quantity 7
d. Multi-page Document Scanner	Quantity 7
e. DL/Passport Scanner	Quantity 7

2. Functional Characteristics

To meet OAK's objectives for an IdMS, the system will need to adhere to the high level of functional characteristics identified below and indicated in **Attachment 12-3:** OAK IdMS Specification and Technical Specifications Requirements Compliance Matrix. The successful Respondent should provide an IdMS that meets the following list of functional capabilities:

A. The IdMS shall have the capability to track each person (applicant or badge holder) as a uniquely identified entity; associating it with related activities such as employers, documents, fingerprints, security checks, training records, badges, keys, etc.

B. The IdMS shall enforce and prevent physical badge issuance (i.e., printing badges) until all applicable procedures (e.g., employment verification, I-9 documents, CHRC/STA, training) have been successfully completed.

C. The IdMS shall comply with all applicable laws, regulations, rules, procedures, and standards, including any of their updates and amendments ("Governing Standards"). The Governing Standards include, without limitation, federal airport security regulations as outlined in the Code of Federal Regulations (CFR) Title 49 Chapter XII Part 1542, active aviation security policy enforcement (e.g., those promulgated with Transportation Security Administration (TSA) regulations and Security Directives (SD) 1542-04-08O), and with any subsequent updates or new laws or regulations that apply to the activities of the IdMS. The Governing Standards also include, without limitation, all laws and regulations governing privacy, consumer protection, handling of financial and personal information, and data security.

D. The IdMS shall be intuitive and easy to follow, requiring minimum training. The user interface shall drive the user to completing relevant tasks and clearly display next step and missing mandatory information.

E. The IdMS shall provide the capability to mask all or specific Personal Identifiable Information (PII) (e.g., SSN) and non-PII (e.g., PIN) data fields for display after initial input, consistent with the Governing Standards.

F. All data in the IdMS shall be encrypted in transit and at rest, using Transparent Data Encryption (TDE), consistent with the Governing Standards.

G. The IdMS shall integrate with the existing:

   i. Fingerprint systems CrossMatch (the Port will consider recommendations for new technology);

   ii. Designated Aviation Channeling (DAC) Service (Telos ID);

   iii. Learning Management system (SSi);

   iv. Physical access control system (CCURE • 9000);

   v. Cyber keys (Videx CyberLock);

vi. The IdMS shall assign a Unique Person ID (UPI) for each person employed at the airport. This ID will be used across all systems and will remain constant for that person.

H. The IdMS shall provide configuration of business rules driven by regulatory and operational requirements, including the Governing Standards.

I. The IdMS shall provide capability for the Authorized Signer to perform, at a minimum, the following functions for any and all companies the Authorized Signer is assigned to:

   i. Enroll new applicants.

   ii. Authorize renewal of badges, replacement of badges, badge management (including de-activation).

   iii. Manage company information including updates to personal and insurance contract information.

   iv. Request access levels, keys, and permits.

   v. Respond to badge audits.

J. The IdMS shall include a cloud-based web portal that allows applicants to pre-submit the badge application online and the Authorized Signer to review and submit the badge application.

K. The IdMS shall enable the association of scanned documents, with the badge application and other functions in document management systems. IdMS must accommodate for all identification types shown in **Attachment 14:** OAK ID Badging Office Acceptable Documents List.

L. The IdMS shall provide ability to scan, validate, and store breeder documents provided by applicants. Data retrieved from the documents should have the ability to auto-populate fields, reducing keying errors and saving time.

M. The IdMS shall provide the ability to archive, maintain, and destroy electronic documents and badge records automatically and on a preset schedule, following Port records and data retention policies.

N. There should be no material or physical changes required to the existing ID Badging Office or office layout, resulting from implementation of the new IdMS. All equipment should fit within OAK's existing physical floor and desk plan, without modification. Each workstation has a L-shaped desk. The dimensions of the front desk are approximately 20 inches wide by 84 inches long; the dimensions of the side desk are approximately 24 inches wide by 72 inches long. Each workstation has one shelf approximately 12 by 42 inches.

3. Operational Procedures

To meet OAK's objectives for an IdMS, the IdMS will adhere to the high-level operational characteristics indicated in **Attachment 12-3:** OAK IdMS Specification and Technical Specifications Requirements Compliance Matrix. The IdMS should comply with the following four critical proposed workflows described in this section:

1. Company / Vendor/ Tenant Onboarding
2. Badge Application Workflow
3. System User Groups and Privileges
4. Citations – Security and Safety

3.1 Company / Vendor / Tenant Onboarding

The IdMS will provide capability for the ID Badging Office to enter and configure new companies, prior to processing any badge applications. The process is initiated by ID Badging Office staff once an agreement is made between OAK and a company, tenant, vendor, or agency to operate at or around the Airport. The process is a joint effort of new company data submission, IdMS technical processes

and notifications, and ID Badging Office staff approvals. Once all approvals are in place, the badging process can begin.

3.2 Badge Application Workflow

Through this set of applications, applicants provide data to the ID Badging Office and are vetted. During this process applicants are denied or granted access to operate in and / or around the Airport. There are many rules and regulations that dictate levels and areas of access, and requirements for acquiring access to each area. The IdMS shall have the capability for applicants to complete a badging application through an online applicant portal, prior to visiting the ID Badging Office for their scheduled appointment. It must also allow the ID Badging Office staff to access the application at the time of the appointment, to review and update information such as:

1. Company types, security checks (Criminal History Records Check (CHRC), STA, CBP, Secure Flight, other 3rd party checks) and includes capability to set exemptions at the company level.
2. Badge types including privileges (escorting, driving, CBP seals etc.) for each badge type.
3. Financial configurations (monthly invoiced, no fee, pay-as-you-go by individual, pay-as-you-go by company; Escrow, etc.)
4. Company-specific fee configurations, documents, and insurance requirement.

After the data is confirmed, ID Badging Office staff will submit the application for background checks and/or updates. See **Attachment 12-1** for more information on the Badge Application Workflow processes pertaining to fingerprinting, training, background check appeals, and badge renewals.

3.3 System User Groups

A goal for the IdMS is to allow tenants and applicants to have a greater role in and understanding of the badging process, to ensure data validity and security, and to streamline the application process. The System User Groups diagram in **Attachment 12-1**, identifies the various users of the IdMS, their functional capabilities and the rules that impact their privileges. The System Administrator has the most extensive system privileges and access rights, including the ability to create system wide permission groups, system configurations, manage system settings and business rules, develop and generate reports, setup notifications, and perform system backup and restore.

3.4 Citations – Security and Safety

The Port issues Security and Safety violations to airport badge holders when they violate Federal, State, local or Airport rules and regulations. Citations can be written in absentia or in the presence of the badge holder. The citation is mailed to the badge holder and an email notification is sent to the AS. To satisfy the conditions of the citation, badge holders will need to complete computer-based training, may be required to meet with an Airport representative and / or pay a fine and/or serve a badge suspension. The IdMS shall provide ID Badging Office staff the capability to enter violation information into a badge holder's record. The IdMS shall generate a violation notice to the badge holder who committed the violation and send an email to the badge holder's AS, informing them of the violation and the requirements associated with the violation level. See **Attachment 12-1: IdMS Citation Requirements**: Security and Safety, and IdMS Citation Requirements, for a diagram of the citation work flow and specific IdMS citation requirements.

4. Implementati on and Maintenance

4.1 Implementation Approach

To achieve the highest probability of project success, the Port requests the written submission of an implementation and maintenance plan. ***The Port highly recommends the IdMS vendors to provide suggestions to reduce the overall project implementation timeline and risk.***

4.2 Environments

The Port will provide the server and network infrastructure software and hardware required for the successful IdMS implementation except where stated such as badging equipment. The Contractor shall provide detailed server and network requirements including minimum specifications and quantities.

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

4.3 Project Deliverables

The project implementation will consist, at a minimum, of the following deliverables for the Airport's review and approval:

1. The Contractor shall provide Project Schedule and Resource plan.
2. Communications Plan: The Contractor shall provide a plan to address at a minimum the following topics:
    a. Project status weekly and monthly meetings followed by minutes
    b. Provide status reports, monthly executive summary reporting including financial statuses, tasks completed and 30-60 look ahead reporting, project risks and schedule impacts / changes

c. Forms and templates to track ongoing project open items checklist, and clearly track issues, actions, decisions and statuses.

3. Change Management Plan to include: The Contractor shall provide a plan to address at a minimum the following topics:
    a. Request for Information (RFI) process, form templates, and a clearly identify method to document resolutions;
    b. Change control process for raising change requests, review and approval methods, form templates, and cost analysis impacts.
4. The Contractor must provide minimum specifications for the Airport to build and supply the development, testing and training and production environments.
5. The Contractor shall install a working demo system (not to include interfaces and badging equipment) in an Airport-provided development environment.
6. The Contractor shall perform requirements review sessions based on (Attachment 12.3) with the Airport team. The Contractor shall submit the following for Airport review and approvals:
    a. Final Agreed Requirements Traceability matrix
    b. Clearly identify customizations agreed with the Airport including supporting documentation
    c. All RFIs and resolutions
    d. Scope changes deferred / denied / approved including supporting documentation
    e. Business processes work flows (swim lanes) for handling Company (onboarding, de-activation, exception scenarios such as name change and mergers, Contractor), AS (onboarding, offboarding, pre-enrollment, renewals, audits and other), , Badge holder (pre-enrollment, badge issuance including exceptions such as background checks fails, re-fingerprinting, adjudications, Rapback work flows, eBadge, badge audit procedures and citation procedures etc.). The document should also include citation work flows and list all business rules that are necessary for the functioning of the IdMS
    f. System and Application configurations – Identify information that the Airport needs to provide.
7. The Contractor shall provide System Design and Technical documentation for Airport review and approval. The deliverable will include at a minimum:

    a. System Architecture – Physical and Logical design indicating all internal and external systems connectivity for Pre-Production and Production environments.
    b. System Software & Hardware Requirements – Server, OS, Database, Network, Firewalls, Workstations, badging equipment's including Quantities for servers, workstations, badging peripherals.
    c. Interface Control Documents –
        i. Standard interfaces
        ii. Non-standard interfaces
    d. Database schema – Entity Relationship Diagrams, Database Dictionary and all data repositories that will be required for data analysis and migration for a consolidated IdMS.
8. The Contractor shall start installation, development of customization and delivery to Test environment, and perform system configuration.
9. The Contractor shall perform data analysis and provide Data Reconciliation Report and Action Plan. The document shall include impact analysis of certain data fields that are mandatory for the normal performance of the IdMS.

    a. Contract to submit reports of preliminary analysis of from the data repositories identifying missing or incorrect data elements.

    b. Recommend the priority for critical and mandatory data elements that need to be cleaned up by the Airport's including implications and timeline per the

project plan. Additionally, provide suggestions clean up priority for non-critical/ non-mandatory data elements.

10. The Contractor shall perform data migration into the Test environment such that the system is Test ready.

11. The Contractor shall provide a Data Migration Plan.

12. The Contractor shall provide the following for the Airport review and approval:

    a. Test Plan to include test timeline, staff and equipment resources required,
    b. Test scripts – scenario based and map to the Functional Specifications Requirements.
    c. Online Issue Tracking system - Method to log, identify issues (bug/missing functionality/ not in scope/ other) and track testing results for actions.

13. The Contractor shall conduct Unit Testing, System Testing and Integration Testing in the Airport's Test Environment. The Contractor shall submit the testing results and demonstrate all IdMS functions are operational as per the Attachment 12.3. The Contractor shall recommend to the Airport that the IdMS is ready for the Airport to participate and conduct System Acceptance Testing.

14. The System Acceptance will be conducted with the Airport end user and Airport data and integration to all 3rd party systems as per the requirements as per Attachment 12.3.

    The system acceptance testing will be performed in the Testing and Training Environment and will be a pre-requisite for go-live. After the demonstration by the Contractor, the Airport staff will perform hands on system testing based on the test plans and test cases (scenarios) provided by the Contractor and approved by the Airport.

    The Contractor shall also provide data migration validation reports including identifying any critical/ mandatory missing data and misrepresentation of data and corrective action for the Airport staff to review and approve.

15. The Contractor shall receive System Acceptance Approval from the Airport after all requirements are demonstrated and tested and there are no open items, and the Airport has provided explicit acceptance of the system in test environment.

16. The Contractor shall provide the following for the Airport review and approval:

    a. Training Plan including syllabus, training modules, time for training, method of training, training resources required etc.

    b. Training shall be performed on the Airport premise and coordinated with the Airport staff ahead of time. It is expected the following training will be performed by the Contractor as listed in Pricing sheet Attachment 13.

        i. Trusted Agents and other Airport staff (security, operations, and others) – Three (3) training sessions, hands on with complete badging setups.
        ii. Authorized Signatories – Five (5) sessions, in-person and online.
        iii. System Administrators – One (1) training session.

    For ongoing training requirements, the Contactor shall coordinate with the Airport for "train the trainer" staff (credentialing staff and operations staff). The training shall be in a class, include hands-on setup and shall be specific to the End User functionality

and workflows. Cases where the Contractor plans to provide generic training shall be submitted to the Airport for review and approval prior to conducting such training.

17. The Contractor shall provide User Manuals – electronic copies (pdfs), method for the specific training manuals to be made available within the IdMS application such as Authorized Signatory portal.

18. The Airport may decide to video record some of the trainings conducted for future use.

19. The Contractor shall perform the implementation and roll out of the system into the Production Environment. The installation in the Production Environment must take place after the Airport has approved the System Acceptance Testing.

20. The Contractor shall provide Run Book that shall include –step-by-step guide for installation, configuration, database migration, 3rd party integration sequence and production sanity testing details. Each step will include resource responsible and time taken for each step.

21. The Contractor shall provide details of all the resources required on site from the Contractor, Airport Security, IT and any 3rd party systems for the production roll out and go-live.

22. The Contractor shall provide at a minimum two (2) full time engineering resources for 2 weeks post Go-live.

23. The Contractor shall provide details, before the IdMS go-live, for the Airport review and approval, of the maintenance and support system. The details should include the ticketing system information. The Contractor shall train key Airport staff to use the ticketing system that will allow to report and track production issues.

24. The Contractor shall support a system stabilization period of a minimum of thirty (30) calendar days after the IdMS is working in the Production Environment. During this period, the Contractor shall monitor and report system health checks to include - performance metrics, integration or network issues, database growth, or other system (functionality) related issues that impact the badging operations.

    The Contractor shall work with the Airport for corrective actions on any of the items identified during this period. The exact start and end date of the stabilization period or if the stabilization period will be reset due to critical issues (as defined in section 4.6 of this document) encountered will be agreed upon with the Airport.

25. The Airport will provide final system acceptance in Production Environment once all functionalities are delivered and working; and, the Airport is experiencing beneficial use of the system, and there are no critical open issues.

26. The Contractor shall provide project Close out documentation to include as-built design documents, agreed on responses to the specification's matrix, list of software licenses, hardware quantities, make, model and licenses, maintenance plans (as recommended by the manufacturer), interface control documents, copies of RFIs and RFI responses from the airports, other planning documentation such as project plan, run book, data migration strategies etc. and the list of support tickets at the time of project close out.

27. The Contractor shall prepare and submit system maintenance documentation of all software and hardware installed. Complete sets of system manuals shall be submitted explaining system maintenance of all software and hardware installed.

    The maintenance services during the contract shall include at a minimum the following:

a) Detailed instructions on how to perform diagnostics and regular preventive maintenance.
b) Correction and repair of all errors and malfunctions.
c) Replacement of all failed hardware and components.
d) Procurement and installation of all recommended and required software upgrades and patches required to operate the system during production.
e) Routine scheduled and recommended maintenance procedures required for the installed components to operate in a production environment. All routine and recommended maintenance shall be coordinated with the Airport.

4.4 Warranty (Hardware and Software)

For the purposes of section **Warranty** the "**IdMS**" represents all the **Software\Solution\Integration\Add-on Modules** installed at par to the contract and will be referenced as such.

The Contractor warrants that the IdMS will be free of defects in workmanship and materials for a period consistent with industry standards and the nature of the ("Warranty Period"). The Contractor include an explanation of the system's warranty coverage and include optional extended maintenance agreement\warranty options. All system maintenance will be completed after hours.

The Contractor shall provide a one (1) year manufacturer-based warranty on all products (software and hardware) provided by the Contractor. The one (1) year warranty period for all components (software and hardware) will commence after the Final System Acceptance in Production Environment by the Airport is complete.

The Contractor shall provide all (software and hardware firmware) upgrades in the first-year warranty and included in subsequent years as part of any additional maintenance agreements. The Contractor shall provide methods for version and periodic upgrades to support changes in platform operating systems, support applications and security requirements. The Contractor shall provide during the warranty period, and any period thereafter where the IdMS is covered by an annual maintenance agreement, no-charge updates to maintain compliance with evolving security regulations and Security Directives.

If the IdMS does not perform in accordance with the Contract during the Warranty Period, then the Vendor shall take such steps as necessary to repair or replace the defective portion at no additional cost to the Airport for material and labor. Such warranty service shall be provided at the Vendor's expense and shall include all media, parts, labor, freight and insurance to and from the Airport.

If any defect in the IdMS is not rectified by the Vendor before the end of the Warranty Period, the Warranty Period shall be extended until, in the opinion of the Airport:
a) the defect has been corrected; and

b) the IdMS functions in accordance with the Contract for a reasonable period.

Once the defect has been rectified, it is at the sole discretion and option of the Airport to request that the acceptance testing for the IdMS be reperformed.

Despite any other provision, the Airport, at the Airport's option, may return a defective IdMS to the Vendor within thirty (30) days of delivery of the IdMS and the Contractor shall immediately provide full exchange or refund. For this section, "defective Solution" includes, but is not limited to:

a) IdMS has not met contractual obligations during acceptance testing or during the valid "Warranty Period";

b) IdMS causes significant impact and disruption to Airport's operations and requires excessive downtime and interaction of Airport staff.

The Contractor shall provide, after the warranty commences for all IdMS components, telephone support to the Airport for assistance with the operation of the IdMS in line with the support agreement between the Contractor and the Airport. If the Contractor is not the Manufacturer of certain components of the IdMS, then the Contractor shall disclose the Manufacturer's warranty for such components to the Airport and, in the event such warranty exceeds the Vendor's warranty under this Contract in any respect, shall ensure that the Airport will receive the benefit of the Manufacturer's warranty.

4.5 Maintenance

The Contractor shall be responsible for maintaining all the software and hardware components procured as part of the IdMS contract. The contractor shall develop, for the Airport's approval, a maintenance plan required under the IdMS agreement and listed in the deliverables section above. The Contractor shall provide the following:

Maintenance period includes two years maintenance which includes 1 year warranty and three (3) one-year extensions, to be exercised at the Port's sole option for maintaining the system after the end of the warranty period.

Document service levels including, but not limited to, coverage time, maintenance request response time and acceptable system downtime.

A plan to address all labor, software upgrades (including all necessary licensing, hosting, and/or design services), documentation revisions and preventive maintenance services necessary to keep the IdMS system and all integration components in good operating condition and in full compliance with all applicable regulatory requirements.

All software upgrades during the warranty period and subsequent years, as part of a maintenance agreement.

The agreement shall provide, at the Airport's option, routine hardware and software maintenance. The contractor shall be responsible to provide all necessary software upgrades and changes to remain compliant with all Governing Standards, including (without limitation) TSA 49 CFR Part 1542 and other applicable regulatory requirements including Security Directives and the National Airport Security Programs (ASP) Amendments.

4.6 Support

The Contractor shall provide two consecutive weeks of onsite engineering support post "go live". Contractor must designate certified individuals with site specific knowledge to function as the account representatives to coordinate support services.

After the Final System Acceptance of the IdMS in the Production Environment, and the Airport has initiated the maintenance phase, the Contractor shall provide updates, enhancements, and/or bug fixes to all systems at no additional charge during the term of any maintenance/service agreements. All system changes shall be conducted after hours in coordination with the Airport. The Contractor shall provide a detailed process including toll-free telephone and support email to Airport representative(s). The Airport shall describe and categorize the support issues as follows:

Critical Issues & Response Times:

Critical issues are defined as catastrophic failures which affect the overall safety, security, or operation of the Airport. For example, the failure of a server, the loss of a badging workstation, the loss of functionality to print or produce badges, or the loss of integration or errors in the integration between the IdMS and external systems. Critical issues require the Contractor to respond per the response times indicated below.

Critical Issues Response Times:

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

Non-critical Issues:

Non-critical issues are defined as failures or problems which do not affect the overall safety, security, or operation of the Airport. For example, the failure of a non-critical redundant piece of equipment or the loss of a single badge printer would usually be considered non-critical.

Non-critical Issues Response Times:

- Initial response and acknowledgement within 15 minutes (business or non-business working hours) of reported issue(s).
- Follow up contact with the ID Badging Office Superintendent and/or representative within two (2) hours (business or non-business working hours) to understand the issue and start trouble shooting process.
- Within six (6) to twelve (12) hours (business or non-business working hours) of the issue having been reported, the Contractor shall provide status and next steps to fix the issue. The Contractor shall diagnose and remedy the problem during normal working hours of the next working day.
- Business working hours are defined as 6:00 AM to 7:00 PM Pacific Standard Time, Monday through Friday.

The Contractor shall provide escalation procedures including contact name, direct phone number and email address.

- In addition to the toll-free number, the Contractor must provide an online portal for support ticket requests. The Airport must be able to select the currently installed configuration options for the hardware, software and services being supported. The online support portal must provide the customer details such as:
- Software installed with versions.
- Hardware installed with versions.
- Additionally, online support portal must provide the functionalities:
- Knowledge base of previous support cases.
- Estimated response time not to exceed time frame listed via e-mail.
- Technician assigned to support request.
- Status updates on support tickets – via e-mail.

- Listing of all support tickets and who initiated the tickets.
- Support category: warranty, out of warranty, covered, not covered.
- Designate issue criticality (Critical or Non-Critical) and designate priority: Low, Medium, High.
- Ticket resolution with details.
- All support personnel (including 3rd party personnel) responding to support issues, via on-site or phone, must be certified in the software\hardware configurations. All support personnel (including 3rd party personnel) responding to on-site support issues must complete applicable security background check (STA and CHRC) requirements.

Additional requirements / submittals are contained in **Attachment 12-3:** OAK IdMS Specifications and Technical Specifications Compliance Matrix.

The Maintenance and Support shall be enforced by liquidated damages and payment retainage, as described in the Standard Professional Services Agreement **(Attachment 11)**.

III. Port Policy and Other Requirements

The selected Respondent will be required to comply with the following Port Policy and Other Requirements:

1. Non-Discrimination and Small Local Business Utilization Policy (NDSLBUP):

The Port desires to maximize the participation of small local business and has instituted a Non-Discrimination and Small Local Business Utilization Policy (NDSLBUP). The NDSLBUP consists of two parts:

- Non-Discrimination policy which all Suppliers (Respondents) must adhere to, by providing the enclosed "Non-Discrimination and Small Local Business Utilization Policy Program Affidavit" **(Attachment 6)** with their proposals
- Preference points are awarded to small local businesses who qualify under the Port's definition of a small local business. In order to qualify for preference points, Suppliers (Respondents) must be either certified by the proposal due date or may apply online at: http://srd.portofoakland.com/. The application and any supporting documentation must be submitted to the Port's Social Responsibility Division seven (7) business days prior to the proposal due date. To apply, please click on the above link and then on the link titled "Register New Company?" and follow the instructions.

A summary of the Port's Non-Discrimination and Small Local Business Utilization Policy is included herein as **Attachment 5**. The entire policy is available at:

http://www.portofoakland.com/files/PDF/responsibility/NDSLBUP_00810.pdf

Suppliers already certified with the Port do not need to submit proof of certification, but still need to check the Port's certification database at: http://srd.portofoakland.com/ to ensure their certification has not expired and must fill out the Chart for Submitting Data for Calculation of Preference Points **(Attachment 5-A)**, and the Local Participation Questionnaire **(Attachment 5-B)**, and submit them with your proposal. All Suppliers (Respondents) must still provide proof of adhering to the Port's Non-Discrimination policy by submitting the NDSLBUP Program Affidavit.

A copy of the Port-certified Small Local Business Enterprises can also be downloaded at: http://srd.portofoakland.com/

For questions or assistance regarding NDSLBUP, contact Ms. Marlene Rubain, Contract Compliance Officer, (510) 627-1485, at the Port's Social Responsibility Division, or email mrubain@portoakland.com.

2. Insurance Requirements:

All Respondents who plan on submitting a proposal in response to this RFP must meet the Port's Insurance requirements listed in **Attachment 9** and must provide proof of insurance at the time of project award. Respondents must include a statement **(Attachment 10)** with their proposal agreeing to the Port's insurance requirements and indicate they will be able to obtain the proper insurances at the time of project award.

3. Security Sensitive Information:

By submitting a proposal, Respondent acknowledges that in the course of performing services under the Agreement, the selected Consultant/Contractor will come into possession of sensitive information subject to Port of Oakland regulation. The selected Consultant/Contractor will be required to comply strictly with the Port of Oakland's policies and practices for sensitive information.

4. Living Wage Policy:

On March 5, 2002, the voters in the City of Oakland passed Measure I, adding to the City Charter Section 728 ("§728") entitled "Living Wage and Labor Standards at Port-assisted Businesses." §728 requires Port Aviation and Maritime businesses that meet specified minimum threshold requirements to pay all nonexempt employees a Living Wage rate established by City Ordinance and adjusted annually based on the Consumer Price Index for the San Francisco, Oakland, and San Jose area. The current Living Wage rate as of July 1, 2021 is at least $15.30 with credit given to the employer for the provision to covered employees of health benefits, and $17.56 without credit for the provision of health benefits. Specifically, §728 applies to Port contractors and financial assistance recipients with the Aviation or Maritime divisions that have contracts worth more than $50,000 and that employ more than 20 employees who spend more than 25% of their time on Port-related work. §728 also provides covered employers with incentives to provide health benefits to employees, establishes a worker retention policy, requires covered employers to submit quarterly payroll reports and requires covered employers to allow Port representatives access to payroll records in order to monitor compliance and labor organization representatives access to workforces during non-work time and on non-work sites. Covered employers are responsible for complying with the provisions of §728 from the date the covered contract is entered into. When a contract is awarded, the Respondent will be required to fill out the attached Employer Self-Evaluation for Port of Oakland Living Wage Form **(see Attachment 7-A)** and Certificate of Compliance—Living Wage **(see Attachment 7-B)** and return them to the Social Responsibility Division. (i.e., do not include these forms in with your proposal). For more information, please call Amy Tharpe in the Port of Oakland's Social Responsibility Division at (510) 627-1302.

Respondent shall acknowledge reviewing the Port's Living Wage program and compliance, by submitting the Statement of Living Wage Requirement **(Attachment 8)** with their proposal.

5. Port's Standard Professional Services Agreement:

Submission of a proposal will confirm that the Respondent fully understands the provisions of the Port's Standard Professional Services Agreement **(Attachment 11)** which will be revised as necessary to be consistent with the provisions of this RFP, and will execute such revised agreement if awarded the contract. Any objections to any provisions in the Port's Standard Professional Services Agreement and/or this RFP must clearly be identified in your proposal. Changes are discouraged.

IV. Submission Requirements

Please respond to the following 8 submission requirements in a straightforward, concise delineation of your capabilities proposed to satisfy the requirements of the RFP. The Port will use your responses to objectively determine your capabilities and experience. Please label your responses 1 through 8, in the order presented below. Please limit your total response to the number of pages indicated below

(excludes the required attachment forms provided with this RFP).

Submittal Format:

Responses may not be longer than 50 pages (double sided), printed on 8 ½" x 11" paper and formatted in no smaller than 10-point font. The page limit must include all attachments and references to outside materials (including those on websites). The page limit does not, however, include the required Port forms detailed below. Each section shall be labeled according to the sections below. All submitted material must be bound with only **one staple or binder clip** in the upper left corner. Please no binders or any other type of binding. Submittals must be able to fit into a 9 x 11.5 inch folder.

1. **Company Information:** Provide the name of your company (including the name of any parent company), business address, email address, Federal Tax ID number, telephone and fax numbers, and names and titles of key management personnel, and a brief history of your company. Provide a brief statement of who is authorized to submit the proposal on the behalf of your company. Please make sure that person signs and dates the statement. If your company is making any exceptions to the Port's Standard Professional Services Agreement **(Attachment 11)** and/or this RFP, they must be clearly set forth in your proposal and noted in this section. Exceptions are discouraged and may result in lower evaluation points during the Port's evaluation of your proposal.

2. **Knowledge and Experience:** Provide relevant information about your company's knowledge and experience, including a list of at least three (3) projects for airports in the United States within the past 5 years, with brief descriptions that demonstrate your experience.

3. **Client References**: Provide names, addresses, and contact information for the main project contacts for the three (3) or more projects described in the Knowledge and Experience section above. Provide the size and scope of each project and a brief description of the projects. Please make sure all contact information is current. By providing such information, you authorize us to contact such clients. Airport References must include at a minimum:

    i. Airport name.
    ii. Airport contact person name and title (Project Manager or principal individual) with direct knowledge of contract and service performance.
    iii. Telephone number.
    iv. E-mail address.
    v. ID count and quantity of badging workstations.
    vi. List interfaces at the reference airports, clearly indicate interfaces in production and planned not yet in production.
    vii. Specialized system interfaces (such as financial, mass notification system, etc.).

4. **Plan and Approach**: Provide an overview describing your plan and approach, scope of services and methodology of your company's ability to fulfill the general functions required in this RFP as well as quality control and assurances. Please use this section to describe the services you propose to provide to the Port. Your services can be above and beyond the requirements listed in the "Scope of Service" section. Proposer shall include an implementation approach (see Section 4.1 through 4.6, also making sure you have discussed all required deliverable listed in section 4.3). Through your implementation approach, the proposer shall discuss potential risks and mitigation strategies.

    Additionally, proposers must respond to the following two supplemental questions:

    a) Supplemental Question No. 1: From a prior IdMS deployment at a U.S. airport, describe the largest or most significant unanticipated technical issue that arose during implementation (no need to identify the client/airport). How did your firm / team address the issue to the client's satisfaction? What was your firm / team's approach to (i) client communications, (ii) driving results / solutions, (iii) "work arounds," (iv) technical excellence, and (v) change orders?

b) Supplemental Question No. 2: Consider the following hypothetical situation: During IdMS deployment at OAK, the Airport advises your firm / team that it must implement an emergency version upgrade to its access control system (Software House CCURE 9000) to correct a cybersecurity vulnerability. How would your firm / team address this unanticipated change? What steps would you take to mitigate schedule and cost impacts?

5. **Proposed Costs:** Provide your cost to implement an IdMS solution at Oakland International Airport and attach any proposed fee schedule. It is important that you provide all costs for implementation, hardware, software, and the one-year warranty (during the 2-year base years), and two years of Maintenance and Support, and the three (3) additional one-year extensions of Maintenance and Support fee schedule so that the Port can properly evaluate your proposal. Your cost proposal summary and detail pricing should be presented on the Oakland International IdMS Pricing Sheet (Appendix 13).

6. **Debarment Statement:** Provide a written statement that your company has not been debarred from providing services to any State or Federal Agency within the last five (5) years. Sign and date your statement. If your company has been debarred, you will need to provide background information and the reason(s) for the debarment. Provide the name and contact information for the agency that debarred your company. The Port must review the reason(s) and duration for the debarment before it can determine if your company can be considered for this project.

7. **Litigation and Other Information:** Provide information describing any litigation, arbitration, investigations, or any other similar actions that your company, its principals, directors, and/or employees have been involved in during the last five (5) years relating to your company's services. Please list (a) name and court case or other identification number of each matter, (b) jurisdiction in which it was filed, and (c) outcome of matter (e.g. whether the case is pending, a judgment was entered, a settlement was reached or the case was dismissed). The Port will review the reason and timing of the action before it can determine if your company can be considered for this project. Failure to provide the litigation information may disqualify your proposal.

8. **Required Forms and Adherence to Port Policy and Other Requirements:** The Respondent must fill out all of the forms included in this RFP (listed under the "Attachments" section and marked with a "Yes" in the column titled "Must Be Returned with Proposal"), and return them with your proposal. By returning the listed forms, your company is supporting and agreeing to the Port Policy and Other Requirements (listed in Section III, "Port Policy and Other Requirements" of this RFP). Failure of the Respondent to provide any of the required forms may result in your proposal being rejected for non-responsiveness. These required forms will not count against the maximum page count (indicated above) for your response.

V. Evaluation Criteria

Prior to contract award, the Port must be assured that the Respondent selected has all of the resources required to successfully perform under the contract. This includes, but is not limited to, personnel with skills required, equipment/materials and financial resources sufficient to provide services called for under this contract. If during the evaluation process, the Port is unable to assure itself of the Respondent's ability to perform under the contract, if awarded, the Port has the option of requesting from the Respondent any information that the Port deems necessary to determine the Respondent's capabilities. If such information is required, the Respondent will be notified and will be permitted five (5) working days to submit the requested information.

In awarding the contract, the Port will evaluate a number of factors in combination. Please make sure you have submitted responses to all items listed in the Submission Requirements section, as your responses will be evaluated based on the weights listed below.

A. Evaluation Weights

Item	Criteria	Weights
1	Adherence to Port Policy and Other Requirements and Debarment Statement Proposals from companies who have not or will not adhere to the Port Policy and Other Requirements or who have been debarred and have not provided sufficient reasons/justification for the Port to review the circumstances surrounding the debarment will not be forwarded to the evaluation committee for review. (Items 6 and 8 of the Submission Requirements section.)	Pass/Fail
2	Company Information, Client References, Litigation and Other Information, and Required Forms Respondent's capacity to provide professional service as evidenced by past performance, company information, reference checks, litigation and other information, and required forms. (Items 1, 3, 7, and 8 of the Submission Requirements section.)	5%
3	Knowledge, Experience and Client Reference Validations Respondent's knowledge and experience in providing Identity Management Systems as evidenced from your response to item 2 of Submission Requirements section.	30%
4	Plan and Approach As evidenced from your response to item 4 of the Submission Requirements section.	30%
5	Proposed Costs As evidenced from your response to item 5 of the Submission Requirements section, and as provided on the OAK IdMS Pricing Sheet (Appendix 13).	20%
6	Non-Discrimination and Small Local Business Utilization Policy (NDSLBUP) Does your company meet the Port's definition of Small Local Business and/or make a commitment to the Port's values and programs {e.g., mentoring small and/or very small local businesses and providing meaningful work for small and/or very small local sub-consultants; utilization of college and high school interns from the Local Impact Area (LIA); participation in job fairs and trade fairs targeted to LIA residents and businesses; and other work showing the consultant's efforts to contribute to the economic development of the LIA. The Port will evaluate companies that have provided substantiating documentation to prove they meet the Port's NDSLBUP program award points accordingly to qualifying companies.	15%
	Total	100%

B. Selection Procedure:

All proposals received by the deadline which meet the RFP's requirements will be presented to the evaluation committee comprised of Port of Oakland staff and possibly external members. The evaluation committee will evaluate the proposals and score all submissions according to the evaluation criteria above. The selection process may include interviews (at the discretion of the evaluation committee) for the top-scoring submissions. If interviews are to take place, the Port will notify the top scoring Respondents. Interview details and scoring requirements will be provided to selected Respondents prior to the interviews. A demonstration of your solution will be required.

VI. Additional Provisions

The terms "Company", "Consultant", "Contractor", "Proposer", "Respondent", "Seller", "Supplier", and "Vendor" whenever appearing in this RFP or any attachments, are used interchangeably to refer to the company or firm submitting a proposal in response to this RFP.

A. Port's Legal Name and Jurisdiction

The Port of Oakland (the "Port") is legally known as the City of Oakland, a municipal corporation, acting by and through its Board of Port Commissioners. The Port is an independent department of the City of Oakland. The Port has exclusive control and management of all Port facilities and properties. Port facilities and properties consist of marine terminals, a railway intermodal terminal and container storage areas (collectively, the "Seaport"); the Oakland International Airport (the "Airport"); and commercial and industrial land and properties (collectively, "Commercial Real Estate"); and other recreational land, other land, undeveloped land, and water areas, all located in Oakland, CA. The Port issues Purchase Orders under the name "Port of Oakland".

B. Ownership of Proposal

All rights to information developed, disclosed, or provided in a Proposal and its attendant submissions are the property of Port, unless a Respondent makes specific reference to data that is considered proprietary. To the extent that a Respondent does not make specific reference to data that is considered "confidential" and proprietary, submission of an RFP constitutes the Respondent's express (a) grant and assignment of a perpetual, transferable (in whole or in part), non-exclusive, royalty-free license to the Port for copyright, patent, or other intellectual property right (collectively referred to as "intellectual property"), and (b) agreement that the Port may use any such intellectual property without charge for any lawful purpose in connection with other Port development projects, including without limitation the creation of derivative works and issuance of sublicenses.

C. Deadline for Receipt of Proposal

Proposals must be sealed and delivered to the Submittal Address listed in the Request for Proposal (RFP) no later than the time specified in the RFP. The Port will place a clock ("Clock") in a conspicuous location at the place designated for submittal of Proposals. For purposes of determining the time that a Proposal is submitted, the Clock shall be controlling (unless at the time of the receipt the Clock malfunctions, then the Port's clock on its network phone system shall be controlling). The Port suggests that Proposals be hand delivered to the Submittal Address in order to ensure their timely receipt. Any Proposals mailed via an express mail service, US Postal Service, or other courier service shall not be considered timely received until date and time stamped by the controlling Clock. Any Proposals received after the time stated (regardless of the cause of the delay, including whether caused by the express mail service, US Postal Services, other courier service, or the Port's mail handling personnel) shall not be opened and shall be returned, sealed, to the Proposer.

D. Public Records Act

Under the California Public Records Act (Gov. Code § 6250 et seq.), the Port may be obligated to make available to the public the submitted proposal and all correspondence and written questions submitted during the Request for Proposal process. However, such disclosure shall not be made prior to the date on which the Port publishes the identity of the apparent successful proposer or issues a Notice of Intent to Award, if such notice is issued.

If Respondent believes portions of its proposal contain trade secrets or proprietary financial information that should be exempt from disclosure under the Public Records Act, **Respondent shall submit a separate copy of its entire proposal with the protected material redacted with black boxes, which each redaction specifically marked as "CONFIDENTIAL"**. Such separate copy shall not constitute the proposal, but shall be used, if needed and appropriate, in response to an applicable Public Records Act request. If Respondent does not submit such a separate redacted proposal, Respondent shall be deemed

as not claiming that any portion of its proposal contains trade secrets or proprietary financial information.

The Port reserves the right to independently determine whether any document is subject to disclosure and to make such information available to the extent required by applicable law, without any restriction or notice to Respondent.

E. Indemnification

If Respondent is selected to receive a contract, it will be required to agree to the indemnification clause contained in the Port's Standard Professional Services Agreement. **See Section 5** of the Port' Standard Professional Services Agreement **(Attachment 11)**.

F. Reimbursable Expenses

All expenses incidental to performing Consultant's Basic Services including, but not limited to, reproduction of documents and other materials associated with Respondent's deliverables and presentation materials; transportation and subsistence; telephone, computer, facsimile, or other similar costs; and the like, shall be included within the Contract Price.

G. Port's Right to Modify

Respondents are advised that the Port has not incurred any obligations or duties in soliciting this Request for Proposals. The Port, at its sole discretion, reserves the right to reject any or all proposals submitted in response to this RFP; to request additional information or clarification of information submitted; to cancel or modify, in part or in its entirety, this RFP; to request new RFPs or pursue any other means for obtaining the desired services; to waive any informalities or minor irregularities in the RFP, and other inconsequential deviations from the RFP's requirements. The Board of Port Commissioners retains the right to award this project in part or in total to the Respondent(s) of its choice, and to decide to undertake the project or to terminate the project at any time prior to approval of a formal contract.

H. Conflicts of Interest

By submitting a proposal, the Respondent represents that it is familiar with Section 1090 and Section 87100 et seq. of the California Government Code, and that it does not know of any facts that constitute a violation of said sections in connection with its proposal. Respondent also represents that its proposal has completely disclosed to the Port all facts bearing upon any possible interests, direct or indirect, which Respondent believes any member of the Port, or other officer, agent or employee of the Port or any department presently has, or will have, in any agreement arising from this RFP, or in the performance thereof, or in any portion of the profits there under. Willful failure to make such disclosure, if any, shall constitute ground for rejection of the proposals or termination of any agreement by the Port for cause. Respondent agrees that if it enters into a contract with the Port, it will comply with all applicable conflict of interest codes adopted by the City of Oakland and Port of Oakland and their reporting requirements.

I. Cost of Preparing a Response

All costs for developing a response to this RFP and attending any proposal meetings or selection meetings are entirely the responsibility of the Respondent and shall not be chargeable to the Port.

J. Compliance with Law

The Respondent must comply with all laws, ordinances, regulations and codes of the Federal, State, and Local Governments, which may in any way affect the preparation of proposals or the performance of the contract.

K. Respondent's Relationship

The Respondent's (and Respondent's employees' and contractors') relationship to the Port shall be that of independent contractor and not deemed to be an employee or agent of the Port.

L. Proposal Considerations and Legal Proceeding Waiver

The Port has absolute discretion with regard to acceptance and rejection of proposals. In order to be considered the party submitting a proposal waives the right to bring legal proceedings challenging the Board of Port Commissioners choice of the award.

M. False Statements

False statements in a proposal will disqualify the proposal.

N. Taxes

The Respondent will be responsible for all Federal, State, and Local taxes.

O. Grade of Service

The Respondent must provide professional service and maintain appropriate personnel to provide expedient and courteous service.

P. The Respondent's Liability

The Respondent shall be responsible for any and all damages to the Port's premises resulting from the negligent acts or willful misconduct of the Respondent's agents or employees.

Q. Amendments

The Port may, at its sole discretion, issue amendments to this RFP at any time before the time set for receipt of proposals. The Respondents are required to acknowledge receipt of any amendments (addenda) issued to this RFP by acknowledging the Addendum in the space provided on the RFP Acknowledgement and Signature Form. The Port shall not be bound by any representations, whether oral or written, made at a pre-proposal, pre-contract, or site meeting, unless such representations are incorporated in writing as an amendment to the RFP or as part of the final contract. All questions or requests for clarification concerning material terms of the contract should be submitted in writing for consideration as an amendment.

R. Withdrawal or Modification of Offers

The Respondent may modify or withdraw an offer in writing at any time before the deadline for submission of an offer.

S. Acceptance

Any offer received shall be considered an offer which may be accepted or rejected, in whole or in part, by the Port based on initial submission with or without discussions or negotiations.

T. Representations

No representations or guarantees of any kind, either made orally, or expressed or implied, are made with regard to the matters contained in this document, including any attachments, letters of transmittal, or any other related documents. The Respondent must rely solely on its own independent assessment as the basis for the submission of any offer made.

U. Award Consideration and Length of Contract

The Port shall not be bound to accept the lowest-quote fee and will award the contract (if any) to the company/firm selected through the competitive process (and any subsequent interviews) outlined in this RFP.

The Port plans to award a contract for up to 7 years comprised of:

- 2 year Implementation Period for IdMS implementation;
- 2 year Maintenance and Support Period, which includes 1 year Warranty (Warranty to commence after System acceptance by the Port); and
- Three (3) additional one-year extensions of the Maintenance and Support Period, to be exercised at the Port's sole option.

V. Contract Termination

The Port may terminate the agreement (and or contract) with the Respondent on thirty days notice for the failure of the Respondent to comply with any term(s) of the agreement/contract between the Port and the Respondent.

W. Protest Procedures

Any party that has timely submitted a responsive proposal that contends or claims that the Port's proposed award of the subject contract fails to comply with the Port's rules and regulations or with law must file a protest in accordance with the provisions set forth below:

1. Any protest must be submitted in writing to Daria Edgerly, Secretary of the Board, and received by the Port no later than 5:00 p.m. by the third (3rd) business day following publication of the identity of the apparent successful proposer (or of Notice of Intent to Award, if such notice is issued).
2. The protest must include the name, address and telephone number of the person representing the protesting party.
3. The initial protest document must contain a complete statement of the basis for the protest, including in detail, all grounds for protest including referencing the specific portion of the solicitation document that forms the basis for the protest, and including without limitation all facts, supporting documentation, legal authorities and argument in support of the grounds for the protest. Any matters not set forth in the written protest shall be deemed waived. All factual contentions must be supported by competent, admissible and credible evidence.

Any protest not conforming to the foregoing shall be rejected by the Port without recourse.

PORT OF OAKLAND

Non-Collusion Declaration

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

(To Be Executed By Proposer and Submitted With Proposal)

I, _____, declare as follows:

That I am the _____of _____, the party making the attached proposal; that the attached proposal is not made in the interest of, or on behalf of, any undisclosed person, partnership, company, association, organization, or corporation; that the proposal is genuine and not collusive or sham; that the proposer has not directly or indirectly induced or solicited any other proposer to put in a false or sham proposal, or that anyone shall refrain from proposing; that the proposer has not in any manner, directly or indirectly, sought by agreement, communication, or to fix any overhead, profit, or cost element of the proposal price, or that of any other proposer, or to secure any advantage against the public body awarding the contract of anyone interested in the proposed contract; that all statements contained in the proposal are true; and further, that the proposer has not, directly or indirectly, submitted his or her proposal price or any breakdown thereof, or the contents thereof, or divulged information or data relative thereto, or paid, and will not pay, any fee to any corporation, partnership, company, association, organization, proposal depository, or to any member or agent thereof to effectuate a collusive or sham proposal.

Any person executing this declaration on behalf of a proposer that is a corporation, partnership, joint venture, limited liability company, limited liability partnership, or any other entity, hereby represents that he or she has full power to execute, and does execute, this declaration on behalf of the bidder.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed this _____ day of _____, 20__, at

_____, _____

_____

Signature

Authority: Public Contract Code 7106

CCP 2015.5

PORT OF OAKLAND

Statement of Equal Employment Opportunity

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

I hereby certify that I _____(Legal Name of Respondent/Supplier/Consultant/Contractor), will not discriminate against any employee or applicant for employment because of race, color, religion, sex, national origin, ancestry, age (over 40), physical or mental disability, cancer-related medical condition, a known genetic pre-disposition to a disease or disorder, veteran status, marital status, or sexual orientation.

I declare under penalty of perjury under the laws of the State of California that the information I have provided herein is true and correct and is of my own personal knowledge.

_____
Signature

_____
Print Name

_____
Title

_____
Date

PORT OF OAKLAND

RFP Acknowledgement and Signature Form

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

The undersigned having carefully examined the location of the proposed work, the local conditions of the place where the work is to be done, the Invitation, the General Conditions, the Specifications and all of the documents for this project, proposes to enter into a contract with the Port of Oakland to perform the work listed in this RFP, including all of its component parts, and to furnish any and all required labor, materials, equipment, insurance, bonding, taxes, transportation and services required for this project in strict conformity with the plans and specifications prepared, including any Addenda, within the time specified.

Addendum Acknowledgement:

The following addendum (addenda) is (are) acknowledged in this RFP: _____

Acknowledgement and Signature:

1. No Proposal is valid unless signed in ink by the person authorized to make the proposal.
2. I have carefully read, understand and agree to the terms and conditions on all pages of this RFP. The undersigned agrees to furnish the services stipulated in this RFP.
3. I understand my Proposal and all related documents may be released in their entirety in response to a request under the California Public Records Act, subject to any separate copy I submit in accordance with Section VI.D of this RFP.
4. I represent that I am familiar with Section 1090 and Section 87100 et seq. of the California Government Code, and that I do not know of any facts that constitute a violation of said Sections in connection with the proposal.

Respondent's Name: _____

Title: _____

Company Name: _____

Address: _____

Telephone: _____ Fax: _____

Email: _____ Cell Number: _____

Contractor License # (if applicable): _____ Expiration Date: _____

Federal Tax Identification Number: _____

Authorized Signature: _____ Date: _____

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

Oakland International Airport IdMS Pricing Sheet

(See Attachment 13)

PORT OF OAKLAND

Non-Discrimination and Small Local Business Utilization Policy

Non-Discrimination: Port of Oakland (Port) policy prohibits discrimination or preferential treatment because of race, color, religion, sex, national origin, ancestry, age (over 40), physical or mental disability, cancer-related medical condition, a known genetic pre-disposition to a disease or disorder, veteran status, marital status, or sexual orientation.

Local Business Utilization: On October 7, 1997, the Board of Port Commissioners initiated a formal policy to encourage full participation of firms from its Local Business Area ("LBA"), the counties of Alameda and Contra Costa, particularly those in its Local Impact Area ("LIA"), in its work. The LIA includes the cities of Oakland, Alameda, Emeryville and San Leandro. The LBA includes all cities within the counties of Alameda and Contra Costa. The Port will also take into consideration efforts the prime and sub-consultants make to assist in the community, e.g., assigning meaningful work to small and/or very small local sub-consultants, mentor protégé relationships, participation in job/trade fairs, hiring interns, pro bono work, and working with local schools, etc.

Consultant Preference Points: The Port allots preference points for the percentage of work being performed by consultants/sub-consultants located in either the LBA or the LIA and for community involvement (i.e. mentoring, intern programs, job fairs, community rehabilitation groups and re-entry programs) for a maximum total of up to 15 points. These points are added to a maximum of 85 technical points for a composite maximum of 100 points in evaluating consultant proposals as follows:

- Up to 5 points will be credited proportionately (counting the whole team, prime consultant and sub-consultant(s)) for LIA certified firms, and 2.5 for LBA certified firms.
  Note: LIA/LBA credit is given only for certified firms which have had established active offices in the respective area for at least a year at the time of proposal due date, and NOT for outside firms which plan to do the project work at a LIA/LBA office;

- An additional 3 points will be credited for an LIA certified prime consultant (proportionate to the share of prime consultant work in the case of a joint venture) and 1.5 points for an LBA certified prime consultant;

- Up to 4 points will be credited proportionately (counting the whole team, prime consultant and sub-consultant(s)) for Very Small Business Enterprise (VSBE) certified firms, and 2 points for Small Business Enterprise (SBE certified firms); and

- Up to 3 points for commitment to the Port's values and programs, e.g., mentoring small and/or very small local businesses and providing meaningful work for small and/or very small local sub-consultants; utilization of college and high school interns from the LIA; participation in job fairs and trade fairs targeted to LIA residents and businesses; and other work showing the consultant's efforts to contribute to the economic development of the LIA.

In summary, please submit the following attachments in each copy of your proposal:

1. Attachment 5-A, Chart for Submitting Data for Calculation of Preference Points. List the team members' (prime and subs) names, roles, location and LIA/LBA/SBE/VSBE status in the format shown in Attachment 5-A. Be specific as to the nature and estimated percentage of the work to be performed by the prime, any joint venture partners and/or sub-consultants.

2. Attachment 5-B, Local Participation Questionnaire. Complete for each sub-consulting firm or individual, as well as for the prime consultant.

3. Attachment 5-C and 5-D, Monthly and Final Utilization of Local and Small Business Enterprises are required after contract award. Attachment 5-C is required after contract award and a final report attachment 5-D, is required after completion of the project.

Any proposal that fails to complete and submit the above two items (Prime *and* sub-consultants) will not be considered. For firms headquartered outside the LIA/LBA wishing to obtain credit for their local office, for the purpose of this project shall utilize personnel from this local office. Additionally, mail, correspondence and telephone calls will be made to this local office.

To obtain credit for these factors and for any preference points on this RFP, consultants or any team member must be certified by the proposal due date or submit an application:

- Consultants or any team members wishing to be certified by the Port must submit a Certification Application, with all supporting documentation seven (7) business days prior to the proposal due date. The questionnaire and checklist of necessary supporting documents for certification may be obtained at: http://www.portofoakland.com/srd/. For questions regarding certification, you may contact Social Responsibility Division (SRD) at (510) 627-1627 or email SRDAdmin@portoakland.com. Firms certified by the Port of Oakland do not need to submit proof of certification.

(Please note Port certification must be current and not expired to count for preference points. Certification is valid for a two-year period.)

For questions or assistance regarding this section, contact Ms. Amy Tharpe (510) 627-1302, or atharpe@portoakland.com in the Port's Social Responsibility Division.

PORT OF OAKLAND

Chart for Submitting Data for Calculation of Preference Points

Company	Nature of Work to be Performed	Prime or Sub?	Location of Firm	*LIA/LBA SBE/VSBE Certification Status	Percent of Total Contract	Percent of Sub-consulting Work
(Name of Prime)		**Prime**				
(Name of Subs)		**Sub**				
(Name of Subs)		**Sub**				
(Name of Subs)		**Sub**				
(Name of Subs)		**Sub**				
(Name of Subs)		**Sub**				
(Name of Subs)		**Sub**				
(Name of Subs)		**Sub**				
(Name of Subs)		**Sub**				
(Name of Subs)		**Sub**				
(Name of Subs)		**Sub**				
				Total (must add up to 100%)	100%	100%

*** In order to qualify for preference points, the firm must be certified by the Port of Oakland.** Local Impact Area (LIA), Local Business Area (LBA), Small Business Enterprise (SBE), Very Small Business Enterprise (VSBE)

Notes:

- Please make sure the column labeled "Percent of Total Contract" adds up to 100%
- Please make sure the column labeled "Percent of Sub-consulting Work" adds up to 100% of the Sub-consulting work.

(Use additional paper if necessary)

1. Is the consultant or large sub-consultant mentoring or providing a professionally meaningful share of the project to small and/or very small LIA firms on this project? Yes___ No___

   If the response is "yes", please provide specific details on how the mentoring or sharing will be performed. In addition, be specific as to the nature of the relationship and the persons responsible for implementing it.

2. (A) Do any team members regularly use local students as interns in their work? Yes___ No ___
   (B) Do any team members currently use local students as interns in their work? Yes___ No ___
   (C) Have any team members used local students as interns in past work? Yes ___ No___
   (D) If planning to use interns on this project, how will you utilize them?

   If you answered "yes" to any of these questions, please state from what schools or programs the interns were obtained, what type of work was performed by them, and any other details that might be relevant, i.e. paid internship, length of service, number of interns.

3. Have firms in the team participated in other community projects, e.g., job fairs targeted to local neighborhoods, youth or school programs, community rehabilitation groups, etc.? Yes___ No___
   If so, please give details:

PORT OF OAKLAND

Monthly Utilization of Local and Small Business Enterprises

PRIME CONTRACTOR	BUSINESS ADDRESS	CONTRACT BID AMOUNT	DATE OF THIS REPORT

PORT PROJECT NAME	PORT PROJECT NUMBER	WORK AUTHORIZATION #	TOTAL CONTRACT AMOUNT INCLUDING CHANGE ORDERS	PROJECT COMPLETION DATE

(1) Name and Address of Small/Local Firm [Prime, Subcontractor, Supplier or Trucking Broker]	(2) Description of Work Performed and or Materials Supplied	(3) Prime and Sub(s) Original Bid Amount	(4) Port Certification Number	CONTRACT PAYMENTS					
				(5a) * LIABE Dollars	(5b) * LBABE Dollars	(5c) * SBE Dollars	(5d) * VSBE Dollars	(6) Date Work Completed	(7) Date of Final Payment
TOTAL				**$**	**$**	**$**	**$**		

List all certified local/small prime and subs regardless of tiers through out the life of the project, whether or not firms were listed on the original bid. Xerox this page if additional sheets are needed.
If actual sub dollars were different than the approval amount at time of award, provide comments on back of form. List actual amount paid to each sub at the above chart.

* LIABE (Local Impact Area Business Enterprise), LBABE (Local Business Area Business Enterprise), SBE (Small Business Enterprise), and VSBE (Very Small Business Enterprise).

I CERTIFY THAT THE ABOVE INFORMATION IS COMPLETE, TRUE AND CORRECT		
AUTHORIZED CONTRACTOR REPRESENTATIVE SIGNATURE and TITLE	**BUSINESS PHONE NUMBER**	**DATE**

Distribution: **Original – SRD** **Copy To – Engineering Construction / Resident Engineer**

Instructions--Monthly Utilization of Local and Small Business Enterprises

(I) Enter the project information requested on the first two rows on page 00816-1 (Prime Contractor, Business Address, Contract Bid Amount, etc.)

(II) Provide the following information **for each portion of the contract work performed by (and for each amount of materials supplied by) a Port-certified small and/or local business**, including the prime contractor if the prime is a Port-certified small/local business:

Column 1: Name and address of the firm performing work and/or supplying materials.
Column 2: Description of the work performed and/or materials supplied by said firm.
Column 3: For subcontractor, supplier or trucker: dollar amount of the bid submitted by the firm to prime bidder, as listed in the Subcontractor and Supplier List Form submitted by prime bidder with its bid. If the subcontractor, supplier or trucker was not listed in the Subcontractor and Supplier List Form, enter "0". For small/local prime bidder: dollar amount of the prime bidder's bid excluding all subcontractor/supplier/trucking broker bid amounts, as listed in the Subcontractor and Supplier List Form.
Column 4: Port Certification Number of firm. (Port-certified small/local subcontractors, suppliers and truckers should provide their certification number to the Prime Bidder and notify Prime Bidder in writing with the date of the decertification if their status changes during the course of the project.)
Columns 5a-5d Enter the dollar amount of the work performed and/or materials supplied by the firm in either Column 5a, 5b, 5c or 5d, depending on the firm's certification status. Firm certification status must be certified and determined at the time of bid by Port of Oakland. The certified firm is issued a letter by the Port of Oakland that states their certification status as well as the expiration date of the certification. Firms' certification status may be obtained by accessing the Port of Oakland website **(http://srd.portofoakland.com/** or by calling (510) 627-1627. Refer to the following table for a description of the certification status:

Certification Status	Description
LIABE (Local Impact Area Business Enterprise)	firm located in Oakland, Alameda, Emeryville, or San Leandro
LBABE (Local Business Area Business Enterprise)	firm located in Alameda County or Contra Costa County
SBE (Small Business Enterprise)	business with 3 year average annual gross revenue not to exceed $36,000,000
VSBE (Very Small Business Enterprise)	business with 3 year average annual gross revenue not to exceed $5,000,000

If the firm was decertified before completing its portion of the work of this contract, enter the dollar amount of ALL work performed/ materials supplied by the firm, INCLUDING WORK PERFORMED/MATERIALS SUPPLIED AFTER THE DATE OF DECERTIFICATION. **If the amount listed in Column 5 differs from the amount listed in Column 3, provide an explanation in the 'COMMENTS' section as provided.**

Column 6: Date on which the firm listed in Column 1 completed the work described in Column 2.
Column 7: Date on which prime contractor made the 'final payment' for the work described in Column 2 to subcontractor/supplier/trucking broker.

(III) In the 'TOTAL' row, enter the column sums of the dollar amounts listed in Columns 5a through 5d.

(IV) The authorized contractor representative shall certify the information supplied by signing in the space provided. **Per Port of Oakland provisions, Final Payment WILL NOT be made until this form is properly filled out and submitted to the Port of Oakland.**

COMMENTS:

PORT OF OAKLAND

Final Utilization of Local and Small Business Enterprises

PRIME CONTRACTOR	BUSINESS ADDRESS	CONTRACT BID AMOUNT	DATE OF THIS REPORT

PORT PROJECT NAME	PORT PROJECT NUMBER	WORK AUTHORIZATION #	TOTAL CONTRACT AMOUNT INCLUDING CHANGE ORDERS	PROJECT COMPLETION DATE

(1) Name and Address of Small/Local Firm [Prime, Subcontractor, Supplier or Trucking Broker]	(2) Description of Work Performed and or Materials Supplied	(3) Prime and Sub(s) Original Bid Amount	(4) Port Certification Number	CONTRACT PAYMENTS					
				(5a) * LIABE Dollars	(5b) * LBABE Dollars	(5c) * SBE Dollars	(5d) * VSBE Dollars	(6) Date Work Completed	(7) Date of Final Payment
TOTAL				**$**	**$**	**$**	**$**		

List all certified local/small prime and subs regardless of tiers through out the life of the project, whether or not firms were listed on the original bid. Xerox this page if additional sheets are needed.
If actual sub dollars were different than the approval amount at time of award, provide comments on back of form. List actual amount paid to each sub at the above chart.

* LIABE (Local Impact Area Business Enterprise), LBABE (Local Business Area Business Enterprise), SBE (Small Business Enterprise), and VSBE (Very Small Business Enterprise).

I CERTIFY THAT THE ABOVE INFORMATION IS COMPLETE, TRUE AND CORRECT		
AUTHORIZED CONTRACTOR REPRESENTATIVE SIGNATURE and TITLE	**BUSINESS PHONE NUMBER**	**DATE**

Distribution: **Original – SRD** **Copy To – Engineering Construction / Resident Engineer**

Instructions--Final Utilization of Local and Small Business Enterprises

(I) Enter the project information requested on the first two rows on page 00816-1 (Prime Contractor, Business Address, Contract Bid Amount, etc.)

(II) Provide the following information **for each portion of the contract work performed by (and for each amount of materials supplied by) a Port-certified small and/or local business**, including the prime contractor if the prime is a Port-certified small/local business:

Column 1: Name and address of the firm performing work and/or supplying materials.
Column 2: Description of the work performed and/or materials supplied by said firm.
Column 3: For subcontractor, supplier or trucker: dollar amount of the bid submitted by the firm to prime bidder, as listed in the Subcontractor and Supplier List Form submitted by prime bidder with its bid. If the subcontractor, supplier or trucker was not listed in the Subcontractor and Supplier List Form, enter "0". For small/local prime bidder: dollar amount of the prime bidder's bid excluding all subcontractor/supplier/trucking broker bid amounts, as listed in the Subcontractor and Supplier List Form.
Column 4: Port Certification Number of firm. (Port-certified small/local subcontractors, suppliers and truckers should provide their certification number to the Prime Bidder and notify Prime Bidder in writing with the date of the decertification if their status changes during the course of the project.)
Columns 5a-5d Enter the dollar amount of the work performed and/or materials supplied by the firm in either Column 5a, 5b, 5c or 5d, depending on the firm's certification status. Firm certification status must be certified and determined at the time of bid by Port of Oakland. The certified firm is issued a letter by the Port of Oakland that states their certification status as well as the expiration date of the certification. Firms' certification status may be obtained by accessing the Port of Oakland website **(http://srd.portofoakland.com/)** or by calling (510) 627-1627. Refer to the following table for a description of the certification status:

Certification Status	Description
LIABE (Local Impact Area Business Enterprise)	firm located in Oakland, Alameda, Emeryville, or San Leandro
LBABE (Local Business Area Business Enterprise)	firm located in Alameda County or Contra Costa County
SBE (Small Business Enterprise)	business with 3 year average annual gross revenue not to exceed $36,000,000
VSBE (Very Small Business Enterprise)	business with 3 year average annual gross revenue not to exceed $5,000,000

If the firm was decertified before completing its portion of the work of this contract, enter the dollar amount of ALL work performed/ materials supplied by the firm, INCLUDING WORK PERFORMED/MATERIALS SUPPLIED AFTER THE DATE OF DECERTIFICATION. **If the amount listed in Column 5 differs from the amount listed in Column 3, provide an explanation in the 'COMMENTS' section as provided.**

Column 6: Date on which the firm listed in Column 1 completed the work described in Column 2.
Column 7: Date on which prime contractor made the 'final payment' for the work described in Column 2 to subcontractor/supplier/trucking broker.

(III) In the 'TOTAL' row, enter the column sums of the dollar amounts listed in Columns 5a through 5d.

(IV) The authorized contractor representative shall certify the information supplied by signing in the space provided. **Per Port of Oakland provisions, Final Payment WILL NOT be made until this form is properly filled out and submitted to the Port of Oakland.**

COMMENTS:

PORT OF OAKLAND

Non-Discrimination and Small Local Business Utilization Policy Program Affidavit

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

I hereby certify that I_____(Legal Name of Respondent/Supplier/Consultant/Contractor), shall carry out applicable requirements in the award and administration of this contract and cooperate with the Port of Oakland in meeting its commitments and objectives with regard to ensuring nondiscrimination, and shall use best efforts to ensure that barriers to participation of Small Local Businesses do not exist.

Upon execution of an Agreement, the selected consultant will be required to complete Small and Local attainment reports and a final report at contract completion, and submit them to the Social Responsibility Division.

I declare under penalty of perjury under the laws of the State of California that the information I have provided herein is true and correct.

_____
Signature

_____
Print Name

_____
Title

_____
Date

PORT OF OAKLAND

City of Oakland City Charter § 728
Living Wage Information

EMPLOYERS SUBJECT TO §728 OF THE CITY CHARTER MUST COMPLY WITH THE FOLLOWING REQUIREMENTS:

1) Pay all non-exempt employees the living wage rates (As of July 1, 2021, $17.56 without health benefits or $15.30 with health benefits). Port Ordinance No. 3666, as amended also requires that covered businesses provide employees at least twelve compensated days off per year, including holidays.
2) Pay at least $2.26 per hour worked toward the provision of health care benefits for employees and/or their dependents, if the employer claims credit for health benefits.
3) **Provide written notification to each current and new employee, at time of hire, of his or her rights to receive the benefits under the provisions of these regulations.** The notification shall be provided in English, Spanish and other languages spoken by a significant number of the employees, and shall be posted prominently in communal areas at the work site. A copy of said notification is available from the Port Division of Social Responsibility.
4) Provide all employees earning less than $12/hour notification in English, Spanish, and any other language spoken by a significant number of employees of their right to advance Earned Income Credit payments.
5) **Submit name, address, date of hire, occupation classification, rate of pay, benefits paid for each of its employees, and compensated time off in a web accessed monitoring system at https://www.elationsys.com/app/Registration/ by March 31st, June 30th, September 30th, and December 31st of each year.** If a covered employer has obtained a waiver from the Port Board of Directors, then the employer must still submit an annual payroll report covering each of its employees by December 31st of each year. Failure to provide the list within five days of the due date will result in a penalty of $500 per day. Covered employers shall maintain payrolls and basic records for all employees and shall preserve them for a period of at least three years after the close of the compliance period.
6) Require subcontractors, tenants and subtenants, or licensees who are covered by these requirements to comply with the provisions of these regulations. **Covered employers shall be responsible for including language committing the subcontractor's, tenant's or licensee's agreement to comply, in the contract with the subcontractor**. Covered employers shall submit a copy of such subcontracts or other such agreements to the Port Division of Social Responsibility.
7) Permit authorized Port representatives access to work sites and, with employee consent, relevant payroll records for the purpose of monitoring compliance with these regulations, investigating employee complaints of non-compliance and evaluating the operation and effects of these regulations, including the production for inspection and copying of its payroll records for any or all of its employees for the applicable compliance period. Permit a representative of the labor organizations in its industry to have access to its workforce at the Port during non-working time and in non-work areas to ensure compliance.

Employers who fail to submit documents, declarations or information required to demonstrate compliance with these regulations shall be deemed noncompliant or non-responsive and subject to the remedies as set forth in §728.

PORT OF OAKLAND

Employer Self-Evaluation for Port of Oakland Living Wage

COVERED BUSINESS CHECKLIST WRITE YES/NO ANSWER IN APPROPRIATE BOX:

1. ☐ Is the Business entering into a contract, tenancy agreement or subordinate agreement (such as, subcontract, subtenancy, or sublicense) with the Port? *If no, go on to question 2. If yes, go to question 3.*

2. ☐ Has the Business amended an existing contract, tenancy agreement or subordinate agreement at any time since April 2002? *If no to 1 and 2, stop here: the business is not covered. If yes, go to question 3.*

3. ☐ Is the contract with Aviation or Maritime divisions for a value of greater than $50,000 over the life of the contract (over the next five years if contract is for less than a year and expected to be renewed or extended)? *If no, stop here; the contract is not covered. If yes, go to question 4.*

4. ☐ Is the contract for service other than the delivery of products, equipment or commodities? *If no, stop here: the business is not covered. If yes, go to question 5.*

5. ☐ Does the Business employ more than 20 employees who spend at least 10 hours per week (4 hours per week if part time employees) working under the contract with the Port or on Port property? Indicate the number of employees that are employed by the Contractor_____. *If no, stop here the business is not covered. If yes, go to question 6, exemptions for specified employees of a covered employer.*

All employees of a covered employer are required to be provided compensation and other benefits as provided under §728 of the Charter, except for specified employees exempt under the following exemptions. The following questions should be answered for each employee.

6. ☐ *Does the employee work less than 25% of his/her time (10 hours per week for full time employee) under the contract with the Port?* If yes, stop here; the specified employee is exempt. If no, go to question 7.

7. ☐ *Is the employee under 21 years of age, employed by a government agency or nonprofit for after school or summer employment, or as a trainee for 90 days or less?* If yes, stop here; the specified employee is exempt. If no, go to question 8.

8. ☐ *Has the Business obtained a waiver that covers the employee?* If yes, stop here; the specified employee is exempt. If no, go to question 9.

9. ☐ *Is the employee participating in a bona-fide temporary job-training program in which a significant part of the compensation consists of acquiring specialized knowledge, abilities or skills in a recognized trade?* If yes, stop here; the specified employee is exempt. If no, go to question 10.

10. ☐ *Is the employee a volunteer who is not compensated other than for incidental expenses or stipends?* If yes, stop here; the specified employee is exempt. If no, go to question 11.

11. ☐ *Is the employee working for the Business less than 20 hours per week for a period of 6 months or less?* If yes, stop here the specified employee is exempt. If no, go to question 12.

12. ☐ *Of the remaining employees (employees for which no exemption applies as indicated by your answers to questions 6 through 11), are there 20 or fewer non-exempt employees working for the employer under the Port Contract?* If yes, stop here; each of the remaining specified employee(s) is/are exempt. If no, each of the remaining specified employee(s) is covered by §728.

The undersigned authorized representative of Contractor hereby certifies under penalty of perjury that all of the information on this form is true and accurate.

_____ Company Name	_____ Signature of Authorized Representative
_____ Address	_____ Type or Print Name & Title
_____ Area Code and Phone	_____ Email Address
_____ Name of Primary Contact	_____ Date

_____
Project Name (Be Specific)

Submit Completed Checklist To:
Amy Tharpe

Port of Oakland
Social Responsibility Division
530 Water Street
Oakland, CA 94607
Phone: (510) 627-1302
Email: atharpe@portoakland.com

PORT OF OAKLAND

Certificate of Compliance – Living Wage

The City of Oakland Living Wage Charter §728 ("§728") and Port Ordinance No. 3666 ("Ordinance 3666") as amended, provide that certain employers that enter into a contract, lease, license (or a subcontract, sublease, sublicense, or other agreement) with the Port for $50,000 or more over the term of the contract and certain recipients of Port financial assistance for $50,000 or more shall pay a prescribed minimum level of compensation to their covered employees ("Employees").

The undersigned ("Contractor") submits this certificate under penalty of perjury and as a condition of payment of its invoice(s) for service provided under the _____ agreement between the Port and Contractor.

1) Contractor hereby certifies that it is in compliance with §728 and Ordinance 3666 with respect to all non-exempt Employees of Contractor engaged in Port-related employment or work on Port property.
2) Contractor herby acknowledges that the Port is relying on Contractor's certification of compliance with §728 and Ordinance 3666 as a condition of payment of Contractor's invoice(s).
3) Contractor understands that it may be subject to fines or penalties for noncompliance with §728 and Ordinance 3666 up to and including potential fines of $500 per day until Contractor complies.
4) Contractor hereby certifies that claims, records and statements relating to Contractor's compliance with §728 and Ordinance 3666 are true and accurate, that such claims, records and statements are made with the knowledge that the Port will rely on such claims, records and statements, and that such claims, records and statements are submitted to the Port for the express benefit of Contractor's employees engaged in Port-related employment or work on Port property.

Please check the appropriate box and sign below

☐ Contractor hereby certifies its compliance with all of its obligations under §728 and Ordinance 3666;

☐ Contractor hereby certifies that all Employees of Contractor working under Contractor's contract with the Port are compensated at wage rate(s) greater than $12.00 per hour;

☐ Contractor hereby certifies that it is not currently covered by §728 or Ordinance 3666. Contractor further certifies that should §728 or Ordinance 3666 become applicable, Contractor will comply with all of its Living Wage obligations.

All terms used herein and not defined shall have the meaning ascribed to such terms in §728 and Ordinance 3666.

The undersigned authorized representative of Contractor hereby certifies under penalty of perjury that all of the information on this form is true and accurate.

_____ Company Name	_____ Signature of Authorized Representative
_____ Address	_____ Type or Print Name & Title
_____ Phone and Email	_____ Date

_____ Project Name (Be Specific)

Submit to: Amy Tharpe, Port of Oakland, Social Responsibility Division, 530 Water Street, Oakland, CA 94607. Email: atharpe@portoakland.com

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

I hereby certify that I_____(Legal Name of Respondent/Supplier/Consultant/Contractor), has reviewed the Living Wage Requirements, included herein as Attachment 7 to this Request for Proposal and will comply with said Requirements. Upon execution of an Agreement, the selected consultant will be required to complete the Employer Self-Evaluation Form and Certificate of Compliance – Living Wage Form of this Request for Proposal, and submit them to the Social Responsibility Division.

I declare under penalty of perjury under the laws of the State of California that the information I have provided herein is true and correct.

_____
Signature

_____
Print Name

_____
Title

_____
Date

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

All the Port's Insurance requirements are incorporated into the Port's Standard Professional Services Agreement attached to this Request for Proposal **(Attachment 11).**

PORT OF OAKLAND

Insurance Acknowledgement Statement

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

I hereby certify that _____ (Legal Name of Respondent) agrees to meet all of the Port's Insurance requirements included in the Professional Services Agreement attached to this Request for Proposal and Respondent will be able to evidence such insurance when and if awarded the contract and will provide proof of insurance at the time of project award if awarded the contract.

I declare under penalty of perjury under the laws of the State of California that the information I have provided herein is true and correct and is of my own personal knowledge.

_____
Signature

_____
Print Name

_____
Title

_____
Date

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

Professional Services Agreement

(Attachment 11)

RFP No. 21-22/33

ATTACHMENT 11

PROFESSIONAL SERVICES AGREEMENT
("Agreement")

Between

CITY OF OAKLAND, A MUNICIPAL CORPORATION,
ACTING BY AND THROUGH ITS BOARD OF PORT COMMISSIONERS
("Port of Oakland")

And

_____
("Consultant")

[Development, Implementation, and Maintenance of Identity Management System (IdMS) at Oakland International Airport]

[Contract No., if any]

Reference Date

_____

Table of Contents

Appendices

THIS PROFESSIONAL SERVICES AGREEMENT ("Agreement") is entered into between the Port and Consultant (as defined below, and collectively referred to as the "Parties"), who agree as follows. All Appendices described herein are attached and made part of this Agreement.

1. Parties

1.1 **Consultant.** Consultant is identified in **Appendix D (Parties)** ("Consultant"). Consultant shall at all times be deemed an independent contractor wholly responsible for the manner in which it performs the Services, and fully liable for the acts and omissions of its employees, subconsultants, and agents. Under no circumstances shall this Agreement be construed as creating an employment, agency, joint venture, or partnership relationship between the Port and Consultant, and no such relationship shall be implied from performance of this Agreement. References in this Agreement to direction from the Port shall be construed as providing for direction as to policy and the result of services only, and not as to means and methods by which such a result is obtained.

1.2 **Port.** This Agreement is entered into by the City of Oakland, a municipal corporation, acting by and through its Board of Port Commissioners ("Port of Oakland" or "Port"). The Port's Project Manager ("Project Manager") is identified in **Appendix D (Parties)**.

2. Term

2.1 **Term.** The term of this Agreement ("Term") is described in **Appendix A (Services)**. Unless otherwise provided in this Agreement, this Agreement shall be effective during the Term, provided it has been signed by the Parties and approved as to form and legality by the Port Attorney.

2.2 Suspension and Early Termination.

2.2.1 **Suspension.** The Port may (in writing and without cause) direct Consultant to suspend, delay, or interrupt the Services, in whole or in part, for such periods of time as the Port may determine in its sole discretion. Such suspension of Services shall be treated as an excusable delay.

2.2.2 **Port Termination for Cause.** The Port may (in writing) terminate this Agreement in whole, or from time to time in part, for cause, should Consultant commit a material breach of all or part of this Agreement and not cure such breach within ten (10) calendar days of the date of the Port's written notice to Consultant demanding such cure. Upon such Port termination for cause, Consultant shall be liable to the Port for all loss, cost, expense, damage, and liability resulting from such breach and termination.

2.2.3 **Port Termination for Convenience.** The Port may (in writing) terminate this Agreement in whole, or from time to time in part, for convenience as the Port may determine in its sole and reasonable discretion. Upon such Port termination for convenience, Consultant shall be entitled to recover its costs expended up to the termination plus reasonable profit thereon to the termination date, but may recover no other cost, damage, or expense.

3. Services

3.1 **Scope of Services.** Consultant shall perform all services ("Services") described in **Appendix A (Services)**. All Services whenever performed shall be deemed performed under this Agreement.

3.2 **Standard of Performance.** Consultant represents that it possesses all necessary training, licenses, permits, and approvals to perform the Services, and that its performance of the Services will conform to the standard of practice of a person (or persons) specializing in performing professional services of a like nature and complexity to the Services.

3.3 **Subconsultants.** Consultant shall perform the Services using any persons and subconsultants listed in **Appendix A (Services)**. Consultant shall hire only qualified persons or firms who are experienced in performing work of a like nature and complexity as the Services, and who agree to be bound to the terms of the Agreement to the extent of the scope of Services. Consultant may substitute personnel or subconsultants prior to any such personnel or subconsultants commencing work only upon the Project Manager's written consent, which may be withheld or delayed in the Port's sole discretion. When using any person who has retired from a California Public Employees' Retirement System ("CalPERS") agency, Consultant and any subconsultants shall comply with all laws and regulations applicable to CalPERS.

3.4 **Ownership of Non-Software Work Product.** Any interest (including copyright interests) of Consultant or its subcontractors or subconsultants, in studies, reports, memoranda, computational sheets, drawings, plans, or any other documents (including electronic media) prepared by Consultant or its subcontractors or subconsultants in connection with the Services (but not including any Software, unless otherwise provided in this Agreement), shall become the property of the Port. To the fullest extent permitted by Title 17 of the United States Code, work product produced under this Agreement shall be deemed works for hire and all copyrights in such works shall be the Port's property. With the Port's prior written approval, Consultant may retain and use copies of such works for reference and as documentation of experience and capabilities.

If the Services include any Software, any licensing or ownership matters shall be addressed in **Appendix A-1** (Software).

4. Payment

4.1 **Payment Terms.** Consultant shall perform the Services for compensation only set forth in **Appendix B (Payment)** ("Payment"). All compensation paid to Consultant on account of the Services performed shall be deemed payments under this Agreement.

4.2 **Taxes.** Consultant shall, without additional compensation, pay all applicable taxes (including California sales and use taxes and the City of Oakland business tax), deficiency, interest, or penalty levied upon or asserted with respect to this Agreement, the Services performed thereunder, or the goods delivered hereunder, regardless of which Party has liability for such payment under applicable law. Consultant shall collect, report, and pay all applicable California sales and use taxes and shall, in accordance with California Revenue and Taxation Code Section 6203, issue the Port a receipt relieving the Port of all liability for any tax relating to this Agreement. Consultant shall comply with all applicable administrative regulations relating to the assumption of liability for the payment of payroll taxes and contributions under this Section and shall provide all necessary information with respect thereto to the proper authorities.

5. Insurance; Indemnification

5.1 **Insurance.** Consultant shall, at its own expense and during the Term, maintain in force the insurance in the types and amounts required by **Appendix C (Insurance)**.

5.2 **Indemnification.** Consultant shall comply with all provisions set forth in **Appendix F (Indemnification)**.

6. Compliance With Laws

6.1 **Compliance With All Laws.** Consultant shall comply with all laws, regulations, ordinances, rules, permits, or land use restrictions or limitations at any time applicable to the Services ("All Laws"), including those applicable to any public or governmental authority (including the City of Oakland and the Port, such as the City Charter), regardless of whether All Laws are specifically stated in this Agreement or are in effect at the beginning of the Term. Consultant further represents that all plans, drawings, specifications, designs and any other product of the Services will comply with All Laws, consistent with the standard of care in this Agreement.

Consultant's compliance with All Laws shall include, but not be limited to, compliance with the following, to the fullest extent applicable:

6.1.1 Oakland Living Wage provisions, including Section 728 of the Oakland City Charter and Port Ordinance Nos. 3666 and 3719.

6.1.2 Security requirements imposed by authorities with jurisdiction over the Services (such as the Federal Aviation Administration and U.S. Department of Transportation), which may include providing information, work histories, and/or verifications requested by such authorities for security clearances or compliance.

6.1.3 If the Services are part of a "public works" or "maintenance" project, California Department of Industrial Relations ("DIR") requirements, which include compliance with California Labor Code Sections 1725.5 and 1771.1, Consultant and subconsultant registration with DIR and licensing by the California Contractors State License Board, and compliance with all laws, regulations, and other requirements for public works of improvement.

6.2 **Non-Discrimination.** Consultant shall not discriminate against or harass any employee or applicant for employment because of race, color, religion, sex, national origin, ancestry, age (over 40), physical or mental disability, cancer-related medical condition, known genetic pre-disposition to a disease or disorder, veteran status, marital status, or sexual orientation. Consultant shall take affirmative action to ensure that applicants and employees are treated fairly with respect to all terms and conditions of employment, which include (without limitation): hiring, upgrading, recruitment, advertising, selection for training or apprenticeship, demotion, transfer, compensation, layoff, or termination. Consultant acknowledges it has reviewed, or had a full opportunity to review, the current version of the Port's Discrimination Complaint Procedures/Unlawful Harassment Policy and Complaint Procedures, which provide an effective and expedited method of resolving employment discrimination allegations and prevent unlawful workplace harassment.

6.3 **Conflicts of Interest.** Consultant shall comply with all applicable laws and regulations relating to conflicts of interest, including any requirements adopted by the City of Oakland or the Port. Consultant represents that it is familiar with California Government Code

Sections 1090 and 87100 et seq., and that it does not know of any facts that may constitute a violation of said sections.

Consultant represents that, to the best of its knowledge, it has disclosed to the Port all facts bearing upon any possible interests, direct or indirect, Consultant believes that any employee, officer, or agent of the Port presently has, or will have, in this Agreement, in the Services, or in any portion of the profits hereunder. Willful failure to make such disclosure, if any, shall constitute grounds for termination of this Agreement by the Port for cause.

Consultant covenants that it shall never have any interest (direct or indirect) that would conflict in any manner with the performance of the Services under this specific Agreement, including an interest Consultant has (or may have in the future) with a person or entity that has an interest adverse or potentially adverse to the Port with respect to this specific Agreement, as determined in the reasonable judgment of the Port.

Provided that this Agreement or the performance thereof does not violate any applicable conflict of interest laws, nothing in this Section shall serve to prevent Consultant from providing services similar to the Services to other entities. The provisions of this Section shall survive the termination of this Agreement.

6.4 FAA AIP Grant-Required Provisions. Consultant shall comply with all provisions in Appendix E (FAA AIP Grant-Required Provisions).

7. Confidentiality; Publicity

7.1 **Confidentiality.** Consultant acknowledges that, in the performance of the Services or in the contemplation thereof, Consultant may have access to private or confidential information that may be owned or controlled by the Port, the disclosure of which to third parties may be damaging to the Port. Consultant agrees that all information disclosed by the Port to or discovered by Consultant shall be held in strict confidence and used only in performance of the Agreement. Consultant shall exercise the same standard of care to protect such information as a reasonably prudent consultant would use to protect its own proprietary data, and shall not accept employment adverse to the Port's interests where such confidential information could be used adversely to the Port's interests. Consultant shall notify the Port immediately in writing if Consultant is requested to disclose any information made known to or discovered by Consultant during the performance of the Services. The provisions of this Section shall survive the termination of this Agreement.

7.2 **Publicity.** Any publicity or press releases with respect to the Project or Services shall be under the Port's sole discretion and control. Consultant shall not, without the Port's prior written consent, discuss the Services or Project, or matters pertaining thereto, with the public press, representatives of the media, or public bodies or representatives of public bodies. Consultant shall have the right, however, to include representations of Services among Consultant's promotional and professional material, and to communicate with persons or public bodies where necessary to perform the Services. The provisions of this Section shall survive the termination of this Agreement.

8. Audit and Inspection

8.1 **Retention.** Consultant shall maintain unaltered all Records during the Retention Period.

8.1.1 "Retention Period" means the Term and an additional three (3) years following the later of: (a) termination of this Agreement, (b) the Port's final payment under this

Agreement, or (c) resolution of pending issues between the Parties under this Agreement.

8.1.2 "Records" means full and adequate records, in electronic and other mediums, related to this Agreement or prepared by or furnished to Consultant during the course of performing the Services or which show the actual costs incurred by Consultant in the performance of this Agreement, including (without limitation) documents, correspondence, internal memoranda, calculations, books and accounts, accounting records documenting work under this Agreement, invoices, payrolls, and data.

8.2 **Audit and Tolling.** During the Retention Period, the Port may Audit the Records. Consultant agrees to toll all applicable periods of any statutes of limitations: (a) commencing on the first day of an Audit and ending four (4) years after the Port delivers to Consultant the final Audit findings; (b) commencing on the first day of an Audit and ending four (4) years after the Port's completion of the Audit, if no final Audit findings are produced; and (c) commencing on the day the Port's claim or right or cause of action arises with regard to any matter under this Agreement and ending four (4) years thereafter.

8.2.1 "Audit" means to audit, inspect, make copies of, and obtain excerpts and transcripts from the Records.

8.3 **Production.** During an Audit or as otherwise requested by the Port, Consultant shall Produce Records to the Port or the Port's designated representatives. If Consultant fails to Produce Records to the Port within ten (10) business days of the Port's written request, Consultant shall pay the Port a delinquency charge of $25 for each day it does not Produce Records. The Parties agree that such delinquency charges are liquidated damages that represent a reasonable estimate of expenses the Port will incur because of Consultant's failure to Produce Records, and that such charges shall be deducted from the Port's next payment to Consultant.

8.3.1 "Produce" means to, at no cost to the Port and within ten (10) business days of the Port's written request, provide the Port (or the Port's representatives): (a) copies of Records requested by the Port; (b) the ability for the Port to inspect the Records at a location within a fifty (50) mile radius from the Port offices at 530 Water Street, Oakland, California, or if the Records are not located within said fifty mile radius, the ability for the Port to inspect the Records at another location after Consultant pays the Port all reasonable and necessary costs incurred (including, without limitation, travel, lodging, and subsistence costs); and (c) copies of Records in electronic format through extracts of data files in a computer readable format, such as email attachments, data storage devices, or another adequate electronic format.

9. Performance Milestones and Liquidated Damages.

9.1 The Port and Consultant recognize that time is of the essence of this Agreement and that the Port will suffer financial loss in the form of contract administration expenses (including project management and Consultant's expenses) if Services are not completed within the time specified herein. Consultant and the Port agree that because of the nature of the Services, it would be impractical or extremely difficult to fix the amount of actual damages incurred by the Port because of a delay in completion of the Services. Accordingly, the Port and Consultant agree that as liquidated damages, Consultant shall pay the Port as follows:

9.1.1 If Consultant's staff does not respond to Critical issues (as described more fully in Appendix A, Section 3.3.1) within the response time specified in Section 3.3.1 of Appendix A, one thousand dollars ($1,000) for each day Consultant fails to respond, or portion thereof until Consultant responds.

9.1.2 If Consultant's staff does not respond to Non-Critical issues (as described more fully in Appendix A, Section 3.3.2) within the response time specified in Section 3.3.2 of Appendix A, two hundred and fifty dollars ($250) for each day Consultant fails to respond, or portion thereof until Consultant responds.

9.1.3 If Consultant fails to repair or replace and restore the System to full System operation within twelve (12) hours of the initial cause that disabled the System, one thousand dollars ($1,000) for each day, or portion thereof, until full restoration of the System.

9.1.4 These measures of liquidated damages shall apply cumulatively and shall be presumed to be, except as provided below, the damages suffered by the Port resulting from delay in completion of work.

9.1.5 Liquidated damages for delay shall only cover administrative, overhead, general loss of public use damages, interest on bonds and lost revenues, suffered by the Port as a result of delay. Liquidated damages shall not cover the cost of completion of the Services, damages resulting from defective Services, costs of substitute facilities or damages suffered by others who then seek to recover their damages from the Port (for example, delay claims of other contractors, subcontractors, tenants, or third-parties, and defense costs thereof).

9.2 **Collection Costs and Attorneys' Fees**. Consultant shall be responsible for paying all fees, costs, and expenses, including attorneys' fees (including in-house time of the Port Attorney's Office) and costs, incurred by the Port in collecting unpaid Liquidated Damages.

10. Notices; Agent for Service of Process

10.1 Notices. The Port's and Consultant's Notice Addresses are set forth in **Appendix D (Parties)**, unless otherwise amended in writing with notice to the other Party. All notices or other communications given or required to be given under this Agreement shall be effective only if given in writing to the Party's Notice Address and: (a) sent by certified mail with return receipt requested, (b) sent by overnight delivery service, or (c) delivered personally. Any such notice shall be deemed to have been given: (x) five calendar days after the date it was sent by certified mail; (y) one business day after the date it was sent by overnight delivery service; or (z) on the date personal delivery was made. The Parties shall also endeavor to send courtesy copies of all notices and communications electronically.

10.2 **Agent for Service of Process.** Pursuant to California Code of Civil Procedure, Section 416.10, Consultant hereby designates an agent for service of process as identified in **Appendix D (Parties)**. Consultant may at any time designate a new agent for service in the State of California by providing written notice in compliance with this Agreement of the full name and address of its new agent. No attempt to revoke the agent's authority to receive service shall be valid unless the Port has first received a duly executed designation of a new agent meeting the requirements of California law.

11. Disputes; Statutes of Limitation; Governing Law

11.1 **Dispute Resolution.** In the event of any dispute between the Parties under this Agreement, the Parties shall make their best efforts to meet and confer in good faith to resolve the dispute amicably. Consultant shall continue its work throughout the course of any dispute, and Consultant's failure to continue work during a dispute shall be a material breach of this Agreement.

11.2 **Attorneys' Fees.** If either Party commences an action against the other in connection with this Agreement, the prevailing party shall be entitled to recover from the losing party reasonable attorneys' fees and costs of suit.

11.3 **Statutes of Limitation.** As between the Parties, any applicable statute of limitations for any act or failure to act shall commence to run on (a) the date of the Port's issuance of the final Certificate for Payment or termination of this Agreement, or (b) termination of this Agreement, whichever is earlier, except for latent defects, for which the statute of limitation shall begin running upon discovery of the defect and its cause.

11.4 **Governing Law.** This Agreement shall be construed and interpreted in accordance with the laws of the State of California, without regard to principles of conflict of law. Consultant hereby consents to the exclusive jurisdiction of the state and federal courts in Alameda County, California and/or the United States District Court for the Northern District of California, and any actions arising out of or filed in connection with this Agreement shall be filed solely in such courts.

12. Miscellaneous

12.1 **No Third Party Beneficiaries.** Except as expressly provided in this Agreement, nothing in this Agreement shall confer rights or benefits on persons or entities not party to this Agreement.

12.2 **Time of the Essence.** Time is of the essence in the performance of this Agreement.

12.3 **No Waiver.** Any progress payments, approvals, inspections, reviews, oral statements, or certifications by any Port representative or by any governmental entity with respect to this Agreement shall in no way limit Consultant's obligations under this Agreement. Either Party's waiver of any breach, or the omission or failure of either Party, at any time, to enforce any right reserved to it, or to require strict performance of any provision of this Agreement, shall not be a waiver of any other right to which any Party is entitled, and shall not in any way affect, limit, modify, or waive that Party's right thereafter to enforce or compel strict compliance with every provision hereof.

12.4 Covenant Against Contingent Fees. As required by the Port's Purchasing Ordinance No. 4321 (as it may be amended from time to time), Consultant warrants that no person or agency has been employed or retained to solicit or obtain the Agreement upon an agreement or understanding for a contingent fee, except a bona fide employee or agency. For breach or violation of this warranty, the Port, at its option, may annul the Agreement or deduct from the contract price or otherwise recover from Consultant the full amount of the contingent fee. The following definitions apply to this Section:

12.4.1 "bona fide agency" means an established commercial or selling agency, maintained by Consultant for the purpose of securing business, that neither exerts nor proposes to exert improper influence to solicit or obtain the Port contracts nor holds

itself out as being able to obtain any Port contract or contracts through improper influence.

12.4.2 "bona fide employee" means a person, employed by Consultant and subject to Consultant's supervision and control as to time, place, and manner of performance, who neither exerts nor proposes to exert improper influence to solicit or obtain the Port contracts nor holds itself out as being able to obtain any Port contract or contracts through improper influence.

12.4.3 "contingent fee" means any commission, percentage, brokerage, or other fee that is contingent upon the success that a person or concern has in securing a Port contract.

12.4.4 "improper influence" means any influence that induces or tends to induce a Port Commissioner, employee or officer to give consideration or to act regarding a Port contract on any basis other than the merits of the matter.

12.5 **Warranty of Signatories.** Every person signing this Agreement on behalf of Consultant represents and warrants that such person has sufficient authority to sign this Agreement and create a valid and binding obligation on Consultant.

12.6 **Counterparts.** This Agreement may be executed in counterparts, each of which shall be deemed an original instrument and all such counterparts, taken together, shall constitute one and the same instrument. Signatures delivered by facsimile or electronic mail shall be deemed effective as originals.

12.7 **Severability.** If any provision (or portion thereof) of this Agreement is found to be invalid by a court, arbitrator, or government agency of competent jurisdiction, the remainder of this Agreement shall remain in full force and effect. If any provision (or portion thereof) of this Agreement is prohibited by, or made unlawful or unenforceable under any applicable law of any jurisdiction, such provision shall, as to such jurisdiction, be ineffective without affecting the remainder of this Agreement, which shall be enforceable to the fullest extent permitted by law. To the greatest extent permitted by law, the provisions of such applicable law are hereby waived so that this Agreement may be deemed to be a valid and binding agreement.

12.8 **Entire Agreement.** This Agreement contains the entire, exclusive, and integrated agreement between the Parties regarding the subject matter of this Agreement and shall supersede any and all prior negotiations, representations, understandings, or agreements, written or oral, express or implied, that relate in any way to the subject matter of this Agreement. All prior negotiations are merged into this Agreement and shall be inadmissible in any enforcement of this Agreement. This Agreement may not be modified, nor may compliance with any of its terms be waived, except by mutual written agreement by the Parties.

[SIGNATURES CONTINUED ON NEXT PAGE]

IN WITNESS WHEREOF, the parties hereto have executed this Agreement.

PORT OF OAKLAND	**CONSULTANT**
CITY OF OAKLAND, a municipal corporation, acting by and through its Board of Port Commissioners, By: _____ **DANNY WAN,** Executive Director _____ **THIS AGREEMENT SHALL NOT BE VALID OR EFFECTIVE FOR ANY PURPOSE UNLESS AND UNTIL SIGNED BY THE PORT ATTORNEY.** Approved as to form and legality: _____ **MARY C. RICHARDSON,** Port Attorney (Or Assistant Port Attorney or Deputy Port Attorney signing on behalf of) **Port Resolution/Ordinance No.:** **Board Approval Date:** **PA#: 2022-**	_____, a [State] [business form/type, i.e. corporation, etc.], By: Name: Title: Email: _____ ***ATTEST*** (only if California Corp.) By: Name: Title: Email:

APPENDIX A

SERVICES

Consultant and Port agree that the terms and conditions set forth in the body of this Agreement or in the other Appendices supersede any term, condition, or other language in this Appendix A (or any other document attached to this Appendix A, other than Appendix A-1) that conflicts with or is inconsistent with those terms and conditions.

[The below scope, terms and requirements are a partial list of the minimum scope and terms of Consultant's services; the complete Scope of Work will be inserted following award and prior to the finalization of any associated agreement.]

A. SCOPE OF WORK

If applicable, the following capitalized terms, as used in this Agreement or in this Appendix or any of the other Appendices, have the following meanings:

☒ "Software" means: any and all computer software required for the System (as defined below), including any add-on modules, hardware firmware and updates thereto.

☒ "Equipment" means: all equipment (including hardware) required for seven (7) fully equipped badging workstation setups and one (1) additional setup for testing purposes, and includes the following:

a. Badge Printer (Networked)	Quantity 5
b. LiveScan	Quantity 7
c. Camera	Quantity 7
d. Multi-page Document Scanner	Quantity 7
e. DL/Passport Scanner	Quantity 7

1. **General**. Consultant shall develop and implement an automated and paperless Identity Management System to issue and manage Airport Identification badges with access to Sterile, Secured, and Security Identification Display Area (SIDA) areas ("SIDA Badges"); and keys with access to restricted areas of the Oakland International Airport (Airport)("System" or "IdMS").

Consultant shall also provide warranty and ongoing maintenance and support of the System, once deemed "Accepted" by the Port (as used in this Agreement, the term "Accepted" refers to when the System has been installed, activated, set up and configured to the Port's satisfaction and has passed all testing parameters set forth in in this Agreement, and has been accepted in writing by the Port, confirming that the setup has been complete, all testing has been completed and passed, and the System is live). Consultant's services under this Agreement are collectively referred to as "Services" and set forth in more detail below. Consultant's Services are broken down into three phases/categories: (1) Phase 1 - System Development and Implementation; (2) Phase 2 - Ongoing Maintenance and Support; and (3) As -Needed System Changes/Improvements.

Consultant's Services shall be performed in accordance with the additional terms, conditions and requirements as set forth in the attached Appendices (Appendix A-1 (Software); Appendix A-2 (System Badge Application Workflow Processes); Appendix A-3 (System User Groups); Appendix A-4 (Citation

Requirements and Citation/Violation Workflow Processes); and Appendix A-5 (System Specifications/Requirements), which are incorporated herein by reference.

2. Phase 1 – Development and Implementation of the System

Consultant shall develop and implement the System, will include all Software, Software customization, training, and Equipment. The System shall manage the approximately 6,500 active SIDA Badges previously issued by the Port for all Port staff and non Port staff (for purposes of this Agreement, non Port staff includes, but it not limited to employees of the airlines, tenants, contractors, concessionaires, consultants, and government (local, State, and Federal) agencies conducting business at the Airport or otherwise requiring SIDA Badges, as directed and approved by the Port) as well as process and manage all new and renewal badge applicantions, issue replacement badges, and manage all vehicle permits, keys and citations, including but not limited to cyber and metal keys, and ramp permits.

Consultant shall review and be familiar with the Port-provided information and documentation that reflects the Port's existing business processes for Airport SIDA Badging and ensure the System incorporates and integrates with the processes. Consultant shall also ensure that the System follows the workflow processes as depicted in the Appendices A-2 through A-4.

Consultant shall configure the System and assign system privileges and access rights for System Users (as used in this Agreement, the term "System Users" refers to both Port staff and non-Port staff, as directed and approved by the Port) in accordance with Appendix 5 (System User Groups), which identifies the various users of the System, their functional capabilities and the rules that impact their privileges.The System shall integrate, at a minimum, with all of the following existing other systems used by the Port related to SIDA Badging:

(1) Crossmatch fingerprint systems (or comparable system as approved by the Port Project Manager);

(2) TSA Designated Aviation Channeling (DAC) service provider (Telos ID);

(3) Learning Management system (SSi);

(4) Access control system (C•CURE 9000); and,

(5) Cyber keys (Videx CyberLock).

3. Phase 2 – Warranty; Ongoing Maintenance and Support

Following the Port's Acceptance of the System, Consultant shall provide warranty, ongoing maintenance, and support for the System, as set forth in more detail below.

3.1 Warranty

Consultant warrants that the System, including the Software, will be free of defects in workmanship and materials for a period consistent with industry standards and the nature of the Services, for a one year period of time following Acceptance by the Port of the System ("Warranty Period"). Consultant shall also take all measures to ensure the Equipment is covered by a manufacturer's warranty of no less than one year, unless a shorter duration of time has been approved in writing by the Port's Project Manager. All system maintenance will be completed outside of the Port's regular business hours (for purposes of this Agreement, outside of the Port's regular business

hours shall mean after 5:00 p.m. and before 8:30 a.m., Pacifc time, seven days a week, 365 days per year) .

Consultant shall provide and perform all Software updates and upgrades to the System during the Warranty Period. Consultant shall provide version and periodic upgrades to the System in a frequency as agreed upon by the Port Project Manager. Consultant shall provide all System updates to maintain current compliance with all laws, regulations, orders, and directives that apply to the Services.

If the System does not perform in accordance with this Agreement during the Warranty Period, Consultant shall take such steps as necessary to repair or replace the defective portion of the System at no additional cost to the Airport for material and labor. Such Warranty service shall be provided at Consultant's expense and shall include all media, parts, labor, freight and insurance to and from the Port.

If any defect in the System is not rectified by Consultant to the Port's satisfaction before the end of the Warranty Period, the Warranty Period shall be extended until, in the opinion of the Port, the defect has been fully rectified.

Once a particular identified defect has been rectified, it is at the sole discretion and option of the Port to request that the acceptance testing for the System be re-performed.

The Port, at the Port's option, may return the System, including Equipment to Consultant if it is deemed by the Port as "defective," within thirty (30) days of Acceptance of the System and Consultant shall immediately provide full exchange or refund. For purposes of this Agreement, the System may be deemd "defective" for a number of reasons, including, but not limited to the following:

(1) The System has not passed acceptance testing or achieved "Acceptance":

(2) The System is found to have defects during the "Warranty Period";

(3) The System causes significant impact and disruption to Airport's operations and requires excessive downtime and interaction by Airport staff.

Following Acceptance, Consultant shall provide telephone support to the Port for assistance with the operation of the System. Consultant shall disclose the warranty of any other manufacturers of components of the IdMS and, in the event such warranty exceeds the Consultant's warranty under this Agreement in any respect, Consultant shall take all measures to ensure that the Airport will receive the full benefit of such other manufacturer's warranty.

3.2 **Maintenance**

Consultant shall provide Maintenance Services for the System, in addition to the Warranty services provided during the Warranty Period (as set forth in Section 3.1 above), as follows:

(1) Consultant shall maintain the Software and Equipment. Consultant shall develop a maintenance plan for the System, subject to Port approval ("Maintenance Plan"). Consultant shall perform all maintenance Services in accordance with the Maintenance Plan.

(2) Consultant shall review the System and document/record service levels including, but not limited to, coverage time, maintenance request response time and acceptable system downtime.

(3) Consultant shall provide monthly reports to the Port demonstrating its performance against all required service levels.

(4) Consultant's Maintenance Plan shall include a plan to address all labor, software upgrades (including all necessary licensing, hosting, and/or design services), documentation revisions and preventive maintenance services necessary to keep the System and all integrations with other required systems in good operating condition and in full compliance with all applicable regulatory requirements.

(5) Consultant shall perform all Software upgrades.

3.3 Support

Consultant shall provide two consecutive weeks of onsite engineering support post Acceptance and "go live" (as used in this Ageement, the term "go live" refers to when the System has achieved Acceptance and is fully operational). Consultant must designate certified individuals within its staff with site specific knowledge to function as the Consultant's account representatives to coordinate support services with the Port.

After the System Acceptance, and the completion of Phase 1 Services, , Consultant shall provide Support for the System, including but not limited to updates, enhancements, and/or bug fixes necessary to ensure the functionality of the System and integration with other systems. All System changes (including updates) shall be conducted outside the Port's regular business hours, in coordination with Port staff. Consultant's support services are broken down into two categories: (1) Critical Issues; and (2) Non-Critical Issues, and are set forth in more detail below:

3.3.1. Critical Issues.

Critical Issues, as used in this Agreement, are defined as catastrophic failures of the System which affect the overall safety, security, or operation of the Airport. For example, the failure of a server, the loss of a badging workstation, the loss of functionality to print or produce badges, or the loss of integration or errors in the integration between the System and other systems. Critical issues require Consultant to respond per the response times indicated below.

Critical Issues Response Times:

Consultant shall provide the following response times to the Port for Critical Issues affecting the System:

(1) Initial response and acknowledgement within 15 minutes (if issue occurs within business or non-business working hours) of reported issue(s).

(2) Follow up contact with the Port's ID Badging Office Superintendent and/or representative within thirty (30) minutes (business or non-business working hours) to understand the issue and to start the trouble shooting process. Consultant shall establish a conference line and hourly status calls.

(3) Within two (2) hours (business or non-business working hours) of the issue being reported, Consultant shall provide next steps to fix the issue or advise and initiate restoring the System and integrations with all other systems..

3.3.2. Non-Critical Issues.

Non-critical issues, as the term is used in this Agreement, are defined as failures or

problems which do not affect the overall safety, security, or operation of the Airport. For example, the failure of a non-critical redundant piece of Equipment or the loss of a single badge printer would usually be considered non-critical.

Non-critical Issues Response Times:

Consultant shall provide the following response times to the Port for Critical Issues affecting the System:

(1) Initial response and acknowledgement within 15 minutes (business or non-business working hours) of reported issue(s).

(2) Follow up contact with the ID Badging Office Superintendent and/or representative within two (2) hours (business or non-business working hours) to understand the issue and start trouble shooting process.

(3) Within six (6) to twelve (12) hours (business or non-business working hours) of the issue having been reported, the Contractor shall provide status and next steps to fix the issue. The Contractor shall diagnose and remedy the problem during normal working hours of the next working day.

(4) Port's Business working hours are defined as 8:30 AM to 5:00 PM Pacific Time, seven days a week, 365 days a year.

3.3.3. Escalation Procedures and Support Requests

Consultant shall provide escalation procedures including contact name(s), direct phone number and email address(es) for escalating Critical and Non-Critical Issues.

Consultant shall provide all of the following Services relating to the Port's ability to submit support requests:

(1) In addition to a toll-free support number, Consultant must provide an online portal for the Port's use to submit support ticket requests. Port staff must be able to select the currently installed configuration options for the hardware, Software and services being supported. The online support portal must provide the customer details such as:

(a). Software installed with versions.

(b). Hardware installed with versions.

(2) Additionally, online support portal must provide the functionalities:

(a). Knowledge base of previous support cases.

(b). Estimated response time not to exceed time frame listed via e-mail.

(c). Technician assigned to support request.

(d). Status updates on support tickets – via e-mail.

(e). Listing of all support tickets and who initiated the tickets.

(f). Support category: warranty, out of warranty, covered, not covered.

(g). Designate issue criticality (Critical or Non-Critical) and designate priority: Low, Medium, High.

(h). Ticket resolution with details.

(3) Consultant shall ensure all staff assigned by Consultant to respond to support issues under this Agreement, via on-site or phone, must be certified in the software\hardware configurations.

(4) Consultant shall ensure all staff assigned by Consultant to provide support for and address on-site support issues must complete applicable security background check (STA and CHRC) requirements.

4. As-Needed System Changes/Improvements

Consultant shall also provide additional, as needed services required to complete and implement changes and/or improvements to the System, as specifically requested by the Port following completion of all Phase 1 Services. This category of services is included so that Consultant can provide services for unanticipated conditions or events relating to the System. No Services under this Section shall be performed without written authorization from the Port Division Director and are subject to the cost limitations as set forth in Appendix B-1 (Payment Schedule and Rates), and the "Maximum Compensation" amount for this Agreement, as set forth in Appendix B (Payment).

B. APPROVED SUBCONSULTANTS

Consultant shall use only the following personnel and subconsultants in performing Services: _____.

C. TERM OF AGREEMENT

The term of this Agreement shall be for _____ year(s) commencing _____ and terminating _____.

☐ The Port has the option of extending the Agreement for an additional _____ in _____ increments as authorized by the Executive Director and documented by a supplemental agreement to this Agreement, provided, however, that there shall be no increase in the Maximum Compensation payable hereunder.

APPENDIX A-1

SOFTWARE

1. **License.** Consultant hereby grants to the Port a fully-paid, non-exclusive, and non-transferable license to access and use the software described in **Appendix A** (the "Software"), during the Term, without any limitation as to the number or nature of users, machines, devices, or platforms, subject to any limitations described in **Appendix A**.

   a. **Back-Up Copies.** The Port may make copies of the Software as reasonably necessary for back-up disaster recovery purposes only.

   b. **No Other License.** Except as expressly set forth in this Agreement, no license is granted and none shall be deemed granted by implication, estoppel, or otherwise.

   c. **License Restrictions.** Any use of the Software not expressly permitted by this Agreement is prohibited. Without limiting the generality of the foregoing, the Port shall not commit any of the following:

      i. Sublicense use or access to any Software.

      ii. Remove or modify any Software markings or any notice of Consultant's or its licensors' proprietary rights.

      iii. Cause or permit reverse engineering (unless required by law for interoperability), disassembly, or decompilation of the Software.

   Except for the licenses granted herein and rights to data as set forth herein, all right, title, and interest in and to the Software, including (without limitation) all tangible or intangible material of any nature produced by Consultant related to the Software shall remain exclusively with Consultant and its licensors, as applicable. The Software is licensed, not sold.

2. **Equipment.** If the Services include any "Equipment" (as defined in **Appendix A**), then, unless otherwise agreed in writing by the Port, Consultant will be responsible for installing the Equipment and installing the Software on the Equipment or on the Port's systems. Consultant will be responsible for ensuring compatibility and that the Software and Equipment are functioning as intended.

3. **Delivery and Installation.** To the extent possible, Consultant will deliver Software to the Port electronically, unless otherwise requested by the Port in writing. Unless otherwise agreed in writing by the Port, and only to the extent applicable, Consultant will be responsible for installing the Software on the Port's systems and for ensuring compatibility and that the Software is functioning as intended.

4. **Data.** As between the Port and Consultant, the Port owns all right, title, and interest in any data that the Port, or others acting on behalf of the Port, have entered into, have associated with, or have otherwise prepared for use in or with the Software ("Port Data").

   ☒ Port Data shall include (without limitation): any and all information relating to new and renewal SIDA badge applicantions, badge replacement, vehicle permits, key issuance, including but not limited to cyber and metal keys, citations/violations and ramp permits.

   Within thirty (30) days of the expiration or termination of the Agreement for any reason, Consultant shall, at no charge to the Port and without the Port's request:

   a. Export and deliver to the Port all data input into the Software, including (without limitation) the Port Data. Consultant shall provide such data to the Port in a format reasonably requested by the Port.

☐ Acceptable data formats shall include (without limitation): _____.

b. Certify to the Port that all Port Data has been destroyed or removed from Consultant's possession and control.

5. Additional Warranties. Cumulative to any representations and warranties in the Agreement:

a. The Software is compatible for access and use on the Port's systems and devices. The Software (and, if applicable, the Equipment) will operate in all material respects as described in its product descriptions and/or documentation provided or published by Consultant. For all Equipment, Consultant will ensure that any manufacturer warranties are in the name of the Port, or transferred promptly to the Port, such that the Port has all benefits of any such warranties.

b. The Software (and, if applicable, the Equipment) will not contain or deliver any viruses, Trojan horses, worms, time bombs, trap doors, or other undisclosed code, program routine, device, or other feature or hidden file designed to damage, delete, disable, deactivate, interfere with or otherwise harm the Software or any hardware, software, data, or other programs of the Port.

c. Consultant will use all commercially reasonable best practices to ensure the security, safety, and integrity of all Port Data.

d. Consultant has all right, title, and authority necessary to grant any licenses or provide any Software, the Equipment (if applicable), or related services under this Agreement, including (without limitation) the absence of any contractual or other obligations that conflict with this Agreement or limit, restrict, or impair the rights granted under this Agreement.

e. The Software (and, if applicable, the Equipment) will not infringe or otherwise violate the patent rights, copyright, trade secret, trade name, trademark, service mark, or any other intellectual property or proprietary right of any person or persons.

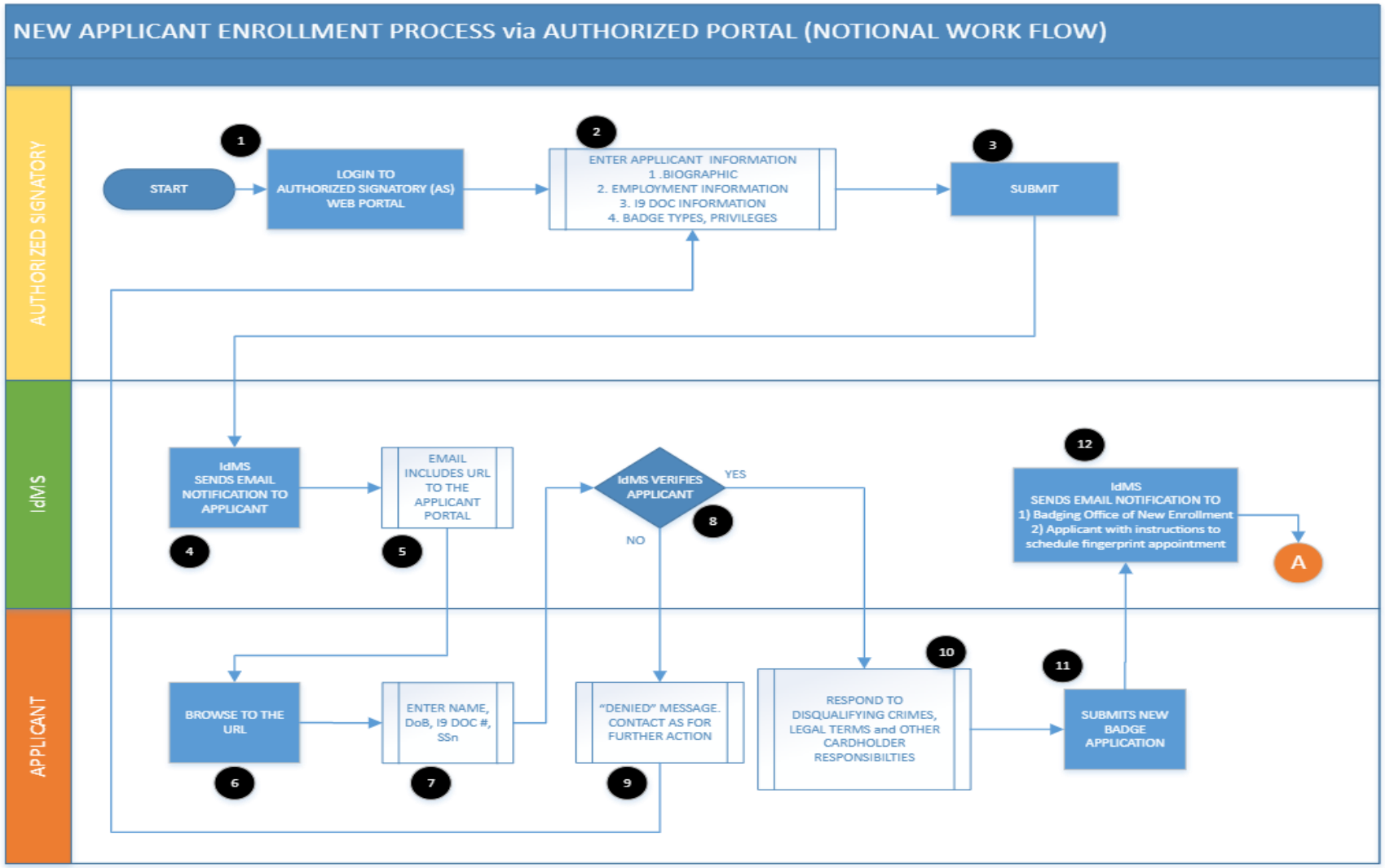
6. Additional Bankruptcy Provisions. All rights and licenses granted under or pursuant to this Agreement are and shall be deemed to be, for purposes of 11 U.S.C. § 365(n), licenses of rights to "intellectual property," as defined under 11 U.S.C. § 101. The Parties agree that the Port, as a licensee of such rights under this Agreement, will retain and may fully exercise all of its rights and elections under the U.S. Bankruptcy Code; however, nothing in this Agreement may be deemed to constitute a present exercise of such rights and elections.

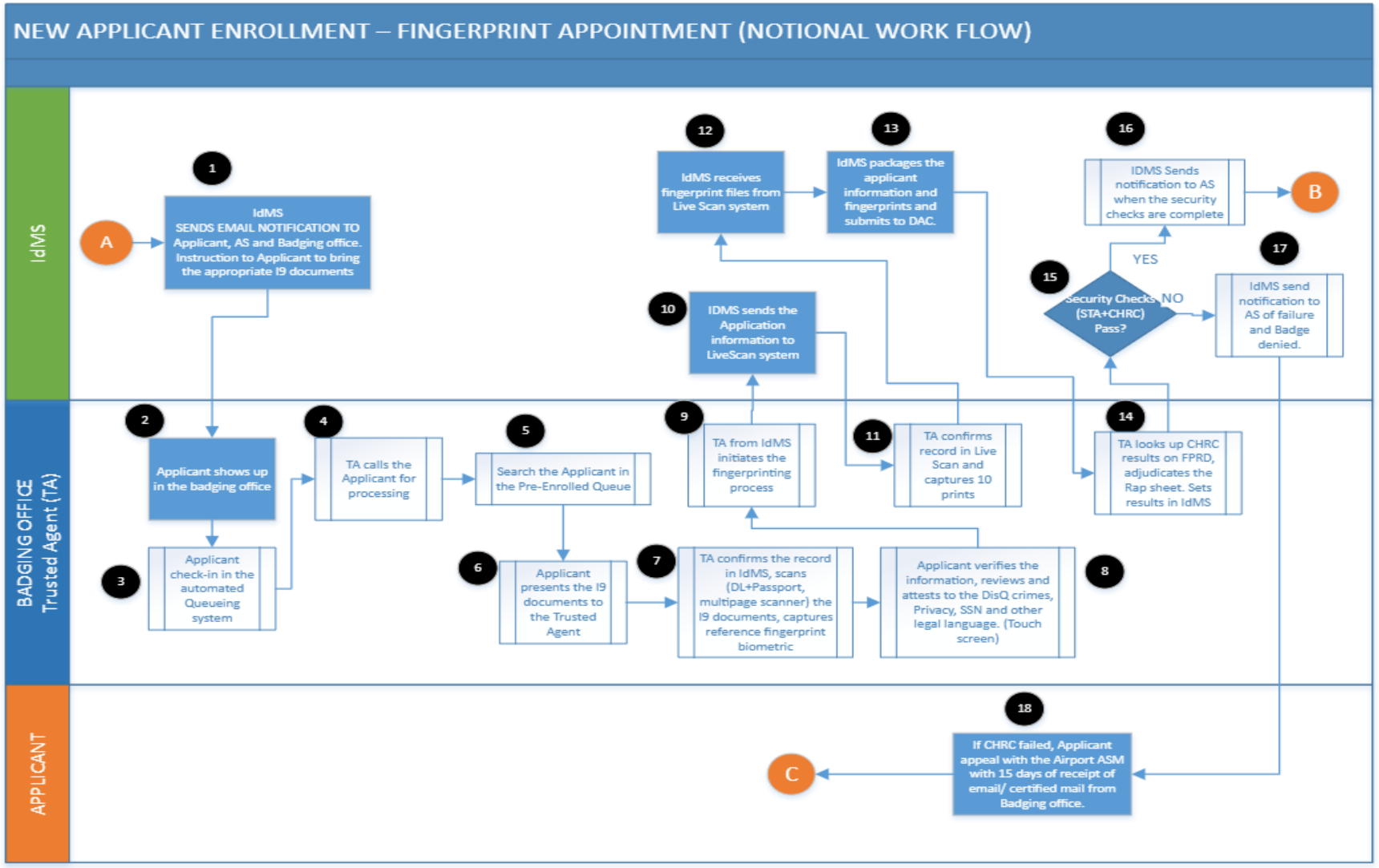
Consultant hereby agrees and consents that, in the event an order for relief under the U.S. Bankruptcy Code has been entered with respect to the Port, the Port will be permitted to assume this Agreement and all licenses set forth herein pursuant to 11 U.S.C. § 365, notwithstanding any right Consultant may have pursuant to 11 U.S.C. § 365(c)(1) to object to such assumption. This consent will constitute an irrevocable consent pursuant to 11 U.S.C. § 365 (c)(1)(B), but only with respect to the Port's assumption of the License (and not with respect to any assignment of this Agreement and the licenses set forth herein).

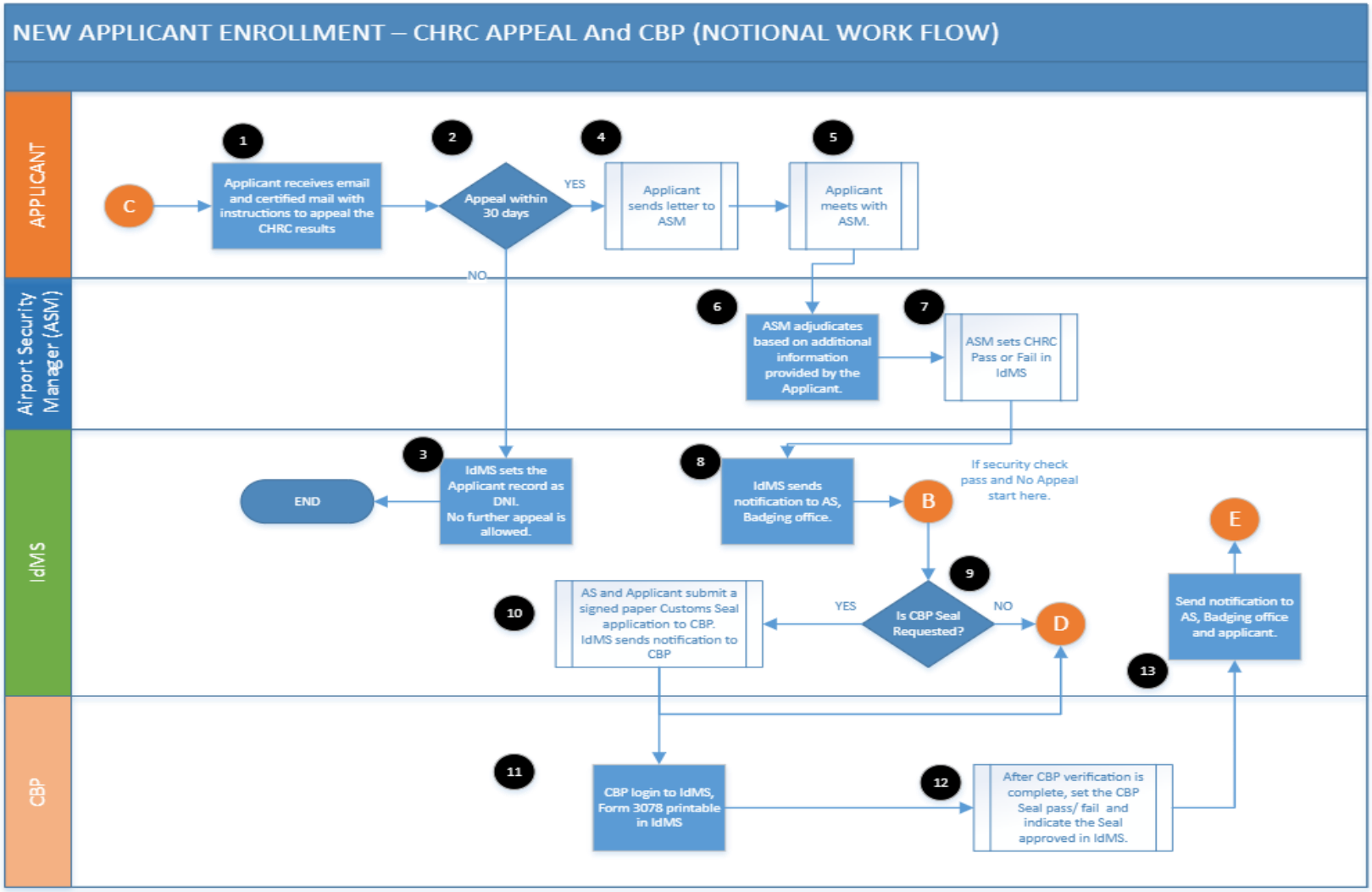
APPENDIX A-2

SYSTEM BADGE APPLICATION WORKFLOW PROCESSES

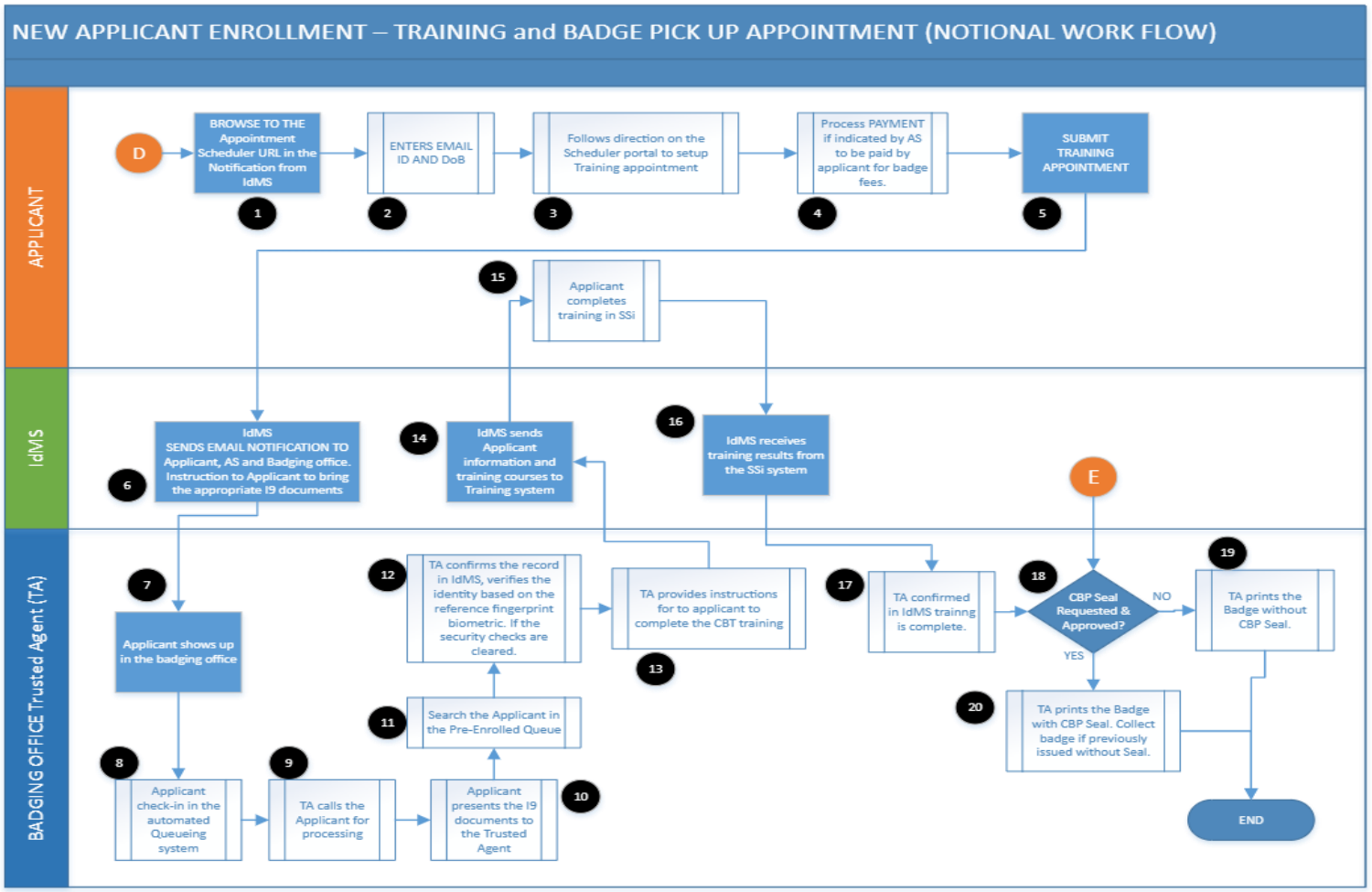
Consultant shall ensure the System follows the System Badge Applcation Workflow Processes as depicted in the attached images.


NEW APPLICANT ENROLLMENT PROCESS via AUTHORIZED PORTAL (NOTIONAL WORK FLOW)
AUTHORIZED SIGNATORY
IdMS
APPLICANT
1
START
LOGIN TO AUTHORIZED SIGNATORY (AS) WEB PORTAL
2
ENTER APPLLICANT INFORMATION
1 .BIOGRAPHIC
2. EMPLOYMENT INFORMATION
3. I9 DOC INFORMATION
4. BADGE TYPES, PRIVILEGES
3
SUBMIT
IdMS SENDS EMAIL NOTIFICATION TO APPLICANT
4
EMAIL INCLUDES URL TO THE APPLICANT PORTAL
5
IdMS VERIFIES APPLICANT
YES
NO
8
12
IdMS SENDS EMAIL NOTIFICATION TO
1) Badging Office of New Enrollment
2) Applicant with instructions to schedule fingerprint appointment
A
BROWSE TO THE URL
6
ENTER NAME, DoB, I9 DOC #, SSn
7
"DENIED" MESSAGE. CONTACT AS FOR FURTHER ACTION
9
10
RESPOND TO DISQUALIFYING CRIMES, LEGAL TERMS and OTHER CARDHOLDER RESPONSIBILTIES
11
SUBMITS NEW BADGE APPLICATION


NEW APPLICANT ENROLLMENT – FINGERPRINT APPOINTMENT (NOTIONAL WORK FLOW)
IdMS
BADGING OFFICE Trusted Agent (TA)
APPLICANT
A
1
IdMS SENDS EMAIL NOTIFICATION TO Applicant, AS and Badging office. Instruction to Applicant to bring the appropriate I9 documents
2
Applicant shows up in the badging office
3
Applicant check-in in the automated Queueing system
4
TA calls the Applicant for processing
5
Search the Applicant in the Pre-Enrolled Queue
6
Applicant presents the I9 documents to the Trusted Agent
7
TA confirms the record in IdMS, scans (DL+Passport, multipage scanner) the I9 documents, captures reference fingerprint biometric
8
Applicant verifies the information, reviews and attests to the DisQ crimes, Privacy, SSN and other legal language. (Touch screen)
9
TA from IdMS initiates the fingerprinting process
10
IDMS sends the Application information to LiveScan system
11
TA confirms record in Live Scan and captures 10 prints
12
IdMS receives fingerprint files from Live Scan system
13
IdMS packages the applicant information and fingerprints and submits to DAC.
14
TA looks up CHRC results on FPRD, adjudicates the Rap sheet. Sets results in IdMS
15
Security Checks (STA+CHRC) Pass?
YES
NO
16
IDMS Sends notification to AS when the security checks are complete
B
17
IdMS send notification to AS of failure and Badge denied.
18
If CHRC failed, Applicant appeal with the Airport ASM with 15 days of receipt of email/ certified mail from Badging office.
C


NEW APPLICANT ENROLLMENT – CHRC APPEAL And CBP (NOTIONAL WORK FLOW)
APPLICANT
Airport Security Manager (ASM)
IdMS
CBP
C
1
Applicant receives email and certified mail with instructions to appeal the CHRC results
2
Appeal within 30 days
YES
NO
4
Applicant sends letter to ASM
5
Applicant meets with ASM.
6
ASM adjudicates based on additional information provided by the Applicant.
7
ASM sets CHRC Pass or Fail in IdMS
3
IdMS sets the Applicant record as DNI.
No further appeal is allowed.
END
8
IdMS sends notification to AS, Badging office.
B
If security check pass and No Appeal start here.
9
Is CBP Seal Requested?
YES
NO
D
10
AS and Applicant submit a signed paper Customs Seal application to CBP.
IdMS sends notification to CBP
11
CBP login to IdMS, Form 3078 printable in IdMS
12
After CBP verification is complete, set the CBP Seal pass/ fail and indicate the Seal approved in IdMS.
13
Send notification to AS, Badging office and applicant.
E

New Applicant Enrollment – Training and Badging Pick Up



APPENDIX A-3

SYSTEM USER GROUPS

System User Groups

User Groups	Person Biographics	Documents & Security Checks	Training	Payments	Badge & Privileges	Assets (Keys & Permits)	Company	Citations / Infractions	Capture Fingerprint for CHRC	Badge Printing	Business Rules Override
System Administrator	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	Yes	Yes	
Airport Security Manager (ASM)	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	Yes	Yes	Yes
ID Badging Office Superintendent	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	Yes	Yes	Yes
ID Badging Office Trusted Agent	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R	Yes	Yes	
Training Coordinator (Security & Operations) [5]	R		R / W		R			R			
Airport Security – Cypher Keys Group	R	R	R	R	R	R / W					
Airport Security – Security / Safety Citation Groups	R	R	R	R	R	R		R / W			
Airport Representative (Properties, Engineering, and others)							R / W				
Port							R / W				
Finance	R	R	R	R	R	R		R	R	R	
Customs and Border Protection (CBP) [1]	R	R / W [1]	R	R	R	R					
Airport Operations Center (AOC) [2]	R	R	R	R	R / W [2]	R					
Authorized Signer [3]	R / W [3]			R / W [3]			R / W [3]				

* R = Read, W = Write

1 - CBP Seal Status change and notes only

2 - Badge status change to In Active / Lost / Stolen only, No reactivation

3 - Authorized Signer via Authorized Signer portal only can change specific information on employee biographic.

4 - Applicant via Applicant portal can ONLY make changes prior to badge application submission. Once submitted no further access is permitted.

5 - Training Coordinator will need access to the validate the identity of the applicant using the fingerprint template stored.

APPENDIX A-4

SYSTEM CITATION REQUIREMENTS AND CITATIONS/VIOLATIONS WORKFLOW

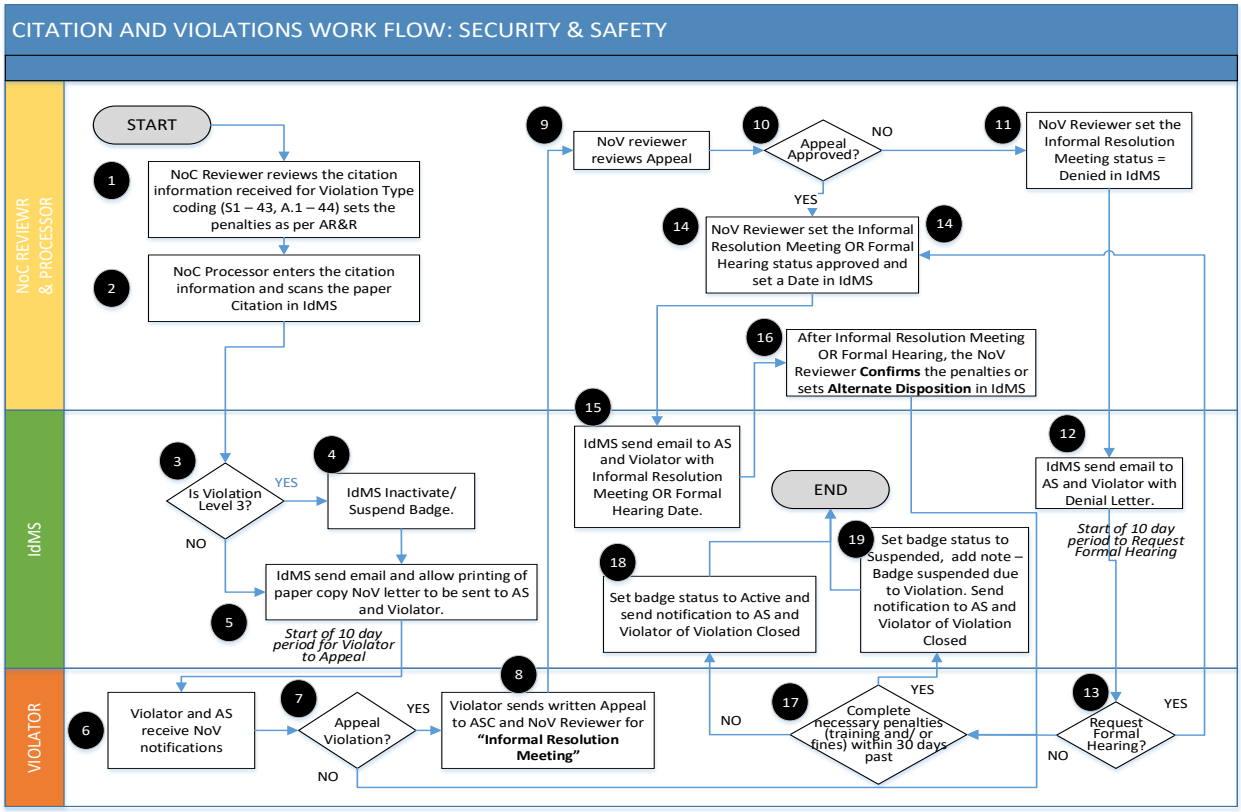
Consultant shall ensure the following Citation Requirements are incorporated into the System:

1. IdMS performs point calculation / penalty assignment based on violator's prior record and level of citation (based on Violation Type coding)
2. IdMS performs mail merge into correct NOV template
3. IdMS provides editable "print preview" for any changes by NOC processor
4. IdMS prints NOV, envelope, and label for certified mail
5. IdMS shall track if NOC/NOV process is "open" (violator still "in process" of resolving) or "closed" (violator has complied with all steps to resolve citation)
6. IdMS shall have user input fields for tracking if a NOC/NOV is going to informal resolution and formal hearing, including outcome of each (e.g., drop-down, pick-list)
7. IdMS has ability to input and track NOC warnings (0 points) (NOV not issued)
8. IdMS has ability for certain users to add documents to violator's NOC/NOV record, such as email correspondence, electronic evidence, notes, follow-on letters, etc.
9. IdMS can annotate violator's NOC/NOV record with notes and status
10. IdMS has ability for Aviation Security Manager/Airport Operations Manager or delegate to note that the meeting with the Aviation Security Manager/Airport Operations Manager (or delegate) occurred and note date (internal (temporary) expiration date remains "limited" until violator retakes computer-based training)
11. IdMS will mail merge (including preparation of envelopes and labels) and allow for selection of checkboxes / data input on the following correspondence:
    - Informal Resolution Denial Letter / Notice of Confirmation / Alternative Disposition
    - NOV Rescission Letter (IdMS resets internal (temporary) expiration date back to expiration date printed on the badge if violation when violation is rescinded)
12. IdMS shall allow Aviation Security Manager/Airport Operations Manager or delegate to manually reduce / remove / edit points, NOCs/NOVs, etc.
13. IdMS shall provide data-rich reports and graphs re: NOCs / NOVs (e.g., # of violations by type within a certain timeframe, # of individuals who are repeat violators, # of open v. closed citations, etc.)
14. IdMS shall provide a "view only" page for Airport Duty Managers and Airport Operations Specialists to view citation-related history of a badge holder

Consultant shall also ensure the System follows the Citations and Violations Workflow as depicted in Image 1 below.

[Image 1 continued on next page]

Image 1


CITATION AND VIOLATIONS WORK FLOW: SECURITY & SAFETY
NoC REVIEWR & PROCESSOR
IdMS
VIOLATOR
START
1
NoC Reviewer reviews the citation information received for Violation Type coding (S1 – 43, A.1 – 44) sets the penalties as per AR&R
2
NoC Processor enters the citation information and scans the paper Citation in IdMS
3
Is Violation Level 3?
YES
NO
4
IdMS Inactivate/ Suspend Badge.
5
IdMS send email and allow printing of paper copy NoV letter to be sent to AS and Violator.
Start of 10 day period for Violator to Appeal
6
Violator and AS receive NoV notifications
7
Appeal Violation?
YES
NO
8
Violator sends written Appeal to ASC and NoV Reviewer for "Informal Resolution Meeting"
9
NoV reviewer reviews Appeal
10
Appeal Approved?
NO
YES
11
NoV Reviewer set the Informal Resolution Meeting status = Denied in IdMS
12
IdMS send email to AS and Violator with Denial Letter.
Start of 10 day period to Request Formal Hearing
13
Request Formal Hearing?
YES
NO
14
NoV Reviewer set the Informal Resolution Meeting OR Formal Hearing status approved and set a Date in IdMS
15
IdMS send email to AS and Violator with Informal Resolution Meeting OR Formal Hearing Date.
16
After Informal Resolution Meeting OR Formal Hearing, the NoV Reviewer Confirms the penalties or sets Alternate Disposition in IdMS
17
Complete necessary penalties (training and/ or fines) within 30 days past
YES
NO
18
Set badge status to Active and send notification to AS and Violator of Violation Closed
19
Set badge status to Suspended, add note – Badge suspended due to Violation. Send notification to AS and Violator of Violation Closed
END

APPENDIX A-5

SYSTEM SPECIFICATIONS/REQUIREMENTS

[The complete System Specifications/Requirements will be inserted following award and prior to the finalization of any associated agreement. However, it will be substantially in conformance with RFP Attachment 12.3]

APPENDIX B

PAYMENT

1. **Services.** The Port will pay Consultant for Services, a Maximum Compensation defined below, which sum includes costs for reimbursable expenses, if any.

Maximum Compensation	**$**

The Maximum Compensation shall be full compensation for all Services required, performed or accepted under this Agreement. If the Port and Consultant previously executed a purchase order for services within the scope of the Services of this Agreement, then the services performed and the compensation paid under that purchase order shall be subject to the terms of this Agreement and the previous payments deemed payments against the Agreement Price established in this Appendix.

The Maximum Compensation may only be increased if such increase is: (a) consistent with all applicable laws and regulations (including, without limitation, the Port's Purchasing Ordinance); (b) consistent with the applicable action authorized by the Board of Port Commissioners; and (c) documented by a supplemental agreement to this Agreement approved by the Executive Director. Any other increases shall only be allowed with a duly adopted authorizing resolution by the Board of Port Commissioners.

2. **Payment Schedule.** Progress payments for Services for each phase of the work shall be made as follows:

☒ upon completion of the work ☐ as invoiced

☐ monthly ☒ as set forth in the attached schedule.

[Additional terms regarding payment schedule and rates will be inserted into this draft agreement following award and prior to the finalization of any associated agreement. All payments for services will be made after deduction of any applicable Liquidated Damages as set forth in Section 9 of this Agreement and as stated in Section 5 below,]

3. **Reimbursable Expenses Allowed?**

☐ **No.** There are no reimbursable expenses allowed under this Agreement.

☒ **Yes.** The Port will reimburse Consultant for the reasonable costs and expenses set forth below, provided they have been pre-approved in writing by the Project Manager. Any other costs or expenses not listed will not be allowed.

3.1 Travel Costs. Consultant shall obtain written approval of the Project Manager for all travel costs prior to submitting the invoice for reimbursement of these costs. The Project Manager will review and determine, in the Port's sole discretion, whether the travel costs are reasonable and reimbursable based on the equivalent standards and procedures set forth in the Port's Travel Authorization and Reimbursement Policy/Administrative Policy No. 406. (The Port will provide a copy of AP 406 to Consultant upon request.)

☐ **Limits:** *[to be determined]*

4. **Invoices.** All payments shall require a written invoice from Consultant in a form acceptable to Port. Port shall make payment on approved amounts within each invoice within 30 days of receipt. **Original invoices shall be sent to:**

Port of Oakland, Accounts Payable, P.O. Box 28413, Oakland, CA 94604

Or emailed to accountspayable@portoakland.com, referencing the purchase order number and/or contract number in the subject line.

5. **Deductions to Payments.** The Port shall have the right to deduct from the amount payable to Consultant, upon written notice, any unauthorized or disputed expenses, any Liquidated Damages imposed (in accordance with Section 9 of this Agreement) or for overpayment of expenses by the Port and any other amounts owed by the Consultant to the Port. If the Port is required or elects to pay any sum, or if it incurs any obligations or expenses, because of the failure, inability, neglect or refusal of the Consultant to perform or fulfill any of the terms and conditions of this Agreement that it is obligated to perform or fulfill, then the Port shall have the right to deduct these sum(s) from the any and all amounts payable to Consultant.

APPENDIX B-1

PAYMENT SCHEDULE AND RATES

The payment schedule and billing rates for Consultant's Services are broken down into three categorie/phasesas follows: (1) Phase 1 Services; (2) Phase 2 Services; and (3) As -Needed System Changes/Improvements, as set forth in more detail below. Consultant's Phase 1 Services are further broken down by Tasks. All invoices shall be submitted and payment subsequently made in accordance with Appendix B (Payment), Section 4 (Invoices), including any applicable payment deductions as referenced in Appendix B (Payment) Section 5 (Deductions to Payments). All invoices shall serve as the basis for payment, subject to Port Project Manager's approval of the invoice(s).

A. Payment Schedule

1. Phase 1 Services.

All Phase 1 Services will be invoiced at the rates as set forth in Section B below and subject to the Maximum Compensation, as set forth and defined in Appendix B. Progress payments for Services under Phase 1 will be invoiced by Consultant and subsequently paid following the completion of each Task (as defined in Appendix A Services). Completion of each particular Task must be verified in writing by the Port's Project Manager, in the Project Manager's sole discretion, before Consultant can submit an invoice for the completed Task. Consultant may only invoice for one Task at a time, following completion of all preceding Tasks.

2. Phase 2 Services

No payments for Phase 2 Services shall be made to Consultant until after Acceptance of the System and completion of all Phase 1 Services (as described and defined in Appendix A (Services)). Phase 2 Services shall be invoiced by Consultant in arrears on an monthly basis and include itemized charges for the preceding calendar month. All Phase 2 Services will be invoiced at the rates as set forth in Section B below and subject to the Maximum Compensation, as set forth and defined in Appendix B.

3. As -Needed System Changes/Improvements

All pre-authorized As-Needed System Changes/Improvements Phase 2 Services shall be invoiced by Consultant at the conclusion of such services, as verified in writing by the Port's Project Manager, in the Project Manager's sole discretion, before Consultant can submit an invoice for the completed Service. All As-Needed System Changes/Improvement Services will be invoiced at the rates as set forth in Section B below and subject to the Maximum Compensation, as set forth and defined in Appendix B.

B. Hourly Billing Rates

[to be determined]

APPENDIX C

INSURANCE

1. **Commercial General Liability Insurance**

- **Coverage:** Standard ISO Commercial General Liability form.
- **Limits**: $1,000,000 per occurrence; $2,000,000 annual general aggregate; $2,000,000 products and completed operations aggregate; $1,000,000 each offense for personal and advertising injury.
- **Deductible/Self-Insured Retention:** Not more than $25,000 per occurrence unless otherwise approved by Port Risk Management.
- **Additional Insured**: The City of Oakland, a municipal corporation, acting by and through its Board of Port Commissioners, Port of Oakland, its commissioners, officers, agents and employees.
- Cross liability/separation of insureds.
- Waiver of subrogation in favor of additional insured.
- If the Services involve construction activities, completed operations coverage must remain in force until at least 5 years after completion and acceptance of the Services.

2. **Business Automobile Liability Insurance**

- **Coverage:** Standard ISO Business Automobile Liability form for all owned, non-owned and hired automobiles.
- **Limits:** $1,000,000 each accident, except $5,000,000 for vehicles operating in the South Field, the Aviation Operating Area ("AOA"), or any active airfields of the Oakland International Airport.
- **Deductible/Self-Insured Retention:** Not more than $25,000 per accident unless otherwise approved by Port Risk Management.
- **Additional Insured:** The City of Oakland, a municipal corporation, acting by and through its Board of Port Commissioners, Port of Oakland, its commissioners, officers, agents and employees.
- Waiver of subrogation in favor of additional insured.

3. **Contractor's Pollution Legal Liability Insurance**

- **When Required:** If the Services involve any construction activities, or any grading, excavating, underground utilities, piping, trenching, or any work below the surface of the ground, or involves the hauling or disposal of hazardous or regulated materials.
- **Coverage:** Contractor's Pollution Legal Liability occurrence or claims made form.
- **Limits:** $1,000,000 per occurrence and $2,000,000 annual aggregate.
- **Deductible/Self-Insured Retention:** Not more than $100,000 per occurrence unless otherwise approved by Port Risk Management.
- **Additional Insured:** The City of Oakland, a municipal corporation, acting by and through its Board of Port Commissioners, Port of Oakland, its commissioners, officers, agents and employees.
- Waiver of subrogation in favor of additional insured.
- **Additional Term if Claims Made Form:** 2 years following completion and acceptance of the Services.
- **Definition of "Covered Operations**" shall include All work performed by Consultant or its contractors or subcontractors.

4. **Workers' Compensation and Employer's Liability Insurance**

- **Coverage:** Statutory Workers' Compensation and Side B Employer's Liability form.

- **Limits:** Statutory for workers' compensation and $1,000,000 per accident, $1,000,000 bodily injury each employee, and $1,000,000 policy limit for bodily injury by disease, for Employer's Liability.
- **Deductible/Self-Insured Retention:** Not more than $25,000 per occurrence for Employer's Liability unless otherwise approved by Port Risk Management.
- Waiver of subrogation in favor of the City of Oakland, a municipal corporation, acting by and through its Board of Port Commissioners, Port of Oakland, its commissioners, officers, agents and employees.

5. **Professional Liability Insurance**

- **Coverage:** For errors and omissions arising out of the Services.
- **Limits:** $5,000,000 per claim and annual aggregate.
- **Deductible/Self-Insured Retention:** Not more than $100,000 per claim unless otherwise approved by the Port Risk Management.
- **Additional Term:** 2 years after completion and acceptance of the Services.
- If the Services involve software or technology services, Technology Liability coverage, including coverage for privacy liability.
- If the Services involve outsourced technology or internet services, Network and Media Liability coverage.
- Waiver of subrogation in favor of the City of Oakland, a municipal corporation, acting by and through its Board of Port Commissioners, Port of Oakland, its commissioners, officers, agents, and employees.

Other Insurance Requirements:

- **Notice of Cancellation**. Consultant or Consultant's agent must provide 30-days prior written notice to the Port Risk Management Department of any insurance policy cancellation, except 10-days prior written notice for non-payment of premium.

- **Proof of Insurance/Insurer Rating**. Consultant must deliver to the Port Risk Management Department, prior to the commencement of the Services, certificates of insurance evidencing all required insurance and additional insured status for the Port. All required insurance shall be provided by insurance companies with current A.M. Best ratings of A- VII or better. Upon failure to so file such insurance certificate, the Port may without further notice and at its option either (1) exercise the Port's rights; or (2) procure such insurance coverage at Consultant's expense and Consultant shall promptly reimburse the Port for such expense (Services may be interrupted without proper evidence). In addition to the certificate of insurance, Consultant shall provide copies of the actual insurance policies if requested by the Port.

- Please send certificates and other required insurance information to:

  Port of Oakland
  Attn: Risk Management Dept.
  530 Water Street
  Oakland, CA 94607
  Email: risktransfer@portoakland.com

APPENDIX D

PARTIES

CONSULTANT

Full Legal Name of Consultant:

Corporate Address:

Form of Business Entity (Check one)

- ☐ **Sole proprietorship**
- ☐ **Corporation: State of _____**
- ☐ **Partnership: ☐ General ☐ Limited**
- ☐ **Limited Liability Company**
- ☐ **Other: _____**

If Corporation, LLC, LP, LLP:
(Required Information)
Agent for Service of Process
(Name and Address)

Contact Individual / Position:

Telephone No.:

Facsimile No. (if any):

E-Mail Address:

Website (if any):

Tax Identification No.:

PORT

Division Director	
Project Manager	
Port's Notice Address	[Project Manager Name] Port of Oakland 530 Water Street Oakland, CA 94607

APPENDIX E

FAA AIP GRANT-REQUIRED PROVISIONS

The following provisions are required in all Port contracts because of the Port's participation in the FAA Airport Improvement Program (AIP). Consultant shall fully comply with all of the following provisions and shall also include each these provisions in all of its contracts and subcontracts related to this Agreement.

Note: Consultant is sometimes hereinafter referred to as "Contractor" and the Port is sometimes hereinafter referred to as "Sponsor". These provisions, as worded below, are required as a result of the AIP and may not be amended.

A. General Civil Rights Provisions.

The Contractor agrees to comply with pertinent statutes, Executive Orders and such rules as are promulgated to ensure that no person shall, on the grounds of race, creed, color, national origin, sex, age, or disability be excluded from participating in any activity conducted with or benefiting from Federal assistance. This provision binds the Contractor and subtier contractors from the bid solicitation period through the completion of the contract. This provision is in addition to that required of Title VI of the Civil Rights Act of 1964.

B. Compliance With Nondiscrimination Requirements.

During the performance of this Agreement, 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 Agreement, 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 Agreement 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 Agreement, the Sponsor will impose such contract sanctions as it or the Federal Aviation Administration may determine to be appropriate, including, but not limited to:

    - Withholding payments to the Contractor under the Agreement until the Contractor complies; and/or
    - Cancelling, terminating, or suspending an Agreement, in whole or in part.

6. **Incorporation of Provisions:** The Contractor will include the provisions of paragraphs 1 through 5 above 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.

C. <u>Title VI List of Pertinent Nondiscrimination Acts and Authorities.</u>

During the performance of this Agreement, 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).

D. Fair Labor Standards Act.

This Agreement incorporates by reference the provisions of 29 U.S.C. § 201, et seq (the Federal Fair Labor Standards Act or "FLSA"), and its implementing regulations, 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. Consultant has full responsibility to monitor compliance to the referenced statute and regulation. Consultant must address any claims or disputes that arise from this requirement directly with the US Department of Labor – Wage and Hour Division.

E. Occupational Safety and Health Act.

This Agreement incorporates by reference the requirements of 29 CFR Part 1910 with the same force and effect as if given in full text. Consultant must provide a work environment that is free from recognized hazards that may cause death or serious physical harm to the employee. Consultant 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 (29 U.S.C. §651, et seq; 29 CFR Part 1910). Consultant 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.

APPENDIX F

INDEMNIFICATION

A. To the fullest extent permitted by law (including, without limitation, California Civil Code Sections 2782, 2782.6, and 2782.8), Consultant shall defend (with legal counsel chosen or approved by the Port Attorney), indemnify and hold harmless the Port and its officers, agents, departments, officials, representatives, and employees (collectively, "Indemnitees") from and against the Liabilities.

"Liabilities" means any and all claims, loss, cost, damage, injury (including, without limitation, injury to or death of an employee of Consultant or its Subconsultants), expense and liability of every kind, nature, and description (including, without limitation, incidental and consequential damages, court costs, paralegal and attorneys' fees (including costs attributable to in-house paralegals and attorneys), Port staff costs, litigation expenses and fees of expert consultants or expert witnesses incurred in connection therewith and costs of investigation) that:

(1) Arise out of, pertain to, or relate to the negligence, recklessness, or willful misconduct of Consultant, any Subconsultant, or anyone directly or indirectly employed or controlled by Consultant or any Subconsultant, who provide design professional services governed by California Civil Code Section 2782.8; and

(2) For Services not governed by California Civil Code Section 2782.8, arise from or relate to, directly or indirectly, in whole or in part:

(a) the Services, or any part thereof,

(b) any negligent act or omission of Consultant, any Subconsultant, or anyone directly or indirectly employed or controlled by Consultant or any Subconsultant,

(c) any claim of infringement of the patent rights, copyright, trade secret, trade name, trademark, service mark or any other intellectual property or proprietary right of any person or persons in consequence of the use by the Port, or any of the other Indemnitees, of any of the articles or Services to be supplied in the performance of this Agreement (including any Software or Equipment, as defined in the Services), and/or

(d) any claim of unauthorized collection, disclosure, use, access, destruction, or modification, or inability to access, or failure to provide data, by any person or persons in consequence of any act or omission by Consultant or any Subconsultant.

Such obligations to defend, hold harmless, and indemnify any Indemnitees shall not apply to the extent that such Liabilities are caused in whole or in part by the sole negligence, active negligence, or willful misconduct of such Indemnitee, but shall apply to all other Liabilities.

Consultant shall cause its Subconsultants to agree to indemnities and insurance obligations in favor of Port and other Indemnitees in the exact form and substance of those contained in this Agreement.

B. *The following provision shall only apply to the extent that Consultant, any Subconsultant, or anyone directly or indirectly employed or controlled by Consultant or any Subconsultant, who provide design professional services governed by California Civil Code Section 2782.8*:

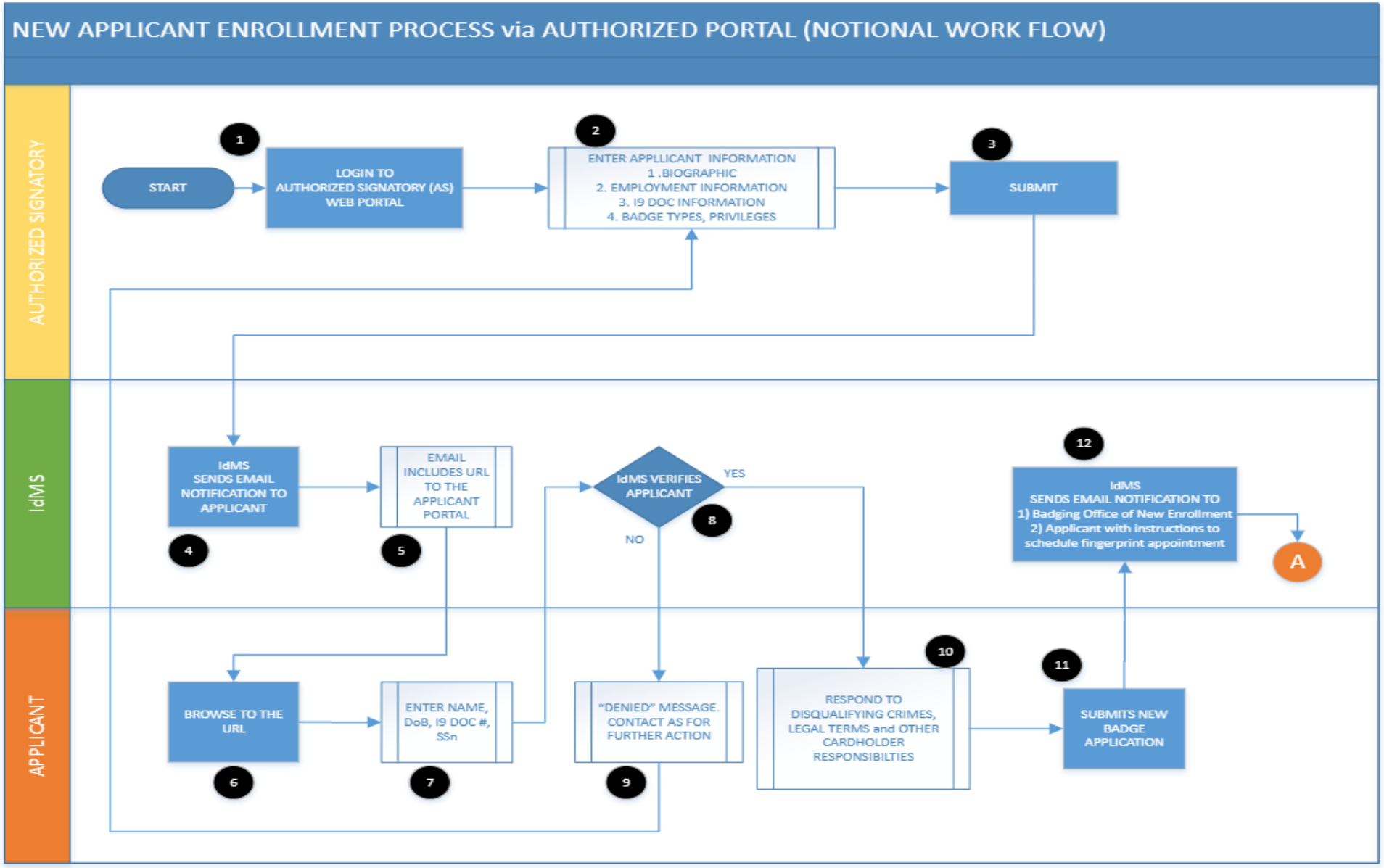
(1) Port shall include a provision in the construction contract with the general contractor on the Project requiring the general contractor to indemnify Consultant for damages resulting from the negligence of the general contractor and its subcontractors. Port shall also include a provision in the construction contract with the general contractor on the project requiring the general contractor to name Consultant as an additional insured on its CGL insurance coverage. The risk of an inadvertent omission of such provisions is on Consultant. Therefore, Consultant shall review the construction contract prior to bidding to ensure that such provision has been included in the draft of the bid documents.

(2) If there is an obligation to indemnify under this Agreement, Consultant shall be responsible for incidental and consequential damages resulting directly or indirectly, in whole or in part, from Consultant's negligence, recklessness, or willful misconduct.

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

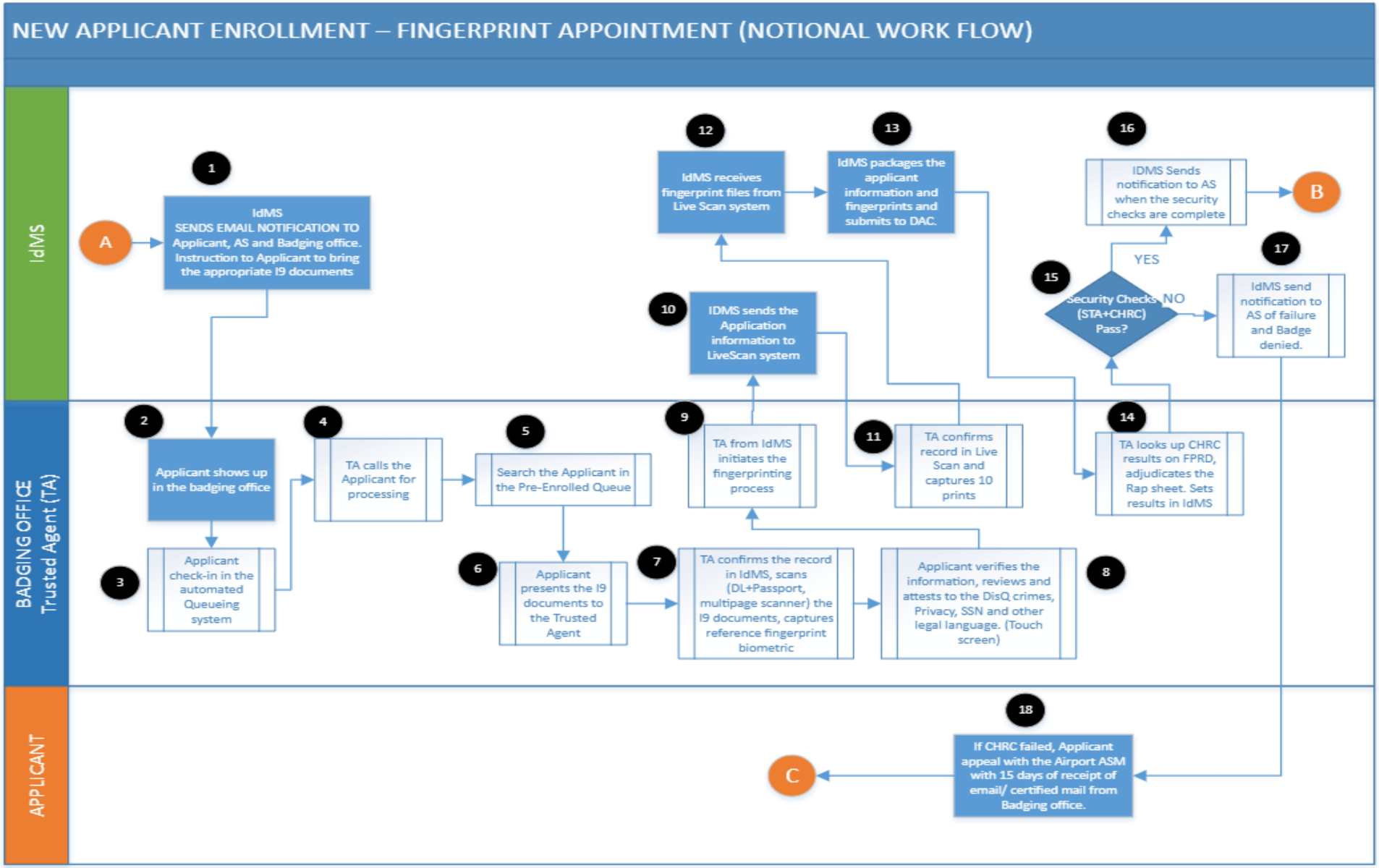
IdMS Citation Requirements

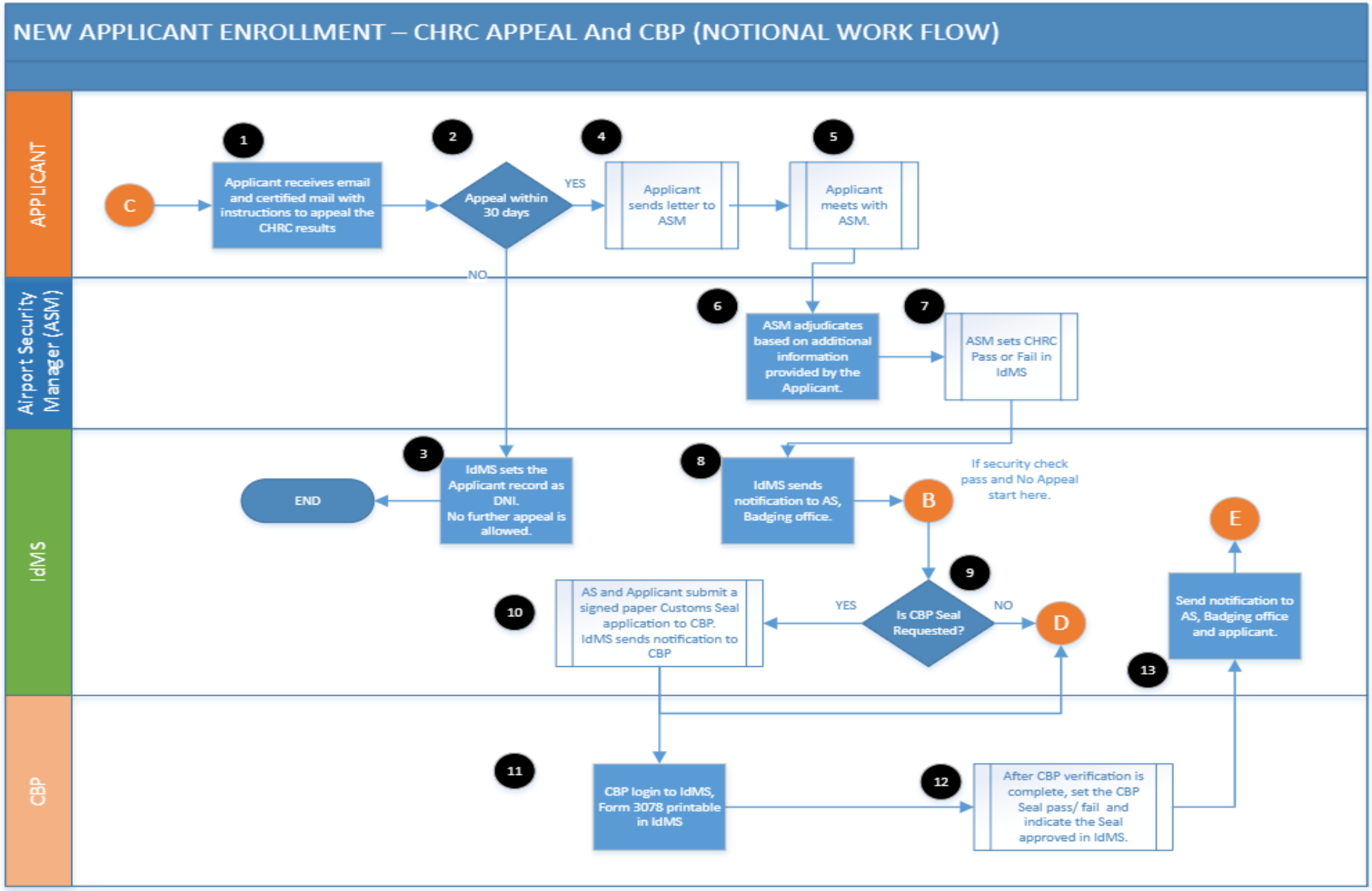
(Attachment 12-1)


NEW APPLICANT ENROLLMENT PROCESS via AUTHORIZED PORTAL (NOTIONAL WORK FLOW)
AUTHORIZED SIGNATORY
IdMS
APPLICANT
1
START
LOGIN TO AUTHORIZED SIGNATORY (AS) WEB PORTAL
2
ENTER APPLLICANT INFORMATION
1 .BIOGRAPHIC
2. EMPLOYMENT INFORMATION
3. I9 DOC INFORMATION
4. BADGE TYPES, PRIVILEGES
3
SUBMIT
IdMS SENDS EMAIL NOTIFICATION TO APPLICANT
4
EMAIL INCLUDES URL TO THE APPLICANT PORTAL
5
IdMS VERIFIES APPLICANT
8
YES
NO
12
IdMS SENDS EMAIL NOTIFICATION TO
1) Badging Office of New Enrollment
2) Applicant with instructions to schedule fingerprint appointment
A
BROWSE TO THE URL
6
ENTER NAME, DoB, I9 DOC #, SSn
7
"DENIED" MESSAGE. CONTACT AS FOR FURTHER ACTION
9
10
RESPOND TO DISQUALIFYING CRIMES, LEGAL TERMS and OTHER CARDHOLDER RESPONSIBILTIES
11
SUBMITS NEW BADGE APPLICATION

PORT OF OAKLAND

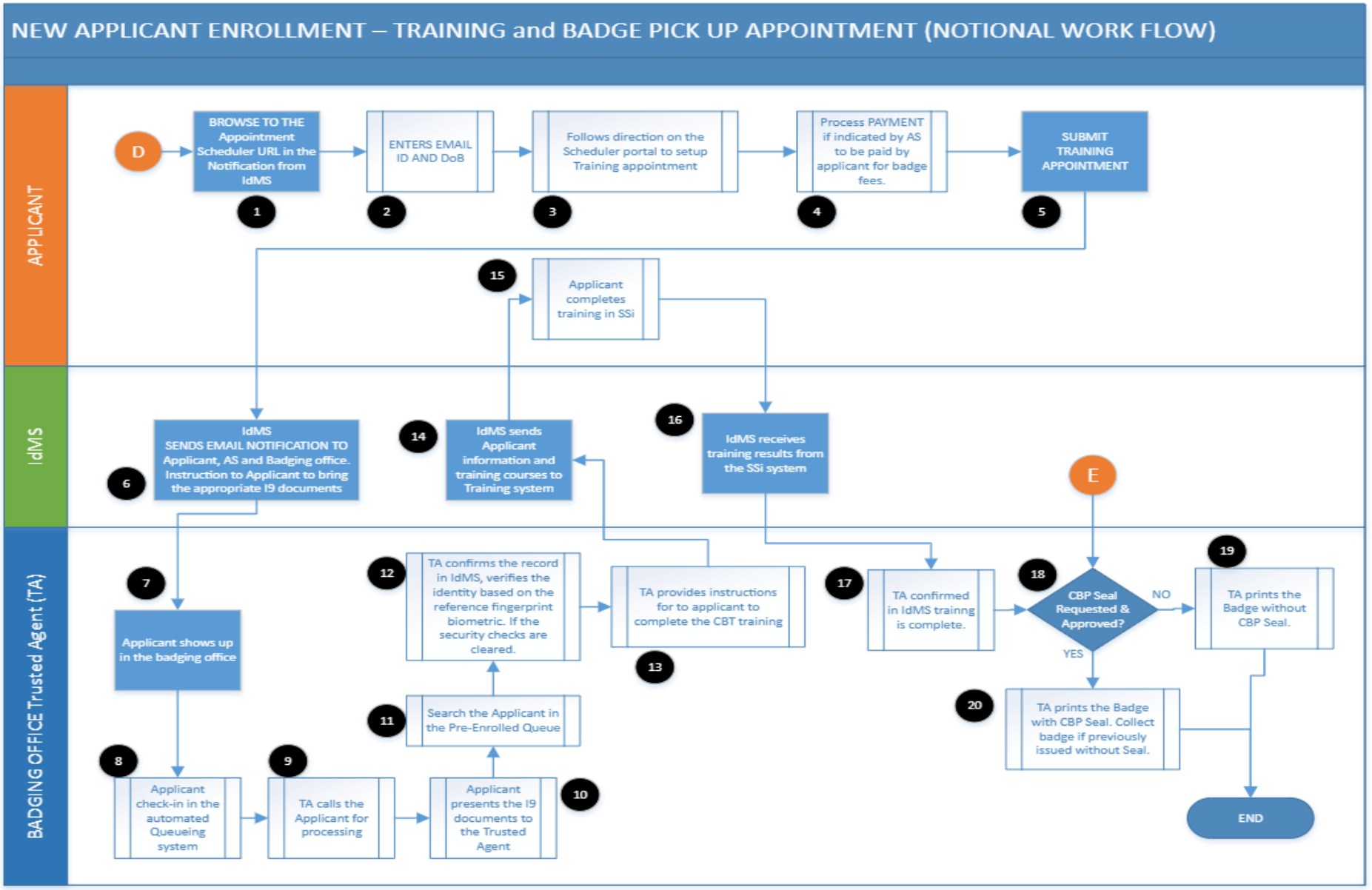
New Applicant Enrollment – Fingerprint Appointment




NEW APPLICANT ENROLLMENT – CHRC APPEAL And CBP (NOTIONAL WORK FLOW)
APPLICANT
Airport Security Manager (ASM)
IdMS
CBP
C
1
Applicant receives email and certified mail with instructions to appeal the CHRC results
2
Appeal within 30 days
YES
4
Applicant sends letter to ASM
5
Applicant meets with ASM.
NO
6
ASM adjudicates based on additional information provided by the Applicant.
7
ASM sets CHRC Pass or Fail in IdMS
3
IdMS sets the Applicant record as DNI. No further appeal is allowed.
END
8
IdMS sends notification to AS, Badging office.
B
If security check pass and No Appeal start here.
9
Is CBP Seal Requested?
YES
NO
D
10
AS and Applicant submit a signed paper Customs Seal application to CBP. IdMS sends notification to CBP
11
CBP login to IdMS, Form 3078 printable in IdMS
12
After CBP verification is complete, set the CBP Seal pass/ fail and indicate the Seal approved in IdMS.
13
Send notification to AS, Badging office and applicant.
E

PORT OF OAKLAND

New Applicant Enrollment – Training and Badging Pick Up Appointment



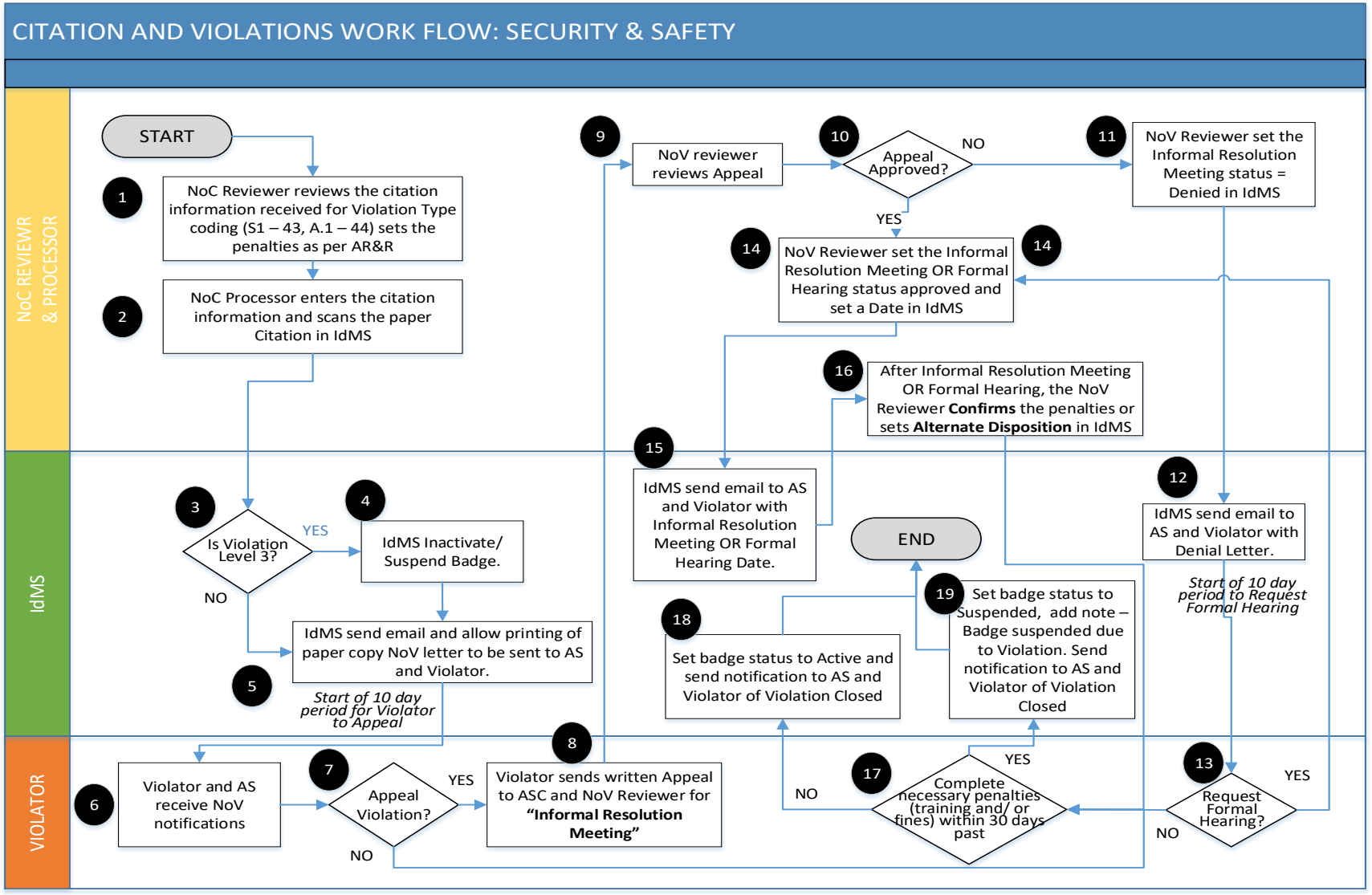
System User Groups											
User Groups	**Person Biographic**	**Documents & Security Checks**	**Training**	**Payments**	**Badge & Privileges**	**Assets (Keys & Permits)**	**Company**	**Citations / Infractions**	**Capture Fingerprint for CHRC**	**Badge Printing**	**Business Rules Override**
System Administrator	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	Yes	Yes	
Airport Security Manager (ASM)	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	Yes	Yes	Yes
ID Badging Office Superintendent	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R / W	Yes	Yes	Yes
ID Badging Office Trusted Agent	R / W	R / W	R / W	R / W	R / W	R / W	R / W	R	Yes	Yes	
Training Coordinator (Security & Operations) [5]	R		R / W		R			R			
Airport Security – Cypher Keys Group	R	R	R	R	R	R / W					
Airport Security – Security / Safety Citation Groups	R	R	R	R	R	R		R / W			
Airport Representative (Properties, Engineering, and others)							R / W				
Port Finance							R / W				
Customs and Border Protection (CBP) [1]	R	R / W [1]	R		R	R					
Airport Operations Center (AOC) [2]	R	R	R		R / W [2]	R					
Authorized Signer [3]	R / W [3]			R / W [3]			R / W [3]				

* R = Read, W = Write

[1] CBP Seal Status change and notes only
[2] Badge status change to In Active/ Lost/ Stolen only, No reactivation
[3] Authorized Signer via Authorized Signer portal only can change specific information on employee biographic.
[4] Applicant via Applicant portal can ONLY make changes prior to badge application submission. Once submitted no further access is permitted.
[5] Training Coordinator will need access to the validate the identity of the applicant using the fingerprint template stored.

PORT OF OAKLAND

Citation and Violation Work Flow



IdMS Citation Requirements

1. IdMS performs point calculation / penalty assignment based on violator's prior record and level of citation (based on Violation Type coding)
2. IdMS performs mail merge into correct NOV template
3. IdMS provides editable "print preview" for any changes by NOC processor
4. IdMS prints NOV, envelope, and label for certified mail
5. IdMS shall track if NOC/NOV process is "open" (violator still "in process" of resolving) or "closed" (violator has complied with all steps to resolve citation)
6. IdMS shall have user input fields for tracking if a NOC/NOV is going to informal resolution and formal hearing, including outcome of each (e.g., drop-down, pick-list)
7. IdMS has ability to input and track NOC warnings (0 points) (NOV not issued)
8. IdMS has ability for certain users to add documents to violator's NOC/NOV record, such as email correspondence, electronic evidence, notes, follow-on letters, etc.
9. IdMS can annotate violator's NOC/NOV record with notes and status
10. IdMS has ability for Aviation Security Manager/Airport Operations Manager or delegate to note that the meeting with the Aviation Security Manager/Airport Operations Manager* (or delegate) occurred and note date (internal (temporary) expiration date remains "limited" until violator retakes computer-based training)
11. IdMS will mail merge (including preparation of envelopes and labels) and allow for selection of checkboxes / data input on the following correspondence:

- Informal Resolution Denial Letter / Notice of Confirmation / Alternative Disposition
- NOV Rescission Letter (IdMS resets internal (temporary) expiration date back to expiration date printed on the badge if violation when violation is rescinded)

12. IdMS shall allow Aviation Security Manager/Airport Operations Manager or delegate to manually reduce / remove / edit points, NOCs/NOVs, etc.
13. IdMS shall provide data-rich reports and graphs re: NOCs / NOVs (e.g., # of violations by type within a certain timeframe, # of individuals who are repeat violators, # of open v. closed citations, etc.)
14. IdMS shall provide a "view only" page for Airport Duty Managers and Airport Operations Specialists to view citation-related history of a badge holder
15. [Optional] IdMS can schedule meeting for the Aviation Security Manager/Airport Operations Manager* or delegate (could be in dedicated meeting windows or via integration with MS Outlook)
16. *Note: For safety citations, the Airport Operations Manager (or delegate) only meets with violators with two or more points

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

Oakland International Airport Existing Business Process

(Attachment 12-2)

Table of Contents

Table of Figures

Table of Tables

(Page left intentIonally blank)

Section 1 Existing Systems & Technologies

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

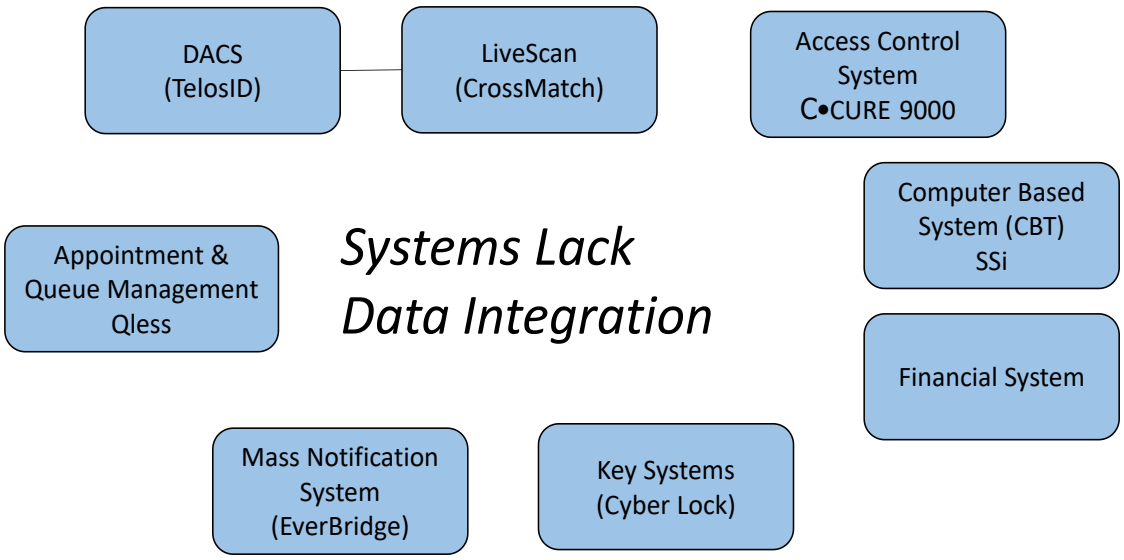


Figure 1: Various Standalone Systems at OAK

Access Control System (ACS) – The Airport ACS consists of a Software House C•CURE 9000 v2.8 application operating in a virtual environment within the Airport data center. The Airport uses the C•CURE ID badging functionality to design badges, store badge holder information, capture photo and print badges using existing badge printers (Fargo HDP 6600). The ACS creates clearance codes that are assigned to badge holders and grants them admittance to only the locations they need to access. The Airport manages a Company clearance code binder. The clearance codes are defined by the Badging Superintendent working with the Company AS and type of business at the Airport. This binder lists all the Companies at the Airport, and the clearance codes that can be assigned for a Company.

Badge #: The Airport keeps a master sheet of all the Badge #s. This number is assigned to a badge holder in the C•CURE system and printed on the front and back of the badge. The Badge # does not change unless the badge is issued for lost / stolen scenarios.

Card Technologies & Badge#- The Airport issues SEOS technology cards. The badge number (hot stamp) printed on the back of the badge by HID is programmed in C•CURE and used for access control. This number is entered in the C•CURE system and used by the access control system for opening /closing doors.

Fingerprint Live Scan Systems – The Airport uses 2 vendors – CrossMatch Guardian and Green Bit to capture Airport employee 10-prints for the Criminal History Records Checks (CHRC). The Airport currently

has six (5) CrossMatch systems and one (1) standby. The Airport is not satisfied with the performance of the Green Bit finger printing machines because they have a high level of difficulty capturing fingerprints that are easily captured with the CrossMatch machines.

Designated Airport Channeling Service (DAC) – The Airport Badging Office enters all the new applications in to the Telos ID Aviation Channeling Service for submission of Airport employee biographic information to the TSA for Security Threat Assessment and LiveScan fingerprints to the FBI for the Criminal History Records Checks (CHRC).

Financial Systems – The Airport currently uses a combination of an Oracle application system for monthly invoicing and Point of Sale devices for credit / debit card transactions for badge related fees.

Receipt Printer Application – The Badging Office uses a standalone browser-based application (Webers) for printing receipts for fingerprinting, badges, permits and key related fees.

Point-of-Sale (PoS) - Standalone Point of Sale devices at each badging counter for processing credit / debit cards. The printed receipt from the PoS and the transaction # are documented in the Weber application.

Computer Based Training Systems – The Airport uses on-premises interactive training system (ILS – Internet Learning System) provided by SSi. The training courses included are Security Awareness (Sterile), SIDA, Movement, Non-Movement, AOS and Vehicle Inspection. (Note: the new Sterile / SIDA training will also include a section on active shooter and IT training).

Cyber Keys – The Airport uses Videx CyberLock (CyberAudit Web Enterprise) system to create, assign doors, and issue cyber keys for certain restricted areas at the Airport. In addition to cyber keys, the Airport also issues metal keys to certain Airport employees. The key cutting system is managed by AVSEC and the maintenance groups at the Airport.

Mass Notification – The Airport uses the Everbridge mass notification system for critical operational notifications to all the Airport employees. The intent for the IdMS to capture and push active cardholder contact information to the Everbridge and when the badge is inactivated then remove the employee from Everbridge system.

Queueing System – The Airport Badging Office uses a queueing system called Qless. This is a standalone web hosted application that manages the day-to-day flow of employees into the Badging Office. The Qless application is also the appointment scheduling system.

Appointment Scheduler – The Airport allows applicants to schedule appoints (fingerprinting, badge renewal, training etc.) using the Qless URL/application made available via hyperlink on the Airport's website. This is a standalone web hosted application that does not interface with the existing badging systems.

Other non-badging systems at the Airport - Milestone XProtect Corporate video management system and Alert Enterprise Sentry insider threat detection software, both of which integrate with C•CURE 9000.

Section 2 Badging Office & Training Room Layout

The OAK Airport Badging Office, located in Terminal 1, is accessible to all Airport employees. The Airport Badging Office is configured with a check-in and waiting area, six (6) front desk workstation for applicant processing (applicant review, fingerprinting, payments, badge productions, key and vehicle permit issuance) and two separate offices for the Airport Security Analyst and Superintendent.

The six workstations are all equipped with the same software applications (Qless, C•CURE 9000, Webers, Telos ID, and SSi Training) and badging equipment – camera, LiveScan fingerprint, PoS, document scanner and badge printer.

Adjacent to the Badging Office is the Training room setup with seventeen (17) computer-based training workstations. The workstations are configured with the SSi training application.

#	EQUIPMENT	QUANTITY	MAKE & MODEL
1	Camera	7	VALCam USB Zoon+ Badging Camera
2	Document Scanner (multi or single page)	7	HP desktop flatbed scanner
3	Kiosk / Touch Screen	1	iPad Plus (customer queue)
4	Badge Printer	4	Fargo HDP 6600(including ability to print UV features)
5	Laminate – Custom or Standard	1	Standard Laminate (may switch to custom laminate)
6	Standard Paper Printer	1	

Table 1: Badging Office Equipment

Section 3 Badge Types, Privileges, and Expirations

The Airport has five Badge types, each providing varied levels of unescorted access to secured (SIDA, AOA, Sterile) areas of the Airport. The Airport issues one badge per person per company. Below is a description of various badge types and combination of privileges associated.

1. **Badge Type**: **ALL AREAS (Stripped GREEN and Gray band on the top)**

   Definition: Complete Unescorted access to all areas of the Airport.

   Badge Expirations: 2 Years (default), if AS or MDT then 1 year

   Example Applicable Airport Employees: Airport Security, Ops, ARFF, Emergency responders, Airlines (GSC's and mechanics) and local, state and Federal Government agencies

2. **Badge Type: SOUTH FIELD AREA (Stripped Red and Gray band on the top)**

   Definition: Unescorted access to South Field areas - pedestrian and vehicular access. There are certain movement and non-movement area restrictions. Vehicle Permits might be required as well.

Badge Expirations: 2 Years (default), if AS or MDT then 1 year

Example Applicable Airport Employees: Airlines - Allegiant, Alaska, Contour, Frontier, Delta, Hawaiian, Sata, Southwest, Spirit and Volaris

3. **Badge Type: NORTH FIELD SIDA (Solid YELLOW band on the top)**

   Definition: Unescorted access to North Field areas - pedestrian and vehicular access. There are certain movement and non-movement area restrictions. Vehicle Permits might be required as well.

   Badge Expirations: 2 Years (default), if AS or MDT then 1 year

   Example Applicable Airport Employees: Airlines Alameda Aero Club, Civil Aviation Patrol, Jet Suite X, Kaiser Air, Oakland Flyer's and Signature

4. **Badge Type: NORTH FIELD SIDA (Solid YELLOW band on the top)**

   Definition: Unescorted access to North Field areas - pedestrian and vehicular access. There are certain movement and non-movement area restrictions. Vehicle Permits might be required as well.

   Badge Expirations: 2 Years (default), if AS or MDT then 1 year

   Example Applicable Airport Employees: Airlines Alameda Aero Club, Aviation Institute, Civil Aviation Patrol, Kaiser Air and Signature

5. **Badge Type: CARGO SIDA (Stripped Blue and Gray band on the top)**

   Definition: Unescorted access to Cargo areas - pedestrian and vehicular access. There are certain movement and non-movement area restrictions. Vehicle Permits might be required as well.

   Badge Expirations: 2 Years (default), if AS or MDT then 1 year

   Example Applicable Airport Employees: Cargo tenants – UPS

6. **Badge Type: STERILE AREA ONLY (Solid GRAY band on the top)**
   Definition: Unescorted access to Sterile areas of the terminal only. No other access to and from the Secured or AOA to the sterile areas.

Badge Expirations: 2 Years, if AS or MDT then 1 year

Example Applicable Airport Employees: Concessionaries – SSP America, High Flying Foods, Soaring Food Group and World Duty Free Group

Note: The badges expiration dates are calculated 1 or 2 years from the training completion date.

List of various Privileges that are printed on the badge:

- ZONE 1 – Red Seal (FIS areas contiguous to aircraft interior with passenger's present)
- ZONE 2 – Black Seal (IT baggage makeup, ramp area, and deplaned aircraft interior and areas of no passenger presence)
- Emergency Access Authorization ("E") for Emergency response personnel
- Escort – To escort unbadged personnel.
- C – Contractor Designation (option available on application form but no longer in use)
- RED – Vehicle denotes AOA Movement Area driving privileges (sticker decals) *
- BLUE – Vehicle denotes AOA Movement Area-Taxiways Only driving privileges (sticker decals) *
- YELLOW – Vehicle denotes AOA Non-Movement Area driving privileges
- LEO – Armed Law enforcement
- Future consideration: "AS" to designate Authorized Signers
- Agency / department / function emblem – AVSEC, , LSO, OPS, FAC - department designation for Port staff

** The Airport's intent is to eliminate the sticker process and print the badge with yellow vehicle icon until the applicant completes the practical movement training with OPS, and then reprint badge with blue vehicle icon. The Badge types have privileges that the AS can requests based on the job description for the Airport Employee. The badge also has a standard laminate on the badge.*

The Airport currently does not issue visitor badges.

	AOA DRIVING PRIVILEGES							CBP ZONES	
BADGE TYPE	NON-MOVEMENT (NMDT)	MOVEMENT (MDT – FULL)	MOVEMENT (MDT – TAXIWAY)	ESCORT	EMERGENCY RESPONSE PERSONNEL	ALT. SHUNT*	A S	RED	BLACK
All Areas	·	·	·	·	·	·	·	·	·
South Field Area	·	·	·	·	·	·	·	·	·
North Field SIDA	·	·	·	·			·		
Cargo SIDA	·	·	·	·			·		·
Sterile Area Only				·			·	·	

Table 2: Badge Types

- - Alt SHUNT – for Gate operators for delayed alarm.

Section 4 Existing User Roles and Business Process

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

4.1 User Roles

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

#	USER ROLE	RESPONSIBILITIES
1	Authorized Signatory	Review and authorization of new badge applicants and access / key requests, authorization of renewals (badge, ramp permits), respond to badge audits and involved with citations hearings and coordinating trainings for applicants, forms submissions for CBP Seal approval.
2	Applicant	Coordinate with Authorized User for the company to complete badge application.
3	Trusted Agents / Badging Office Staff	Badge applicant data entry in various disparate systems, fingerprinting, document verification and scanning, badge production, payment collection, receipt generation, tracking RAP back enrollment and removal in DAC system, paper log for keys, ramp permits and badge holder paper records.
4	Badging Office Admin Analyst II	Manage all tasks of Trusted Agents and management of keys, ramp permits, CHRC adjudication notifications, STA clearance, DAC provider contract maintenance, citations program, finance department coordination, coordination with CBP for Seal approvals.

#	USER ROLE	RESPONSIBILITIES
5	ID Badging Office Superintendent	Manage all tasks of Admin. Analyst II, review of CHRC Rap sheets and security check adjudication, coordinate hearings for CHRC appeals, manage review of, issuance, adjudication and interview process for citation and violations (in lieu of Airport Security Manager).
6	Airport Security Manager	Manage the above tasks for Superintendent and be decision maker for citations and rap sheets adjudications,
7	Airport Operations	Conduct practical movement area training and coordinate with Badging Office for appropriate driver endorsement on the applicant badge. Update citation information (see citation workflow).
8	Risk Transfer Team (Risk Management Department, also referred to as OAK Operations)	Review and verification of company insurance for ramp permit issuance.
9	Airport Facilities Team	Key request review and assignment, coordinate with badge office staff / trusted agents for issuance / return of keys.

Table 3: Users and Responsibilities

4.2 Employee Badge Issuance Workflow

This section describes various workflow processes.

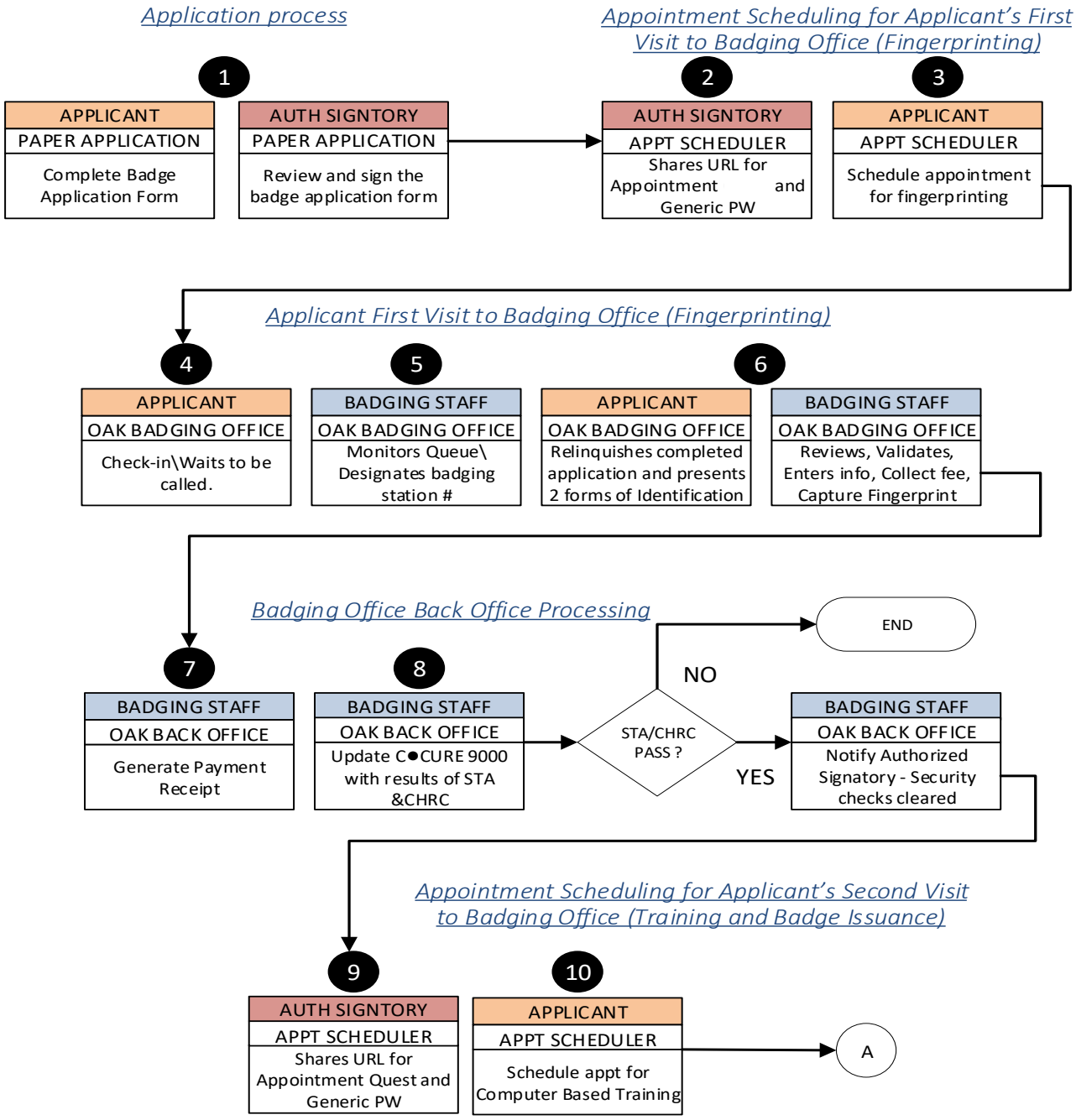


Figure 2: Employee Badge Issuance Work Flow – Steps 1 - 10

Application Process

1) **Paper Application: Applicant & Authorized Signatory (AS)**: Together the applicant and AS complete the necessary paper application forms (Reference Appendix A) available on the OAK website.

   i. OAK-ID-BADGE-Application;

   ii. Badge Fingerprint App and

   iii. Access Control Request

   iv. Authorized Signer form

The AS must submit additional requests for:

   i. if the applicant requires translation services during the training process (Reference Appendix A: Request for Accommodation Application)

   ii. if the applicant needs to access the south field ramp area of the Airport (Reference Appendix A: Southfield Ramp App)

   iii. if the applicant needs Customs area access. (standard Customs form 3078)

Appointment Scheduling for Applicant's First Visit to Badging Office (Fingerprinting)

2) **Appointment Scheduler**: Authorized Signatory: After the application is complete, the Authorized Signatory shares with the Applicant the Qless URL/application.

3) **Appointment Scheduler**: Applicant: The Applicant using the Qless URL/application and schedules an appointment for "FINGER PRINTING".

Applicant First Visit to Badging Office (Fingerprinting)

4) **OAK Badging Office**: Applicant: The applicant appears at the Badging Office at the appointment time. Using the Qless queueing system the applicant checks-in and waits for the name to be called on the display screen in the waiting area or via their smart phone.

5) **OAK Badging Offic**e: Trusted Agent / Badging Staff: The Badging Office monitors the queue and calls the next applicant in the queue processing indicating the Station # and the Trusted Agent's name, where the applicant needs to report to.

6) **OAK Badging Office**: Applicant & Trusted Agent / Badging Staff: The Applicant walks over to the indicated Station # and hands over the completed paper applications and 2 forms of IDs as per OAK I-9 documents (Reference Appendix A: BadgeAcceptableDocuments2020) to the Badging Office staff. The Badging Office staff reviews the application for completion, visually validate the authenticity of the I9 documents, compares the AS signature on the application to the Badging Office reference signature and if all is acceptable then the Badging Office staff:

   i. Makes copies of the I9 documents (Scan using flatbed scanner and print); scanned documents are saved by Telos ID.

ii. Enters the Applicant data in separately in Telos ID and C•CURE 9000 systems.

iii. Collects the payments as check or debit / credit using the Point-of-Sale device. The Payment is collected for fingerprinting and badge production.

iv. Using the CrossMatch to capture slap prints of the Applicant's 10- digits and complete the Telos ID transaction for STA and CHRC.

After this step, the Applicant leaves the Badging Office with instructions that the AS will contact the applicant for the further steps for training and badge pick up.

Badging Office Back Office Processing

7) **OAK Badging Office: Trusted Agent / Badging Staff**: The Badging Office staff then perform back-office tasks such as:

i. Using the Webers receipts application, generate the payment receipt for the Applicant and for the Port Finance department. The receipts and reports are submitted to Finance Department as electronic (excel) files as well as paper copies.

8) **OAK Badging Office: Designated Trusted Agent / Badging Staff**: A designated Trusted Agent in the Badging Office checks the TelosID system and the FBI's FPRD website. The designated trusted agent captures the results of the STA and CHRC from the respective websites and updates the applicant's record in C•CURE 9000.

i. If the applicant has passed both (STA and CHRC) security checks then an email notification is sent to the AS. The email notification provides the AS the instructions for the Applicant to schedule Training appointment. The Trusted Agent configures the SSi system with the necessary training roles / courses as per the Application requirements.

ii. If the applicant has failed one or both (STA and CHRC) security checks then an email notification is sent to the AS. (Reference Appendix B: CHRC letter). The email notification provides the AS with notification that the applicant has not passed a background check, has a denial letter attached (which is sent via certified mail to the applicant) and instructions for the Applicant to appeal the CHRC results with the Airport OR the STA results with the TSA. No further processing (no badge issuance) in C•CURE or Telos ID until further directions are received by the Badging Office Superintendent from the Airport Security Coordinator (ASC). (Note: a similar process occurs when OAK receives notification from Telos regarding hits to a badge holder's RAP sheet, through the RAP Back program).

Appointment Scheduling for Applicant's Second Visit to Badging Office (Training and Badge Issuance)

9) **Appointment Scheduler: Authorized Signatory**: After receiving security checks completion notification, the Authorized Signatory (AS) shares with the Applicant the url for the Qless.

10) **Appointment Scheduler: Applicant**: The Applicant using the Qless url and schedules an appointment for "Training". Depending on the applicant, they will need to determine how many training classes the applicant needs. Please see chart:

Training Class	Sterile Area Only	SIDA	Non-Movement Driver	Movement Driver	Authorized Signer
Frequency Required (Typically)	Every 2 Years (Every Other Year)	Every 2 Years (Every Other Year)	Every 2 Years (Every Other Year)	Every Year (Annually)	Every Year (Annually)
Training (1 Class Only)					
	X	X		X	X
Training (2 Classes)					
		X	X		
		X			X
	X				X
				X	X
Training (3 Classes)					
		X	X	X	
		X	X		X
Training (4 Classes)					
		X	X	X	X

Applicant Second Visit to Badging Office (Training and Badge Issuance)

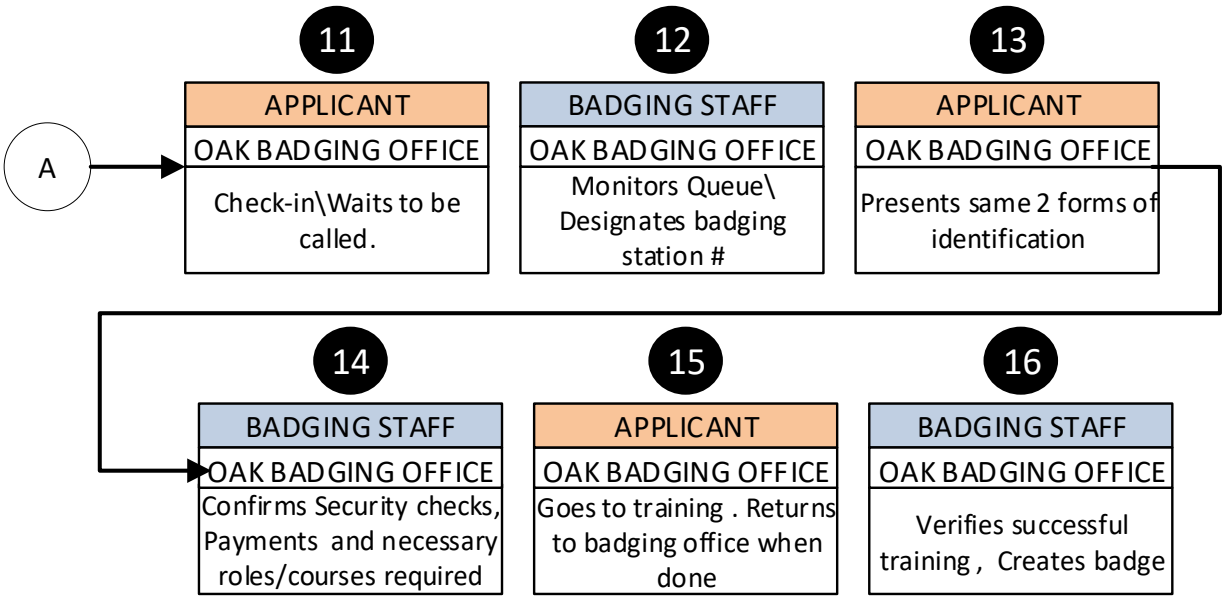


Figure 3: Employee Badge Issuance Work Flow – Steps 11 - 16

Applicant Second Visit to Badging Office (Training and Badge Issuance)

11) **OAK Badging Office**: Applicant: The applicant appears at the Badging Office at the appointment time. Using the Qless queueing system the applicant checks-in and waits for the name to be called on the display screen in the waiting area.

12) **OAK Badging Office**: Trusted Agent / Badging Staff: The Badging Office monitors the queue and calls the next applicant in the queue application indicating the Station # where the applicant needs to report to.

13) **OAK Badging Office**: Applicant & Trusted Agent / Badging Staff: The Applicant walks over to the indicated Station # and hands over the same 2 forms of IDs as per OAK I-9 documents (Reference Appendix A: BadgeAcceptableDocuments2015) to the Badging Office staff.

14) **OAK Badging Office**: Trusted Agent / Badging Staff: The Badging Office staff confirm the security checks are complete and notes indicated in C•CURE, the badge production payments are collected in the Weber and then confirm that the SSi system is configured for the necessary roles / courses that need to be completed by the applicant.

15) **OAK Badging Office**: Applicant: The Applicant walks over to the Training room and logins into to one of the workstations. The applicant completes the training and returns to the Badging Office.

16) **OAK Badging Office**: Trusted Agent / Badging Staff: The Badging Office programs a SEOS iClass card in C•CURE 9000, assigned the necessary clearance codes and printed the badge. The

clearance codes are based on the job description or company name defined in the Company clearance code binder. If the Customs approval is received then the Customs seal is printed else the badge is printed without the customs seal.

The Badging Office staff confirms in the SSi system that the applicant has Passed the training and then hands over the badge making a note in C•CURE 9000 of training completion dates. The Badging Office also enrolls the applicant in the Telos ID system for Rap back program. If the applicant has Failed the training, then the badge is not issued and marked in C•CURE as training failed. If the applicant fails the training 3 times, the Applicant must wait 24 hours to retake the training. If the applicant continues to have difficulty, the applicant will meet with the ASC to discuss accommodations.

Other Badge Related Work Flows

1) **CHRC Appeals Process**: The Airport denies badge to the applicant due to concerns over the CHRC results (Rap sheet) and send notification to the AS. The Applicant can appeal the determination by sending a letter to the ID Badging Office Superintendent or ASC. The Superintendent or ASC schedules an interview meeting with the applicant and if additional information is provided then the Superintendent or ASC can overturn the denial. The Superintendent or ASC informs the applicant and ID Badging staff with decision of the appeal.

2) **Badge Issuance Post Practical Movement Area Training**: The practical movement area training occurs based on Airport Operations availability (typically once a week). The Badging Office will print the badge with Non-movement area insignia on the badge and then once the applicant completes the Movement area training the badge is either re-printed or an appropriate decal sticker (red or blue) is affixed on the badge.

3) **Badge Renewal** work flow is same including signed application forms by Authorized Signatory, except the employee is not required to fingerprint again. The employee must produce two forms of I-9 documents for identity verification and complete the necessary re-trainings (Movement or Non-movement area training and AS training if applicable) prior to badge renewal.

4) **Badge Re-issuanc**e (name change, changes to privileges on existing Active badge, lost / stolen) work flow is same including signed application forms by Authorized Signatory. The employee must produce two I-9 documents for identity verification ad include Alias for name change.

5) **Dual Badge** (two separate badges issued for an individual working for two separate companies) work flow is same including signed application forms by Authorized Signatory, except the employee is not required to fingerprint again. The employee must produce two forms of I-9 documents for identity verification and complete trainings not required for the current badge. The second badge expiration date will coincide with the first badge expiration date.

6) **CBP Zone 1 (Red) or Zone 2 (Black) Work Flow** – The AS completes the standard CBP 3078 form and an Introduction letter for applicants who have never had a customs seal, and manually submits to the CBP office at the Airport. The CBP office performs the security checks and informs the Badging Office of approval or denial of the request of the Customs seal. If approved, the CBP

will inform Badging Office the Zone that the applicant is approved for. The Badging Office send notification to the AS that the CBP seal is approved. The Applicant then visits the Badging Office to pickup / replace the badge endorsed with Customs Seal. Implementation of eBadge process for CBP seal application and approval by the CBP office.

Key (Cipher or Metal) Approval and Issuance

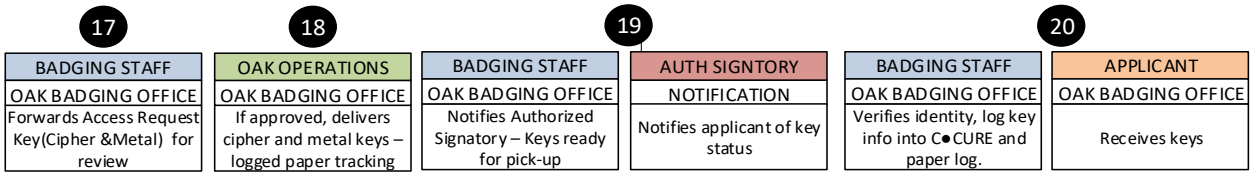


Figure 4: Employee Badge Issuance Work Flow – Steps 17 - 20

Key (Cipher or Metal) Approval and Issuance

The Airport issues metal and cipher keys to badge Airport employees only. The metal keys provide access to Non-restricted areas of the Airport. The Cipher keys provide access to the secured areas of the Airport. The issuance of Cipher is primarily restricted to the Port and Airline Employees.

17) OAK Badging Office: Trusted Agent / Badging Staff: Once the security checks are complete or the badge is issued the Badging Office notifies via email and a paper copy of the Access Request key (cipher and metal keys) form to other Airport staff for review:

   i. ASM, SS – for all types of key requests

   ii. Port Facilities manager – for metal key requests (only X1 and X2 keys)

   iii. IT Manager – for access to IT rooms (IDF / MDF)

   The approved or denied requests are sent back to the Badging Office via email and paper copy.

18) **Airport Facilities Team**: If the request is approved, then the Airport Facilities team delivers the metal keys to the Badging Office or programs cypher locks in the field. The delivery of the keys is documented on a paper based tracking sheet.

19) **OAK Badging Offic**e: Trusted Agent / Badging Staff: The Badging Office informs the Authorized Signatory that the requested keys are ready for the applicant to collect from the Badging Office.

20) **OAK Badging Office**: Applicant and Trusted Agent / Badging Staff: The Badging Office staff verifies the identity based, log the key information in C•CURE and on the paper based tracking sheet and issues the key to the airport employee, who signs for receipt of the key

   NOTE: Currently the Airport conducts key audits on controlled keys as described in the ASP. The Airport employees must return all the keys when returning badge.

South Ramp Permit Approval and Issuance

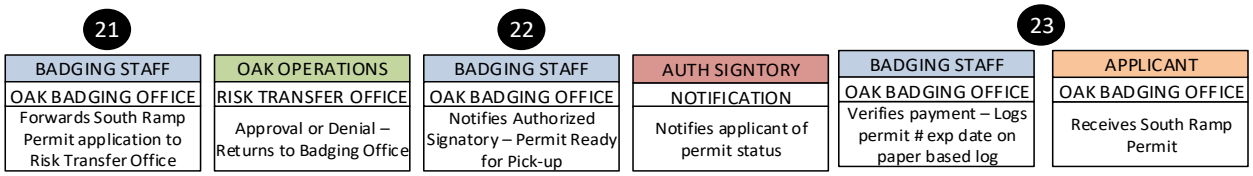


Figure 5: Employee Badge Issuance Work Flow – Steps 21 – 23

South Ramp Permit Approval and Issuance

1) **OAK Badging Office:** ***Trusted Agent / Badging Staff:*** Once the security checks are complete or the badge is issued, the Badging Office forwards the South Ramp Permit Applicant and Agreement including the Certificate of Insurance to the Port's Risk Transfer Office. The approved or denied requests is sent back to the Badging Office from the Risk Transfer office.

2) ***OAK Badging Office:*** If the request is approved, then the Badging Office informs the Authorized Signatory that the requested permit is ready pick up from the Badging Office.

3) **OAK Badging Office:** ***Applicant and Trusted Agent / Badging Staff:*** The Badging Office staff verifies the payment is collected, log the permit number and the expiration date information on the paper based tracking sheet.

Other Ramp Permit Work Flows

1) **Permit Renewal** work flow is same including signed application forms by Authorized Signatory. The Airport Badging Office and Port Risk team verify that that the insurance requirements are valid and then only issue date stickers (Month and Year) that will be affixed to the permit on the vehicle.

4.3 Company Financial Setup

Currently, the Badging Office manages three methods for collecting badge fees.

- Monthly invoicing,
- Over-the-counter (check / money order or credit / debit card), and
- Waived (for Port and some Government agencies)

For monthly invoicing companies, the Badging Office coordinates with the Port's Finance Department to setup a company as monthly invoice. All badge fees (fingerprinting and badge production fees) are then tracked monthly and a report submitted to Finance department for processing via email attachment of excel file and paper copies.

For over-the-counter, the applicants paying using credit / debit cards using the Point of Sale devices. The Point of Sale system is connected to the Port's Union Bank account. For applicants paying with checks, the

Badging Office collects the checks and reconcile all the checks for the day / week / month and send to Financial Department for processing.

The Airport staff raised concerns with the current financial work flows in the Badging Office as well as post processing required for invoice generation and collections. Some of the concerns are listed below:

1) The Badging Office manually generates excel spread sheet style reports and submits to the Finance department via email. The Finance department imports the excel reports and manually verifies the transaction log in the financial system to generate the invoice. The Finance Department issues approximately 40 to 50 invoices monthly to various companies.

2) The financial department currently has no method in place for informing the Badging Office if a company is not paying for the badges or is delinquent and to stop badge processing.

4.4 Citation Program

The OAK Airport has defined a comprehensive Notice of Citations (NoC) and Notice of Violations (NoV) program that encompasses security, safety, individual, commercial, and ground transportation. For the purposes of the IdMS, the focus is on Security and Safety types of violations.

- The Airport has identified specific roles that can issue and administer the citations and violations.
- Security-related violations can be issued and administered by the Port Aviation Security personnel, Port Operations personnel, and the Aviation Security Manager.

Airside safety-related violations can be issued and administered by the Airside Operations Manager.

The citations are issued in the field and followed by a review with the citation issuer and the Security or Operations Manager. The Security or Operations manager decides to issue a Notice of Violation which then requires the Airport employee in question to take certain remedial actions.

Both Security and Safety violations categories are grouped in Four (4) Levels - Level I through IV. Each level has violations defined with varying intensity. Additionally, the citations are counted for a duration of 2-year period. Based on the number of violations and violation level, a severity-related point system is used and there are points assigned and tracked against the Airport employee. The remedial actions are determined by the Managers as defined in the program and that could be a combination of interviews with the Security / Operations Managers, hearings, re-trainings (within 30 days or timeframe identified by the ASC), Fines ($150, or $250) or permanent revocation of badge.

After the 2-year period, closed violations no longer count against the Airport employee's record. If the number of citations reaches 3, and cumulative points are 6 or over, then the Airport has the right to permanently revoke the badge. The employee cannot apply for another badge at the Airport for a period of 1 year.

The current process is labor and time intensive. There are legal requirements for sending the letter of Violations (NoV) as certified mail. Security staff also forward the NoV to the badge holder's AS via email.

4.5 Badge Audit Program

The Airport implements physical access card reader based audit as well as list based audit. The Airport implements random audit (10% of one badge group {ie Cargo}) and an annual comprehensive badge audit.

Appendix A **OAK Badge Application Forms**

1) OAK-ID-BADGE-Application-0220
2) ID Badge Fingerprint Application
3) ID Badge Acceptable Documents
4) Airport Security Access Control Request Form
5) Request for Accommodation
6) Southfield Ramp Permit Application

Appendix B OAK Sample Email Notifications

CHRC Letter (New Applicant with No Escort)

CHRC Letter (New Applicant with Escort)

CHRC Letter (New Application with No Escort)

CHRC Letter (New Application with Escort)

CHRC Follow Up to Submitting Court Record

RAP Back Letter (With Escort)

RAP Back Letter (No Escort)

PORT OF OAKLAND

BRYANT L. FRANCIS
Director of Aviation

May 24, 2018

Via Certified Mail 7013 1090 0002 1073 2824

John Doe
1 Airport Dr
Oakland, CA 94621

RE: Disqualifying criminal offence in accordance with 49 CFR 1542.209

Dear Mr. Pittman,

The Oakland International Airport (OAK) must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based Criminal History Records Check (CHRC) that does not disclose any conviction(s) of a disqualifying criminal offense in accordance with 49 CFR 1542.209. It has been determined based upon your CHRC that you **are not** qualified to obtain unescorted access authority at OAK nor may you be escorted anywhere within the Oakland International Airport SIDA, Secured or Sterile areas.

In order to resolve this matter, within the next 30 calendar days you must produce official records that show you were not convicted of a disqualifying criminal offense as reported to the Airport on your CHRC RAP sheet. After 30 calendar days this determination will become final if the requested information is not provided that permits the Airport to issue you an ID Badge. If you would like a copy of your CHRC rap sheet, it will be provided to you. All requests must be in writing and directed to my contact information below.

Please let me know if you have any questions regarding this determination, please contact me at (510) 563-3848 or JGraef@portoakland.com.

Sincerely,

Jacob Graef
Aviation Security /ID Superintendent
Oakland International Airport
1 Airport Dr. Box 45
Oakland, CA 94621

PORT OF OAKLAND

BRYANT L. FRANCIS
Director of Aviation

January 8, 2018

Via Certified Mail 7013 1090 0002 1073 6199

John Doe
1 Airport Dr.
Oakland, CA 94621

RE: Disqualifying criminal offence in accordance with 49 CFR 1542.209

Dear Mr. Howard,

The Oakland International Airport (OAK) must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based Criminal History Records Check (CHRC) that does not disclose any conviction(s) of a disqualifying criminal offense in accordance with 49 CFR 1542.209. It has been determined based upon your CHRC that you **may not** be qualified to obtain unescorted access authority at OAK.

In order to resolve this matter, within the next 30 calendar days you must produce official records that show you were not convicted of a disqualifying criminal offense as reported to the Airport on your CHRC rap sheet. If you fail to provide the requested documentation after 30 calendar days, this determination will become final. If you would like a copy of your CHRC rap sheet, it will be provided to you. All requests must be in writing and directed to my contact information below.

In the interim, you can be escorted anywhere within the Oakland International Airport SIDA, Secured or Sterile areas. After 30 calendar days this determination will become final if the requested information is not provided that permits the Airport to issue you an ID Badge. Please let me know if you have any questions regarding this determination, please contact me at (510) 563-3848 or JGraef@portoakland.com.

Sincerely,

Jacob Graef
Aviation Security /ID Superintendent
Oakland International Airport
1 Airport Dr. Box 45
Oakland, CA 94621

PORT OF OAKLAND

BRYANT L. FRANCIS
Director of Aviation

August 1, 2018

Via Certified Mail 7013 1090 0002 1073 3302

John Doe
1 Airport Dr.
Oakland, CA 94621

RE: Renewal applicant-disqualifying criminal offence in accordance with 49 CFR 1542.209

Mr. Boyd,

The Oakland International Airport (OAK) must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based Criminal History Records Check (CHRC) that does not disclose any conviction(s) of a disqualifying criminal offense in accordance with 49 CFR 1542.209. It has been determined based upon your CHRC that you **may not** be qualified to retain your ID badge (aka: unescorted access authority) at OAK.

In order to resolve this matter, within the next 30 calendar days you must produce official records that show you were not convicted of a disqualifying criminal offense as reported to the Airport on your CHRC rap sheet. If you fail to provide the requested documentation after 30 calendar days, this determination will become final. If you would like a copy of your CHRC rap sheet, it will be provided to you. All requests must be in writing and directed to my contact information below.

In the interim, you can continue to use your badge anywhere within the Oakland International Airport SIDA, Secured or Sterile areas. Please be aware that your ID Badge will be permanently revoked after 30 calendar days if the requested adjudication information is not provided. Please let me know if you have any questions regarding this determination, please contact me at (510) 563-3848 or JGraef@portoakland.com.

Sincerely,

Chris Haas
Aviation Security Superintendent
Oakland International Airport
1 Airport Dr. Box 45
Oakland, CA 94621

PORT OF OAKLAND

BRYANT L. FRANCIS
Director of Aviation

July 26, 2018

Via Certified Mail 7011 3500 0002 6968 5698

John Doe
1 Airport Dr.
Oakland, CA 94621

RE: Renewal applicant-disqualifying criminal offence in accordance with 49 CFR 1542.209

Ms. Lenard,

The Oakland International Airport (OAK) must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based Criminal History Records Check (CHRC) that does not disclose any conviction(s) of a disqualifying criminal offense in accordance with 49 CFR 1542.209. It has been determined based upon your CHRC that you **ARE NOT** qualified to retain your ID badge (aka: unescorted access authority) at OAK.

In order to resolve this matter, within the next 30 calendar days you must produce official records that show you were not convicted of a disqualifying criminal offense as reported to the Airport on your CHRC rap sheet. If you fail to provide the requested documentation after 30 calendar days, this determination will become final. If you would like a copy of your CHRC rap sheet, it will be provided to you. All requests must be in writing and directed to my contact information below.

In the interim, you cannot work or be escorted anywhere within the Oakland International Airport SIDA, Secured or Sterile areas. Please be aware that your ID Badge will be permanently revoked after 30 calendar days if the requested adjudication information is not provided. Please let me know if you have any questions regarding this determination, please contact me at (510) 563-3848 or JGraef@portoakland.com.

Sincerely,

Jacob Graef
Aviation Security /ID Superintendent
Oakland International Airport
1 Airport Dr. Box 45
Oakland, CA 94621

PORT OF OAKLAND

BRYANT L. FRANCIS
Director of Aviation

March 24, 2018

Via Certified Mail

John Doe
1 Airport Dr.
Oakland, CA 94621

RE: Disqualifying criminal offence in accordance with 49 CFR 1542.209

Ms. Davis,

In reviewing the documentation you provided regarding the results of your fingerprint-based criminal history records check, we have concluded that this conviction for California Penal Code 245(A)(1) in November 2015, is a disqualifying offense pursuant to 49CFR1542.209(d)(20).

At this point in time, your access privileges for the Oakland International Airport are revoked, and you are not allowed to be in any security area of the Airport, even escorted.

Please return you current access badge at your earliest convenience. Badges may be returned to your employer, the Oakland Airport ID Badging Office, or placed in the mail.

Please let me know if you have any questions regarding this determination, please contact me at (510) 563-2906 or CHaas@portoakland.com.

Sincerely,

Jacob Graef
Aviation Security /ID Superintendent
Oakland International Airport
1 Airport Dr. Box 45
Oakland, CA 94621

PORT OF OAKLAND

BRYANT L. FRANCIS
Director of Aviation

December 7, 2018

Via Certified Mail 7013 1090 0002 1073 3739

John Doe
1 Airport Dr.
Oakland, CA 94621

RE: Criminal History Record Check-disqualifying criminal offence in accordance with 49 CFR 1542.209

Dear Mr. Givens,

The Oakland International Airport (OAK) must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based Criminal History Records Check (CHRC) and is successfully enrolled in the FBI RAP Back Program, without receiving notification of any conviction(s) of a disqualifying criminal offense in accordance with 49 CFR 1542.209. It has been determined based upon your RAP Back subscription that you **may not** be qualified to retain your ID badge (aka: unescorted access authority) at OAK.

In order to resolve this matter, within the next 30 calendar days you must produce official records that show you were not convicted of a disqualifying criminal offense as reported to the Airport on your CHRC rap sheet and/or communicate the details of the disqualifying offense/ legal proceedings with the Security Superintendent. The determination to revoke your badge will become final if you fail to do this within 30 calendar days. If you would like a copy of your CHRC rap sheet, it will be provided to you. All requests must be in writing and directed to my contact information below.

In the interim, you can continue to use your badge anywhere within the Oakland International Airport SIDA, Secured or Sterile areas. Please be aware that your ID Badge will be permanently revoked after 30 calendar days if the requested adjudication information is not provided. Please let me know if you have any questions regarding this determination, please contact me at (510) 563-3848 or JGraef@portoakland.com.

Sincerely,

Jacob Graef
Aviation Security Superintendent
Oakland International Airport
1 Airport Dr. Box 45
Oakland, CA 94621

PORT OF OAKLAND

BRYANT L. FRANCIS
Director of Aviation

December 7, 2018

Via Certified Mail 7013 1090 0002 1073 3739

John Doe
1 Airport Dr.
Oakland, CA 94621

RE: Criminal History Record Check-disqualifying criminal offence in accordance with 49 CFR 1542.209

Dear Mr. Givens,

The Oakland International Airport (OAK) must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based Criminal History Records Check (CHRC) and is successfully enrolled in the FBI RAP Back Program, without receiving notification of any conviction(s) of a disqualifying criminal offense in accordance with 49 CFR 1542.209. It has been determined based upon your RAP Back subscription that you **are not** qualified to retain your ID badge (aka: unescorted access authority) at OAK.

In order to resolve this matter, within the next 30 calendar days you must produce official records that show you were not convicted of a disqualifying criminal offense as reported to the Airport on your CHRC rap sheet and/or communicate the details of the disqualifying offense/ legal proceedings with the Security Superintendent. The determination to revoke your badge will become final if you fail to do this within 30 calendar days. If you would like a copy of your CHRC rap sheet, it will be provided to you. All requests must be in writing and directed to my contact information below.

Please be aware that your ID Badge will be permanently revoked after 30 calendar days if the requested adjudication information is not provided. Please let me know if you have any questions regarding this determination, please contact me at (510) 563-3848 or JGraef@portoakland.com.

Sincerely,

Jacob Graef
Aviation Security Superintendent
Oakland International Airport
1 Airport Dr. Box 45
Oakland, CA 94621

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

Oakland International Airport IdMS Specifications and Technical Specifications Compliance Matrix

(Attachment 12-3)

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
1	**General IdMS Capabilities**					
1.01	Provide an Identity Management System with capability to track each person (applicant or badge holder) as a uniquely identified entity, associating with it related activities such as employers, documents, fingerprints, security checks (STA, CHRC, Rapback, eBadge), training records, badges, keys.	M				
1.02	IdMS shall enforce and prevent badge issuance (print) until all applicable procedures (e.g. Employment verification, I-9 Documents, CHRC/STA, and Training) have been successfully completed. The IdMS shall have capability to allow for supervisor override when printing the badge.	M				
1.03	IdMS shall assign a Unique Person ID (UPI) for each person employed at the airport. This ID will be used across all systems and will remain constant for that person.	M				
1.04	Only one UPI will be assigned to a person regardless of the number of companies they work for and cannot be based on the employee's name, SSN, or any other ID.	M				
1.05	IdMS shall have capability to detect duplicate records or existing person record (based on matching criteria SSN, DoB, Name) and immediately indicate to the Trusted Agent at the time of badge application processing.	M				
1.06	The IdMS shall display limited information as per the Airport requirements including a photo of the person that is identified as existing or duplicate in the IdMS. Allow the Trusted agent to accept or deny the individual.	M				
1.07	IdMS shall allow capability by the Trusted Agent or provide a procedure to search and merge multiple badge holder records of the same single individual.	M				
1.08	IdMS must provide a means for Security Office staff to reconcile duplicates and indicate if a near match is indeed a unique person.	M				
1.09	Allow capability to perform advance search the database using multiple fields and combinations of those fields as search criteria. (i.e. person name, DoB, SSN, (partial SSN), company name, badge #, badge status, badge type, designations, citations/violations, contract #, contract name)	M				
1.1	Provide a mechanism for identifying applicants (during badge application processing) 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.	M				
1.11	The IdMS shall encrypt sensitive and personally identifiable information at rest and in transit for internal as well as external users (AS and Applicant).	M				
1.12	Support the creation of new business policies/rules regarding how and when a badge or credential shall be issued without any modifications to code.	O				
1.13	Provide system administrators the ability to implement changes to business rules and variables options without code modifications or programming.	O				
1.14	Manage concurrent user sessions on a single shared credentialing workstation while accurately identifying the user making the change, for audit purposes.	M				
1.15	Support input of unlimited referential comments associated with persons, company, security checks, training, badges, access levels, keys, each of which is automatically user/date/time stamped. (e.g. - Notes for violations to be added within the cardholder profile violation tab, notes for background checks to be entered within the cardholder profile background check tab)	M				
1.16	Restrict Trusted Agent ability to change/delete comments they entered.	M				
1.17	Allow Security Manager, ASC or other Trusted Agents to make modification to the comments entered by the Trusted Agents.	O				
1.18	Provide ability to make comments private or hot note based on user roles.	O				
1.19	Allow operators to flag a note / comment so that the note / comment will be immediately displayed when any user subsequently accesses the record until the user that made the comment, or a supervisor changes or deletes the note / comment.	M				
1.20	Provide a flexible and extensible design change management procedure to incorporate additional features or modules. (e.g. regulatory changes)	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
1.21	Provide warnings or a report for follow-up when the only remaining Authorized Signatory for a company badge is inactivated.	M				
1.22	Ability to print IdMS escort badges, Port management badges, visitor badges, temporary badges. Currently all these badges after checks based on SecurFlight are printed from the Ccure system.	O				
1.23	IdMS shall allow the system administrator to create and modify business rules without requiring major code changes.	O				
2	**User Interface**					
2.01	Intuitive and easy to follow requiring minimum training. The UI shall drive the user to complete relevant tasks and clearly display next step and missing mandatory information.	M				
2.02	The IdMS shall clearly display on the badge holder record the stage / status the person is in, at any giving time (e.g. pending security checks, incomplete training, fee not collected).	M				
2.03	Ensure standard drop down lists / master data values are sorted alphabetically (e.g. US states, country names, ethnicity). Ensure commonly used drop down / master data values are on the top (e.g. United States country when entering Passport or DL).	M				
2.04	The IdMS shall have common sense field formatting / validations. (e.g. age minimum limit to 16 years (configurable), height cannot be in inches only and cannot be 10' or cannot accept alpha characters for age, height, weight.) Ensure the UI enforces data type, field length, and formatting limitations as per all the dependent subsystems (e.g. PACS, fingerprinting, I-9 documents).	M				
2.05	The IdMS shall have capability to interface with USPS address validation API.	O				
2.06	Provide the capability to mask all or specific Personal Identifiable Information (PII) (e.g. SSN) and non-PII (e.g. PIN) data fields for display after initial input. The masking will be based on business rules and allow the airport to modify PII fields. The UI will clearly indicate if the data is missing.	M				
2.07	Provide the capability that the masked data fields are viewable to certain user groups like Airport Security Manager, ASC or designees as determined by the Airport.	M				
2.08	Support user defined data elements and edit controls. (example: Data fields can be made view only, hidden, or modifiable based on user groups.)	M				
2.09	Provide capability to set Alerts, flag records for DNI or Terminations that are easily viewable by any user logging to the record. Restrict further actions based on business rules (e.g. alert the Trusted Agent if a person with DNI status applies for a badge within a predefined time with same or different company).	M				
2.1	Provide ability in the UI to override business rules on a case by case basis to certain user groups (e.g. ASC, Security Manager). (e.g. Law Enforcement applicant may not always be exempt from CHRC and STA, so ASC or designee should have ability to override the global rule from the UI for the particular applicant). Allow supervisor override feature for badge production.	M				
2.11	Allow field validations (e.g. name fields, date fields, zip codes, phone #s, SSN, DL#, Passports and ARN#). Allow selection of country, state where applicable.	M				
2.12	Provide ability to generate SSN's starting with 999-99 that is unique to the airport database for use by applicants that object to providing their own. IdMS shall allow badge application to be submitted without providing SSN or capability to override the SSN information for certain Federal and Law enforcement employees.	M				
2.13	Provide invalid or non conforming entries (e.g. red color) on the screen and prevent invalid or incomplete submissions.	M				
2.14	The IDMS shall have capability to alert the Trusted Agent using a hot note or a pop up window indicating critical information (e.g. open citation / violation, terminated for cause, expiring documents), when record is opened by Authorized Signatory or Trusted Agents	M				
2.15	The IdMS shall have existing data fields that can be customized for use by the airport. (e.g. open text field with capability to change labels, etc.)	O				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
3	**Business Rules**					
3.01	IdMS shall document and provide configuration of business rules driven by regulatory and operational requirements gathered by the IdMS vendor during the implementation phase as described in the Implementation approach section of the RFP.	M				
3.02	IdMS shall have capability to maintain separation of duties for Trusted Agents. The Trusted Agent user that processed the employee badge application and verified identification cannot issue the employee's badge. Other restrictions to enforce separation of duty may apply. Security Badging Office supervisors may override this restriction.	O				
3.03	The IdMS vendor shall configure business rules as per airport operational needs for - archiving background checks, archiving trainings, the data set (like photo, name, DoB) to be retained for certain DNI records, Rapback processing for new, renewal or replacement badge scenarios, returning applicants within airport decided timeframe 30 days, handling of lost, stolen, mutilated badges with requirement for police reports.	M				
3.04	No CHRC is required if it has been less than 30 days since their last badge expired or was deactivated in IdMS and fingerprints were previously taken by the Security Office staff. IdMS will apply the CHRC case number and training completion status to the new badge application.	M				
3.05	If it has been 30 days or more since the badge expired or was deactivated, IdMS will enforce Security Office staff policy and require CHRC, STA, and appropriate training.	M				
3.06	The ldMS vendors will produce generic work flows and work with airport to develop SOPs.	M				
4	**User Roles**					
4.01	The IdMS shall allow at a minimum the following user roles: Badging Office Trusted Agents, Badging Office Manager/ Superintendent, Airport Security Manager, Airport Security staff, Airport Operations staff, Airport Properties staff, Airport Engineering staff, Customs and Border Protection, Security Operations Center staff, other staff at the Airport and Port.	M				
4.02	Allow System Administrator the ability to assign roles such as a Trusted Agent or Airport Operations Control Center, to a pre-defined workgroup. When a new person is assigned to that workgroup the IdMS shall automatically receive all permissions associated with that workgroup definition.	M				
5	**Integrations**					
5.01	Integrate with a TSA certified DAC (the current DAC is the Telos ID) for processing of STA's and CHRC's, Rapback, CBP eBadge. Automate submission of applicant demographics and biometrics to the DAC and return of STA vetting results directly into individual records.	M				
5.02	Integrate with CyberLock System Version # 8.0.57	M				
5.03	Integrate with C•CURE 9000 v2.7	M				
5.04	Integration with the computer based training platform SSi.	M				
6	**Company Management**					
6.01	IdMS will provide capability for the Badging Office staff to pre-enroll a new company and provide at a minimum the following information including but not limited to company name, legal name, address, company representative (CR) / company contact person with name, email, and DoB and job title, start and end dates, contract information, contract start and end dates, sponsor contractor information.	M				
6.02	The IdMS shall check for duplicate company names. If the company name exists, the IdMS shall notify the ASC and Badging Office staff of a potential duplicate. At a minimum the "Doing Business as", FEIN / Tax ID, and the "abbreviated / badge printed" name for a company should be unique in the system.	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
6.03	Provide ability to capture multiple names such as - Business Legal name, Doing business as, abbreviated name to be printed on the badge. All these could differ from the company name used for billing. Also allow mechanism for capturing company name from the PACS for historical purposes.	M				
6.04	Provide ability to store multiple addresses, phone numbers and contacts for each company including roles and job titles. The IdMS should have capability to send notifications to company contacts listed (e.g. violation notifications and financial notifications).	M				
6.05	IdMS will provide capability for the Badging Office to scan and / or upload documents related to company enrollment. For example, company authorization letter, contract documents, insurance certificate, nominate first Authorized Signatory for the company, and others as required by the Airport.	M				
6.06	The IdMS will store all documents associated with the company and allow accessing historical documents from the company profile.	M				
6.07	The IdMS shall have capability to clearly indicate the sponsoring /primary company and sponsored (sub-contractor) company relationship. A company could have multiple companies sponsoring badges and similarly, one company could sponsor multiple companies.	M				
6.08	Subcontractor contract expiration date cannot exceed the contract expiration date of the primary company. If the subcontracting company already exists in IdMS and the new expiration date is greater than the existing expiration date, the expiration date for the subcontractor will be set to the new greater date.	M				
6.09	The IdMS shall allow tracking of the Company statuses, such as Pre-enrolled (pending approval), active, denied, suspended, terminated, inactive, and others as per the Airport business requirements.	M				
6.10	The IdMS shall have capability to add Reason for de-activation or add notes to company profile when the company status has changed from active to another status.	M				
6.11	The IdMS shall allow suspension of a company such that existing active badges will not be automatically de-activated when the status has changed, however will enforce any future processing of the company employees for badge printing or badge renewals. (Example case: company has financial payments due/ defaulted)	M				
6.12	The IdMS shall provide capability for the Badging Office to configure for the approved company the following but not limited to company types, badge and privilege types, financial and fee configurations, insurance requirements.	M				
6.13	The IdMS should allow categorizing companies with one of the Company Type (example: airline domestic or foreign, cargo, government, contractor, vendor, concessionaire). The IdMS shall allow system administrators to change or add company types.	M				
6.14	The IdMS shall allow configuration such that if a company is an airline (following TSR rules 1544) that conducts their own Criminal History Record Check (CHRC) background checks, IdMS shall require input of the applicant's CHRC case number. The IdMS shall have capability for AS to enter the case file number for 1544 carriers.	O				
6.15	Company configuration including: Security checks (e.g. CHRC, STA, CBP, Secure flight, other 3rd party checks) including capability to set exemption for CHRC or STA at the company level or division level.	M				
6.16	Company configuration including: Badge types allowed including privileges (e.g. driving, escort, CBP seals) for each badge type;	O				
6.17	Company configuration including: Financial configurations (e.g. monthly invoiced, no fee, pay-as-you-go by Individual, pay-as-you-go by Company) and Company specific badge and non-badge fee configurations with effective date.	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
6.18	Company configuration including: Number of I9 document requirements (for example: Government agency employees have to provide 1 form ID - PIV)	O				
6.19	The IdMS shall enforce that a Company in Active status should have at least one (1) active Authorized Signatory. There is no limit on the number of Authorized signatories that a company can designate. Use of global AS for 1st AS enrollment is acceptable.	M				
6.20	The IdMS shall have capability to allow the badging office to set an authorized signatory as Active or Inactive.	M				
6.21	Provide capability to set a quota for maximum number of active badges (of certain badge types or all badge types) that can be issued to a company. Notify and alert AS and the badging office (as a dashboard or queue report) if the limit is about to be reached.	M				
6.22	Provide capability to set maximum number of active badges with specific privilege (e.g. Customs Seal, Sterile Area access, movement or non-movement) for a company. (e.g. 25% concessionaire rule, or limiting driving privileges.) Notify and alert AS and the badging office (as a dashboard or queue report) if the limit is about to be reached.	M				
6.23	Provide capability to configure access levels / clearance codes with specific badge privilege, such as Customs Seal, Sterile Area access and movement or non-movement, for a company. (e.g. driving privilege for a company could limit access through certain vehicle gates.)	O				
6.24	Provide capability for Badging Office to configure default access levels / clearance codes for a approved company. The default access levels / clearance codes will be visible in the company profile.	O				
6.25	Provide capability for the Badging Office or system administrator to modify the default access levels / clearance codes per company business requirements.	M				
6.26	Company status should be easily and clearly visible in the company profile.	M				
6.27	The IdMS shall provide capability (as a dashboard or dynamic queue report) to clearly display in the company profile, if the company is reaching or reached badge quotas, is nearing (30 days ahead) company / contract end date, has no active AS, documents or insurance requirements have expired and other visual indicators as required by the Airport Badging Office.	M				
6.28	IdMS should provide capability within IdMS for ASC to bulk de-activate badges. Justification is mandatory when bulk de-activating badges.	M				
6.29	IdMS vendor shall recommend an approach to bulk re-activate badges. The IdMS vendor to provide a procedure to bulk re-activate badges.	M				
6.30	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 the company's insurance expiration date or contract term. A supervisor must be able to override this function if it is not applicable to the company.	M				
6.31	The IdMS shall notify the badging office if a company is set to expire. Once the company has reached the expiration date, no further processing of the records can take place. The badging office can then decide if all existing active badges need to be de-activated using the flag set per requirement above.	M				
6.32	The IdMS shall capability to manage driving privileges only if the company has valid certificate of insurance. If the insurance is expired or does not meet the insurance amounts required by the airport, then driving privileges cannot be assigned to the badge for that company.	M				
6.33	The IdMS shall provide functionality to change company names (e.g. legal name changes and badge printed names) including providing report of all badge holders impacted. Allow corporate name changes while retaining relation to the former corporate name.	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
6.34	The IdMS shall provide functionality to allow merger of companies (e.g. legal name changes and badge printed names) including providing report of all badge holders impacted.	M				
7	**Authorized Signatory**					
7.01	For the 1st Authorized Signer of the new company, the global signer (badging office supervisor or designee) will initiate the badge application.	M				
7.02	The IdMS shall at all times check and enforce the AS to maintain an active badge, valid security checks, valid AS trainings, in order to keep the AS active and maintain access to the AS portal.	M				
7.03	IdMS must assign each Authorized Signer a unique user account and password upon completion of the approval process and required training. This user account will be used for submission of employee badge applications and all other business activities performed using the web interface.	M				
7.04	IdMS shall provide and describe mechanisms to incorporate multi-factor authentication for the Authorizing Signatory Portal. The IdMS shall have the capability to implement OTP / authentication codes via text or email.	M				
7.05	The IdMS shall provide capability for the AS to perform at a minimum, the following functions for his / her company and any other company that the AS is assigned to: 1) Enroll new applicants, 2) Authorize renewal of badges, 3) Submit explicit badge replacement applications for lost, stolen, mutilated, name changes or privilege modification changes, 4) key request application (existing badge holder can request keys only), 5) Responds to badge audit, 6) upload supporting documentation for I-9, CBP forms, driving permits, key request form, and other documentation as necessary for the airport operations	M				
7.06	Provide the ability to send via email to a new badge applicant (mandatory field for all applicants), an expiring link to enter -applicant regulatory information and acknowledgements application information and attest to a disqualifying felony statement.	M				
7.07	The IdMS shall allow the badge application entered by the AS to be saved prior to submission. The application will be saved for 30 days or user defined timeframe prior to permanently deleting the application from IdMS.	M				
7.08	The IdMS shall permit the Authorized Signer to select the badge type, privileges, and change access level / clearance codes requests for a new badge application or for existing badges.	M				
7.09	The Authorized Signer must submit an application in IdMS for replacement of the lost or stolen badge. Changes to access levels and other fields are permitted if the employee's job role has changed.	M				
7.10	AS must request access levels / clearance codes at time of badge application. If there are multiple access levels available for a company then all options should be available and the AS will select appropriately for the badge applicant. A justification for employee access to secure areas, and the areas the employees must have access to, must be provided during application submission. If the AS does not select access levels then the default access levels for that company will be assigned.	M				
7.11	If the Authorized Signer indicated customs clearance is required on the application, IdMS will display instructions on how to obtain clearance through Customs and Border Protection (CBP). The IdMS will allow AS to upload the CBP forms 3078, letter of introduction and associated documentation.	M				
7.12	The IdMS shall allow AS to authorize renewal if the employee badge is due to expire within the next 30 days.	M				
7.13	The IdMS shall allow Authorized Signatories to modify certain employee information while restricting changes to Date Of Birth (DOB), SSN, Birth Country and other fields deemed to be critical to the STA process.	M				
7.14	Prevent Authorized Signatories from sending incomplete application forms through Authorized Signatory portal	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
8	**Applicant Portal for regulatory responses and acknowledgements**					
8.01	Provide capability for the applicant to electronically submit information related to Disqualifying crimes, Privacy Act, SSN, other airport specific legal language currently available in the badge application.	M				
8.02	IdMS shall provide capability for the applicant to electronically submit information as it relates to the badge type or company type. For example Federal and local government employees are not required to respond to Disqualifying crimes, Privacy Act, SSN. However they are required to respond/acknowledge airport specific legal language currently available in the badge application.	M				
8.03	Prevent Applicants from submitting incomplete application forms through Applicant portal.	M				
8.04	The applicant portal shall be mobile friendly such that the web portal aligns to various mobile screen sizes without limiting functionality.	M				
8.05	The IdMS shall have capability for a generic link/ website where the applicant can entered name, DoB, SSN and I9 document for identity verification and then respond to the regulatory information and acknowledgements.	M				
9	**Application Processing**					
9.01	The IdMS shall have capability to list all complete applications submitted by the AS. If the applicant portion of the application is not complete the badge application cannot be processed by the badging office.	M				
9.02	The IdMS shall have capability to clearly identify the type to application such as new badge application, renewal badge application, badge change (for adding or removing privilege - escort, CBP seal, driving privilege), replacement badge application (name change or lost, stolen or mutilated).	M				
9.03	The IdMS shall display all information entered by the AS in the application review process including biographic information, company type, company name, division, job title, badge type and badge privileges requested, supporting documentation if uploaded by the AS (I9 documents, driver permits, key request forms, CBP forms for eBadge) and disqualifying offenses responses and acknowledgments, case file or RAP back subscription numbers if entered by the AS and other information as per the current paper application.	M				
9.04	The IdMS shall allow the Trusted Agent to review and modify as necessary all the information submitted by the AS and the applicant. The Trusted agent can Accept or Reject or Cancel the badge application review step. IdMS shall send notification to AS if application is rejected or accepted.	M				
9.05	The IdMS shall allow the Trusted agent to enter reason for application rejection.	O				
9.06	Once the applications are rejected they will no longer appear in the application list for processing.	M				
9.07	The IdMS shall alert the Trusted agent if the badge applicant is existing person with DNI. The Trusted agent can then review and accept or reject the badge application. DNI can be due to STA adjudication, CHRC adjudication, citation or other ASC decided cause.	M				
9.08	The IdMS shall alert the Trusted agent if the new badge applicant already exists and allow the Trusted Agent to review the duplicate record and merge or process individually.	M				
9.09	IdMS shall have ability (specific field or notes field) for the Authorized Signatory during the badge application process (new/renew/replacement) to indicate if the applicant needs training translation assistance and translator (name and badgeholder).	M				
10	**Badge holder Management**					
10.01	IdMS shall capture and store all employee related information using secure methods for storage and maintenance of personal information.	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
10.02	IdMS shall flag the application for Security Office staff supervisor review if the employee had previously worked at the Airport and their badge was revoked or suspended as a result of citation or violation.	M				
10.03	IdMS shall permit the Badging office or Security Office staff to indicate the status of a badge as returned and destroyed, or lost or stolen.	M				
10.04	When an employee reports their badge as lost or stolen, the badge must immediately be deactivated in IdMS and the PACS.	M				
10.05	IdMS shall flag the application for Security Office staff supervisor review if the employee had previously worked at the airport and their badge was revoked or suspended as a result of an NOV or the adjudication eligibility date has not passed.	M				
10.06	The IdMS shall have capability to provide automated method to enroll badge holder in Rap back program upon submission of fingerprint to Telos and not wait for badge issuance. No CHRC is required if it has been less than 30 days since their last badge expired or was deactivated in IdMS AND not de-enrolled in Rap Back AND fingerprints were previously taken by the Security Office staff. IdMS will apply the CHRC case number and training completion status to the new badge application. Also, the IdMS shall have capability to remove badge holder from the Rap Back program after badge is not active (expired / terminated) for more than 30 days. Suspension of a badge will not trigger de-enrollment from Rap Back.	M				
10.07	Provide ability to issue multiple active badges to one individual working for multiple separate companies	M				
10.08	Provide the ability to issue a badge for each company an individual is employed with and segregate privileges to each individual badge. For example, a Customs Seal or driver authorization icon would only be allowed on the company badge it was approved for.	M				
10.09	The IdMS shall have capability for ASC or ASM to designate certain individuals as protected person (i.e. undercover law enforcement). These individuals will be exempt from security checks, fees and training. Only ASC or ASM or designee can access and modify records for these protected persons.	M				
10.10	Allow for badge applicant to be marked as exempt based on current SD and not undergo STA assessment (i.e. TSA, Law enforcement).	M				
11	**Photo capture requirements**					
11.01	IdMS must permit capture of identification photos with different industry standard formats, using digital cameras, and must be capable of exporting photo images to other systems (e.g. PACS).	M				
11.02	Provide for applicant photo capture, cropping, and digital enhancing from within the client application.	M				
11.03	Photo should be captured every time badge is printed (e.g. replacement, renewal)	M				
12	**Document Management**					
12.01	IdMS shall enable association of scanned documents with badge applications and functions in document management systems. IdMS must accommodate for all identification types shown on the Acceptable Documents List (List A, B & C).	M				
12.02	Provide ability to restrict viewing of scan and stored documents (e.g. Rap sheets) and mark private based on user roles by permission levels.	M				
12.03	Provide Security Office staff an input form for capturing identification document data with appropriate fields displayed based on the type of identification provided.	M				
12.04	Provide ability to scan, validate, and store breeder documents provided by applicants. Data retrieved from the documents should have the ability to auto-populate fields, reducing keying errors and saving time.	M				
12.05	Be able to rotate and zoom in to review scanned documents. The upload document formats will pdf or image files. Use of Adobe acrobat to rotate or zoom is acceptable for pdf files	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
12.06	Provide ability to alert the operator to mismatched data elements (e.g. name on document does not match demographic data previously captured for the applicant). Prevent operator from proceeding unless mismatched data elements are resolved.	M				
12.07	Provide ability to compare the data retrieved from the documents against the data entered by the AS or Applicant including ability to select data fields to merge or ignore.	M				
12.08	Provide the ability to archive electronic documents and badge records automatically on preset schedule following Port data retention policies.	M				
13	**Security Checks and Appeals Process**					
13.01	The IdMS shall have capability to send notifications to the AS (via email to the AS) if the applicant has failed one or both (STA and CHRC) security checks. The IdMS shall track date when the security checks status was changed. The IdMS shall allow the ASM or Badging Office to set Appeals flag if the Applicant has appealed the CHRC results within 30 days or configurable by the system administrator from the date CHRC results received. The IdMS shall limit any further processing of training, badge issuance or payment for the applicant.	M				
13.02	The IdMS shall track the date for the appeal review, interview and any additional documentation provided. The IdMS shall have capability to set the appeal result as Pass/ Fail, add notes and the date when the appeal process was complete. The IdMS shall limit the access to the appeals process and adjudication notes to ASM and Badging Office Superintendent user group.	M				
13.03	The IdMS shall have capability to report on the appeals process timing, number of individuals that appealed the CHRC, interview dates, notes added for each individual.	M				
14	**Keys**					
14.01	IdMS shall integrate with the existing CyberLock system.	M				
14.02	Assignment, Issuance and Tracking: Programming of new Cyber Keys will continue in the CyberLock system where system captures the name, badge #, key number, status, expiration date and other fields. The IdMS shall pull this information from the Cyber Lock system and associate the cyber key with the correct badge holder and make available from issuance.	O				
14.03	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.	M				
14.04	Cyber key de-activation: When a badge holder is terminated and no longer has an Active badge for the company that the Cyber Key is issued to, IdMS shall alert the Trusted Agent to collect the key and manually deactivate the key in CyberLock system.	M				
14.05	IdMS shall allow for various key statuses to be set manually based on business rules or manually set by IdMS user. (e.g. active, inactive, lost, stolen, damaged, returned, not returned)	M				
14.06	Assign keys to badge holders. Automatically require the return of the keys when a badge or credential expires.	M				
14.07	The IdMS shall allow entering key request details at the time of badge application. The IdMS shall allow requesting keys for active badge holders separate from the badge application process such as new badge application or renewal or replacement badge application.	M				
15	**Vehicle Permit Management**					
15.01	RAMP permits are assigned to a company (not a badgeholder). Automatically require the return of the ramp permit when a badge or credential expires.	O				
15.02	Allow the company to have multiple vehicles. (South field only)	O				
15.03	Restrict ramp permit issuance if insurance is expired or updated.	O				
15.04	Track the license plate number and state of the vehicle to which the permit was issued.	O				
15.05	Track the vehicle details (e.g. registration number, vehicle model, type, year, color, permit number issued).	O				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
15.06	Report list of all permits issued, active permits, expired permits, company names.	O				
16	**Financials**					
16.01	Allow for payment methods to be defined at individual company levels. (e.g. while one company might be authorized to receive a single invoice at the end of the month for all services rendered by the Security Badging Office, another company may be required to pay for each badge or credential or service with a check or credit card at the time the service is rendered or at the time the appointment is booked.)	M				
16.02	Provide the capability to manage and track the fees / charges associated with badges, background investigations, and other items issued in the Security Badging Office (e.g. keys, permits, card holders).	M				
16.03	IdMS shall be capable to generate reports that show (itemized or grouped) all of the financial transactions by badgeholder (name, badge #, date, amount, payment method, payment type, etc.) grouped by company over any period of time (a day, a week, a month, year-to-date, or since system inception).	M				
16.04	Support user-defined badge billing rate classes by company and badge type, taking into account CHRC exemptions, external adjudication, and federal employee allowances.	M				
16.05	Restrict the ability to invoice badges only if the company is set up as billable.	M				
16.06	Provide the capability to set customer billing rates for the following: Finger printing, 1st, 2nd, 3rd Lost Badge, Failure to report a lost, stolen or unaccounted badge, Unreturned Badge, south field permit, unreturned south field permit, and Citation / Penalty. The billing rate and types can be add / deleted / modified and put into effective by system administrators. IdMS vendor shall request from the airport and configure the latest ID badge fees.	M				
17	**DACS & Live Scan**					
17.01	The IdMS shall have capability to capture all the STA required fields during the badge application process.	M				
17.02	The IdMS shall integrate with the LiveScan fingerprint devices.	M				
17.03	The IdMS shall have capability to integrate with DAC and submit the data for STA and CHRC.	M				
17.04	The IdMS shall obtain change in status information from the DAC for CHRC and notify the Badging Office when the results are available on the FBI FPRD.	M				
17.05	Automatically retrieve results from the DAC and update / populate matched STA results to the existing badge holder database.	M				
17.06	The IdMS shall send notifications to AS and Applicant when security checks are complete, with instructions for next steps.	M				
17.07	The IdMS shall have the capability to provide an automated method to enroll badge holders in the Rap Back program upon submission of fingerprint to Telos and not wait for badge issuance. Also, the IdMS shall have capability to remove badge holder from the Rap Back program after badge is not active (expired / terminated) for more than 30 days. Suspension of a badge will not trigger de-enrollment from Rap back.	M				
17.08	The IdMS shall have capability to provide automated feedback from FBI of a Rap Back hit either directly from FBI or via the DAC interface.	O				
17.09	The IdMS shall provide immediate notification on dashboard and email notification to the system administrators, badging office and ASC if the connection to any DACS is lost.	M				
17.10	The IdMS shall provide capability to electronically submit the supporting documents to the DAC.	M				
17.11	The IdMS shall provide reports for reconciling badge holder records between DAC and IdMS.	M				
17.12	The IdMS shall provide reports for financial reconciliation of fingerprinting, STA, CHRC and Rapback, eBadge fees against the DAC financial reports.	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
17.13	Provide the functionality to limit the review of background check results to authorized personnel.	M				
18	**Customs and Border Protection (CBP) Seal**					
18.01	IdMS shall provide method for CBP interface (with eBadge via DAC) and ability to receive authorization for CBP Seal from the local CBP Office	M				
18.02	The IdMS shall have capability to create a separate CBP user with access to the IdMS. CBP users can set the seal request status and identify the Zone # directly in IdMS.	M				
18.03	The IdMS shall allow the AS to upload a CBP application from the AS portal as part of badge application process. IdMS shall allow CBP to review the CBP application (3078) via IdMS, provide a report for CBP to track pending application, reviewed (approved/denied) applications and the type of seal.	M				
18.04	Integration with Customs and Border Protection (CBP) Seals program / "e-badge" to the extent available within the DACS.	O				
18.05	If the CBP submission is possible via the DAC interface, the vendor will provide the submission of CBP Seal request via the DAC. Allow responses from CBP to be automated via the DAC.	M				
19	**Training**					
19.01	IdMS shall integrated with the existing computer based training system (SSi) to provision applicant records, training required based on the badge types and privileges requested and retrieve results (pass / fail), training language assistance if indicated in the badge application, training date and expiration dates automatically from the CBT .	M				
19.02	IdMS shall allow the manual entering of additional non-CBT courses (e.g. practical driving training and other part 139 trainings) by Airport Operations staff and track the name of the training coordinator, date completed and expiration dates.	M				
19.03	IdMS shall track the number of training attempts for specific training courses. IdMS will deny badge to applicants that do not pass after 3 attempts. Security Managers can override the condition.	M				
19.04	Provide ability to add / modify training and set expiration date of training.	M				
19.05	The IdMS shall have capability to restrict / control certain training courses. (e.g. Movement Area training is dependent on completing non-movement training.)	M				
19.07	IdMS shall have ability for the Authorized Signatory during the badge application process (new/renew/replacement) to indicate if the applicant needs training translation assistance and translator (name and badgeholder). The language should then coordinated with the SSi system.	M				
20	**PACS Integration**					
20.01	Update PACS with badge holder, badge and clearance codes data immediately (within operational acceptable timeframe). Update requests shall be queued for processing without delay.	M				
20.02	When an employee reports their badge as lost or stolen, the badge must immediately be deactivated in IdMS and the PACS.	M				
20.03	Allow system to automatically grant and revoke access privileges in PACS, based on attribute changes, additions and deletions.	M				
20.04	Provide notification if the connection to PACS is lost.	M				
20.05	Provide ability to display doors / gates access that is associated with a specific Clearance Codes.	M				
20.06	Provide ability to manage higher level of grouping / mapping of clearance codes based on job titles, privileges (e.g. movement area driving would allow assignment of vehicle gate clearance and emergency privilege mapping to all access).	M				
20.07	IdMS should have ability to read back changes made in the PACS made by Security Operations Control Center for badge statuses. (e.g. Lost, stolen, revoked other available in PACS). All other changes should be tracked and reported / notified via email to the ASC, Security Manager	M				
21	**Badge/Credential**					

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
21.01	Automatically calculate, and default the maximum expiration date for each new or reissued badge based on current airport policy, attributes of the badge and document, training, security checks expiration dates.	M				
21.02	The IdMS shall allow at a minimum the following badge statuses with capability for the system administrators to add / modify statuses and reason for de-activation: Active, Inactive, Suspended, Terminated, Revoked, Lost, Stolen, Damaged. The IdMS shall also provide drop down list for "Reason for De-activation"	M				
21.03	The IdMS shall clearly indicate on the UI if the badge was returned, badge returned date, badge printed date, badge pick-up date.	M				
21.04	Support automated reactivation of badges in PACS based on changes made in IdMS.	M				
21.05	Provide ability to limit status changes based on business rules (e.g. the system shall allow the System Administrator to configure badge statuses so that once a badge is stolen it can never be reactivated again).	M				
21.06	When the current date passes an assigned expiration date on a badge, automatically update the badge status to revoked with reason of expired and deactivate the badge in the PACS.	M				
21.07	Require a comment or a reason for de-activation if a badge is moved to any status except active and an explanation must be inserted in order to make the change / save the record.	M				
21.08	Easily indicate active badges versus returned and invalid badges.	M				
21.09	IdMS must support SEOS prox, ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693 and ISO/IEC 7501 smart-card technologies, and must also support the Federal Information Processing Standard 201 (FIPS-201).	O				
21.10	Manage Badge Issuance (printing and read back the encoded number) of multi technology cards (smartcard, prox) for different types of badge layouts (SIDA, AOA, Sterile, Cargo including encoding iClass, SEOS, MiFare, Desire, or Smart MX cards).	M				
22	**Badge Designer**					
22.01	The ldMS will provide a badge layout design tool for Airport badges. The card layout shall allow creation of single sided and double sided designs.	M				
22.02	IdMS shall permit system administrators to change the layout and design of Airport badge templates. The badge designer shall allow printing company name, division, company sponsoring name as required by the airport operations.	M				
22.03	Provide capability to easily add static and dynamic text data. The layout tool shall allow the addition of logos, graphics, images in various formats.	M				
23	**Badge printing**					
23.01	ldMS shall not be able to issue (print) badges until all applicable procedures (e.g. employment verification, I-9 Documents, CHRC/STA, and Training) have been successfully completed.	M				
23.02	IdMS shall provide capability to advance printing (e.g. company name changes, mergers or rebadges).	M				
23.03	Provide ability to pre-print badge when CHRC/STA are cleared or other wise approved, while applicant is undergoing training (e.g. driver practical training or CBP Seal request is pending). This can be done using supervisor override feature.	M				
23.04	Allow creation of new badges as replacements for unaccounted (e.g. lost, stolen) badges by copying previous badge details and establishing a new badge number.	M				
23.05	Notify the Trusted Agent of an individual whose previous badge(s) were not surrendered (e.g. lost, stolen, not returned, and otherwise unaccounted for). When a violation has occurred allow badge issuance after the fine is paid and / or the training has been completed.	M				
23.06	Allow capability to enforce capturing new photo each time a badge is printed (e.g. replaced or renewed).	O				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
23.07	IdMS shall prevent printing of a new badge until the old badge has been surrendered to the Security Office staff, unless the old badge was terminated as lost or stolen. In case of stolen badge, a certification box / acknowledgement from the applicant via touch screen or signature pad certifying that the previously issued badge is no longer in your possession and you are unaware of its whereabouts.	M				
23.08	IdMS should enforce reprinting of a badge if any elements of the badge appearance changes. (e.g. - name, company name, designations and other fields printed on the badge).	M				
23.09	Print a receipt and send notification to the badge holder and / or Authorized Signatory as proof the badge was issued or surrendered	M				
23.1	Provide capability of reprinting a badge with the same badge number and different credential number based on permission level (e.g. production error or production void). The badge number printed on the face of the badge remains constant for the individual for that company. The credential number (hot stamp) printed on the back of the badge by card manufacturer is programmed in C•CURE and used for access control. The credential number changes every time the card in printed.	M				
23.11	IdMS shall have the ability to add or change information (selected fields and privileges) on an existing badge without reprinting.	M				
24	**Access Level / Clearance Code**					
24.01	IdMS will provide a means to define and create templates or other methods of setting default clearance code / groups for employees of a company based on variables such as company name, company type, badge type, privileges, job title, department/division.	O				
24.02	Provide capability to auto assign clearance codes at a minimum based on job title, company name, company type, badge type. Allow manual override of the clearance codes (adding or deleting) by the Trusted Agent.	M				
24.03	Support an unlimited number of access levels per badge or credential type.	M				
24.04	Bulk access levels assignments and removals from badge holders	M				
24.05	Grouping of clearance codes and clearance groups	M				
24.06	Alerting incorrect clearance code assignments. (e.g. Southwest Airline employee cannot be issued American clearance code. Some clearance codes are defined by company name).	O				
24.07	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).	O				
25	**Audit (Operational and TSA)**					
25.01	IdMS shall comply and allow conducting badge audits as per the Security Directive (SD) 1542-04-08O (or subsequent updates) and revisions to TSA-NA-19-02.	M				
25.02	Audit should allow selection of records for Audit based on company, specific individuals and badge type.	M				
25.03	IdMS should generate the Badge status report in pdf format and notify as attachment to the ASC.	M				
25.04	IdMS shall allow generating list of random records to be audited. Allow the badging office staff to edit the list of records prior to activating the badge audit.	M				
26	**Watch List**					
26.01	Provide ability to create an airport "DNI" (allows the airport to add records to a list or mark as DNI so if an individual reapplies under another company or name (using same SSN) the flag would be identified.	M				
26.02	Utilize phonetic algorithms to form matches (e.g. "Andersen" sounds like "Anderson").	O				
26.03	Allow for reverse order of names to form matches (last_name = first_name AND first_name = last_name).	O				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
27.01	Scrub titles and honorifics from the source list (e.g. "Dr.," "Mrs.," "Ms.," "Mr.,").	O				
26.04	Allow the System Administrator the ability to edit the list of titles and honorifics.	O				
26.05	Provide a method for manager or authorized user to clear up any matches by entering notes in the Watch List.	M				
28.01	Flag a badge holders 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.	M				
26.06	Provide capability to check against the Watch List when an application is processed and each time it is changed.	M				
26.07	Report of Watch list, who entered, reason for the individual to be on the watch list (e.g. DNI, terminated for cause, citation, Rap back).	M				
27	**Citations / Violations**					
27.01	Allow users with appropriate permissions to add new types of violations.	M				
27.02	Allow an unlimited number of violation types to be added.	M				
27.03	The IdMS shall incorporate the existing paper citation tickets information including violation #, name, issuing officer, location, company, badge # and corrective actions like fine, badge suspension and trainings required.	M				
27.04	Track the payment status if a fine is imposed, and include the information in the appropriate financial reports.	M				
27.05	Manage a central record of employee's violations at the Airport.	M				
27.06	Record and track airport policy infractions in each identity profile (e.g. safety and security violations, no insurance).	M				
27.07	Record and track repeated infractions (including traffic violations), which may warrant re-training of the employee.	M				
27.08	Track the number of tickets, violations in each identity profile.	M				
27.09	Allow Port to determine if a badge should be suspended, but should not occur automatically unless defined by the System Administrator.	M				
27.10	Track penalties relating to a suspension.	M				
27.11	Track fulfillment of any necessary corrective actions (e.g. penalties, suspension, training).	M				
27.12	Track the payment status of a fine or ticket and automatically send email notification to Authorized Signatory.	M				
27.13	Provide ability to enforce business rules (e.g. to manage employee violations, suspensions, training).	M				
27.14	Provide ability to search existing or historical records (entered and **migrated** in IdMS) of infractions by multiple fields such as name, company, badge number, ticket number, and plate number.	M				
27.15	Provide ability to define and limit users access (e.g. data entry, read-only) to Violations/Citations tab.	M				
27.16	Send violation notices out via email automatically to the Authorized Signatory.	M				
28	**Dashboard Notifications**					
28.01	The IdMS shall provide a action oriented dashboard. The dashboard should list the pending tasks or actions for the Badging Office, AS and other users of the IdMS.	M				
28.02	The ldMS will provide a dashboard for Badging Office staff and the AS. The dashboard should be configurable for each user group and user.	M				
28.03	Provide on dashboard those STA and CHRC results that have not been returned in 10 business days.	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
28.04	At a minimum, following should be displayed on the dashboard: i) Badge holder badge applications in process indicating pre-enrolled, processing security checks, training status, CBP Seal request status, document expiration, badge expirations, audits pending. ii) The AS will see only those companies and badge holders he / she is responsible for. iii) ASM and ID Office will see a list all company applications submitted with all status, pending tasks, request review and review due dates, and all reviewing parties. iv) Upcoming badge expirations and badge renewals.	M				
28.05	Provide users with the ability to design dashboards illustrating high-level metrics (e.g. number of badges awaiting pickup, number of badges expiring within user defined timeframe), and providing the ability to drill down to the supporting detail.	M				
29	**Email Notifications**					
29.01	IdMS shall support the use of templates for emails to the Security Badging Office staff, companies, and Authorized Signers.	M				
29.02	Provide notification to the Authorized Signatory when a badge status changes within the Authorized Signatory's company.	M				
29.03	IdMS shall allow system administrators to add / modify wording within and database references for field values in the email templates.	M				
29.04	Provide ability to notify Airport or Badging Office and AS when a specified document in a record expires (e.g. driver's license, passport, authorization to work).	M				
29.05	Provide capability to send various notifications with reminders and escalations to the Authorized Signatory, Airport Badging, ASC.	M				
29.06	Notifications to AS, applicant and Badging Office for various statuses during badge application process (e.g. pre-enrollment, payment, fingerprinting, security checks complete, training complete (pass/fail), CBP Seals complete, badge issued, violations/citation issued); scheduling appointments (e.g. fingerprinting, document submissions, badge pickup, renewals, key and permit pick ups, training, badge applicant - No show to appointments, applicant failed to pickup badge within 30 days from the security checks completed).	M				
29.07	Notifications to AS, Applicant and Badging Office - Renewals: badge, training, CBP Seals, insurance certifications, contracts.	M				
29.08	Notifications to AS, Applicant and Badging Office - Expirations: badge, training, CBP Seals, documents, contracts, audit responses.	M				
29.09	Specific notifications to ASC: Terminations - badge, certain violations, company terminations, badge holder termination, automated STA or Rap Back hits, Trusted Agent is add or removed from the Badging Office group, changes to default access levels / clearance codes for companies or privileges, AS is no longer active, or company does not have a single active AS.	M				
30	**System Reports**					
31.01	Generate reports based on the status of matches (e.g. cleared, under investigation, actual match), and be capable of being exported into multiple formats (at a minimum .csv, .pdf and .xlsx formats).	M				
31.02	Provide pre-defined reports, in a variety of formats that allow the user to select or specify the grouping and / or sorting criteria.	M				
31.03	Easily generate ad-hoc reports or queries without specialized skills (most easily via filtering, sorting, grouping).	M				
31.04	Provide ability for a system user to create new reports as well as modify existing reports.	M				
31.05	Daily and monthly reports will be created, stored and managed within IdMS. Standard reporting tools, such as SQL Server Reporting Services or Crystal Reports must be supported.	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
31.06	Reports sent using email will follow Sensitive Security Information (SSI) and Personally Identifiable Information (PII) policies.	M				
31.07	IdMS shall allow formatting of the report (e.g. header, footer, page #s, Airport logo, report titles, column headers).	M				
31.08	IdMS should provide following reports at a minimum: · Company names and company types · Company Count Total Badges (e.g. Active, Terminated, Expired, Unaccounted - lost/stolen, returned) · List of Authorized Signatories with details (e.g. Active/inactive, email, phone) · 30 -45- 60 Day Pending Badge Expirations · Active Badge Report · Badge privileges Reports (e.g. Driver, CBP Seal, emergency) by Company · Security Checks reports by status (e.g. pending, submitted, results, DNI) · Rap Back report enrollment and de-enrolled · Security Checks reports STA pending for more than 14 days · Security Checks reports CHRC pending for more than 14 days · Customs Seal requested report by company and badge holder details · Customs Seal request result, date and expiration date by company and candleholder details · 30-day pending Customs seal expiration report · Badge Type report · Badge Expiration By Company & Date · Badges Issued per day, month, quarter	M				
31.09	· Stop list · Watch list · DNI list · Cardholder Record with photo, all companies, privileges, biographic data · Training reports - language preference, date taken, expiration date, results, · Training reports - practical training - administrator name, results, date taken, expiration date · 30 day pending Training expiration date · Keys reports - list of key assigned with cardholder name, badge status · Audit Report by Company · Audit Active Status Report for all the badge holders badge status when the Audit is initiated · Audit Closed Status Report for all the badge holder badge status when the Audit is closed · Audit AS closed Report of all the responses from the AS by Company after the Audit is closed · Audit Comparison Report of inaccuracy in the AS Audit AS closed report and the Audit Active status reports · Citation reports - open, active, closed, no action taken · IdMS User Activity Report · IdMS Audit report (all fields in IdMS old value, new value, date changed, user name	M				
32	**Hardware/ Software Integrations**					
32.01	LiveScan Fingerprint system (existing system - CrossMatch Guardian and Greenbit)	M				
32.02	Telos ID DAC - for execution of STAs, CHRCs and (if possible CBP background checks); bi-directional, real time with demographic data - (existing system)	M				
32.03	CyberLock system Version # 8.0.57 -(existing system)	M				
32.04	Physical Access Control System - C•CURE 9000 v2.8 -(existing system)	M				
32.05	Computer based training (CBT) platforms SSi - (existing system)	M				
32.06	Customs and Border Protection (eBadge Program) - for automation of Customs Seal applications	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
32.07	DL / Passport credential verification system- to import information extracted from breeder documents - (new supplied by vendor)	M				
32.08	SSN check via Telos DAC or other method (vendor to suggest)	O				
32.09	US Citizenship and Immigration Services (USCIS) Systematic Alien Verification for Entitlements (SAVE) web service - to verify immigration and naturalization status.	O				
32.10	FBI National Crime Information Center (NCIC) - to verify background check status	O				
32.11	TSA Watch List vetting of badge holders, badge applicants, and escorts – Secure Flight	O				
32.12	Capability for integration with Ccure for insider threat detection	O				
32.13	HID Fargo HDP 6600 or later (use existing system or suggest alternate); should allow 600DPI, laminate and internal reader to read the hot stamp badge# number back to IdMS.	M				
32.14	Touchscreen - (new supplied by vendor)	M				
32.15	Multi-page to single pdf file high speed document scanner (new supplied by vendor)	M				
32.16	External badge# reader and transmit badge number to IdMS - (new supplied by vendor)	M				
32.17	Port's Active Directory for single sign-on for Port's internal users (non-AS and non-Applicants)	M				
33	**Platform**					
33.01	Architecture (hardware/software/networking) is based on industry standard practices and non-proprietary tools. The IdMS will be tiered server architecture.	M				
33.02	Assume that Port will provide required storage, backup, server, workstation and network hardware.	M				
33.03	System shall run in a virtual environment and provide a highly flexible, redundant architecture for high availability, backups, and long-term scalability.	M				
33.04	The system minimum requirements for server & workstation - SQLServer 2014 or later database - Windows Server 20012/16 or later - Windows 10 or later workstations - Antivirus or later on all servers and workstations provided by the Port (Sophos and Avecto End Point Security) - Microsoft Office Product Suite	M				
33.05	Employs an industry-standard Structured Query Language (SQL) relational database management system.	M				
33.06	Utilize communication links between the tiers of the application, which shall be encrypted using at least Transport Layer Security (TLS) 1.2, using at least a Secure Hash Algorithm (SHA)-256 certificate.	M				
33.07	Utilize servers that are capable of working with current versions of industry standard Anti-Virus software.	M				
33.08	The Contractor shall identify and supply all hardware and software necessary to operate the IdMS except where provided by the airport.	M				
33.09	The Contractor shall provide system requirements including minimum server specifications, network and firewall specifications, database, storage, back-up server and other as needed to operate the IdMS.	M				
34	**System Network requirements**					
34.01	System shall reside on a Port provided segregated Ethernet network. Network configuration and security will be the responsibility of the Port in coordination with vendor system requirements.	M				
34.02	Vendor will coordinate IP addressing and routing with Port network communications staff.	M				
34.03	Provide all communication paths within the application and to external interfaces, and be documented by source Internet Protocol (IP), destination IP, and Transmission Control Protocol (TCP)/IP port.	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
34.04	IdMS shall function in a network and server environment that is compatible with IEEE TCP/IP and 802.3 Ethernet series standards and 802.11X Wireless standards, shall support industry standard network protocols and ports, shall operate within the current Airport and Port network architecture of local LANS and VLANS, and fiber backbones, and shall use and support industry standard network protocols and ports.	M				
34.05	The IdMS shall have capability to operate within a De-Militarized Zone (DMZ) with least common access rule base and any access to resources on the Internet (must be approved by Airport IT).	M				
34.06	IdMS must support the use of firewalls, intrusion detection systems, virtual private networks, virus protection, encryption, access controls, password expiration, identity management, and other technologies to ensure that IdMS complies with all TSA Security requirements.	M				
34.07	IdMS shall provide system level tools (or protocols) to support network intrusion and performance monitoring by Airport IT applications.	M				
35	**Security requirements**					
35.01	Integration between IdMS on secure Port network and systems connected via web services to external network (e.g. authorized signatory portal, Applicant portal, CBT, DAC) must be via secured protocol.	M				
35.02	Have the ability to encrypt sensitive and personally identifiable information at rest and in transit for internal as well as external users (AS and Applicant).	M				
35.03	The data should be encrypted using Transparent Data Encryption (TDE), when the selected Proposer's application database contains Personal Identification Information (PII).	M				
35.04	Provide the capability to mask all or specific Personal Identifiable Information (PII) (e.g. SSN) and non-PII (e.g. PIN) data fields for display after initial input. The masking will be based on business rules and allow the Airport to modify PII fields. The UI will clearly indicate if the data is missing.	M				
35.05	Interface to manage all secure user logins (e.g. Trusted Agents, Authorized Signatories).	M				
35.06	Shall have capability to enforce password policy at a minimum follow the NIST Special Publication 800-63-3: Digital Authentication Guidelines: 1) Disallow use of vendor supplied password defaults for system passwords 2) Prevent passwords that are derivatives of the username 3) Enforce password requirements of > = 8 characters and contains characters from 4 of the following 4 categories: Uppercase alphabetic (i.e., A-Z), Lowercase alphabetic (i.e., a-z), - Numeric (i.e., 0-9), Special characters (e.g.,. !%@*#^()_+|~) 4) Require user to change password after first login 5) Require user to reset password after a set period (90 days or Airport configurable)	M				
35.07	System provides automated means for user password resets with authentication	M				
35.08	Times out IdMS web or client sessions according to system administrator-configured period of idle time no longer than 30 minutes. The re-login should open the same screen / page where auto logout triggered. IdMS mist saves work prior to auto time-out.	M				
35.09	Limit browser-based modules to accept only HTTPS connections for authentication purposes.	M				
35.10	Prevent / Restrict storing of credit card data (e.g. number, expiration date, CSV#) in the IdMS.	M				
35.11	Undo /rollback feature that reverts badge back to the prior state and logs it. (e.g. a badge is accidentally terminated and the user can revert back to the prior state.) Feature is controlled by user access and all rollbacks are logged.	M				
35.12	Provide system security that is role-based allowing for update or read-only access to specific functions and obfuscation of defined data elements (e.g. SSN not visible or redacted on the screen for all users assigned to a specific role).	M				

OAK IdMS Specifications Requirements Compliance Matrix (RFP 21-22/33)

Airport Requirement			Vendor Response			
#	Description	Mandatory (M) Optional (O)	Compliant Out of the Box (O)	Compliant Custom Development (C)	Non-Compliant (NC)	Comments
35.13	Provide method(s) for the System Administrator to view and maintain user profiles such as: add new users, modify and delete user profiles.	M				
35.14	Provide details for any penetration testing, proprietary or 3rd-party, conducted by the vendor.	M				
35.15	Provide details of a data breach Recovery Plan, including liability matrix.	M				
35.16	As soon as security vulnerability is identified, the vendor shall be responsible to provide up-to-date IdMS application security patches and / or hot fixes as it relates to access to IdMS or data within 30 days of risk identified or security patch release.	M				
36	**System Audit**					
36.01	Automatic audit trail logging and generate report of all data sent to integrated systems (e.g. PACS, DAC, CBT), web calls, acknowledgement received from the integrated systems, status of messages - success / fail, error coding of failure.	M				
36.02	IdMS shall provide system integration audit report with error codes and actionable information to fix error.	M				
36.03	Automatic audit trail logging and generate report for data modified by any user - table, field, old value, new value, user ID, date/time	M				
36.04	Automatic audit trail logging and generate report for all queries and reports run (e.g. query/report name or SQL code, date/time, user).	M				
36.05	Automatic audit trail logging and generate report of all configuration updates made by any user (e.g. business rules, validation, required fields, lookup tables).	M				
37	**Data Migration - Data analysis, reconciliation and migrations**					
37.01	A data mapping exercise must be conducted to map existing fields in PACS and determine fields must be maintained in the IdMS.	M				
37.02	Data cleansing must be conducted prior to implementation for remediation of data issues. A review of existing badges must be completed for badge color and access consistency, data accuracy, missing data fields, and compliance. Manual and system automated cleansing may be used.	M				
37.03	The contractor shall perform data analysis and provide reconciliation reports across all data sources integrated in the IdMS including but not limited to PACS, DAC, training, violations and financial transaction details.	M				
37.04	The contractor shall provide reconciliation reports clearly identifying the data mismatches, duplicate records, missing and inconsistent data fields (e.g. DoB, SSN) and action plan for normalizing the data. The recommendations can include automated scripts to fix the data by the contractor, manual clean up missing information by Airport or other 3rd party system updates.	M				
37.05	The new Unique Person ID field must be generated for all existing employees during the data import to IdMS.	M				
37.06	The Unique Personal Identifier must be assigned to each existing badge holder during migration in IdMS and similarly provide plan to update other systems (e.g. PACS, DAC, CBT).	M				
37.07	The contractor shall perform data analysis and provide reconciliation reports in progressively and iterative method.	M				
37.08	Identify all data to be migrated into the IDMS in a transition plan, which shall include a data migration validation. The contract shall perform data migrations during every system acceptance testing iteration.	M				
37.09	The contract shall perform data migrations Dry-run test to validate assumptions for time taken to migrate data, perform quality check of the migrated data.	M				
37.10	Proposer shall include a back out plan for all data and processes in the event the go-live event does not execute as planned.	M				

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

Oakland International Airport IdMS Pricing Sheet

(Attachment 13)

Attachment 13: OAK IDMS Pricing Sheet

Please enter all information. Provide clarification where necessary

			Environments (License)		TOTAL	Implementation	3-Year Maintenance			Option 1 2-Year extension		Option 2 2-Year extension	
#	Item Description	Unit Price ($)	Testing & Training	Production	Quantity	Amount	Year 1 - Warranty	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
A	**Software licenses/ modules**												
1					0	$ -	Included						
2					0	$ -	Included						
3					0	$ -	Included						
4					0	$ -	Included						
5					0	$ -	Included						
6					0	$ -	Included						
7					0	$ -	Included						
8					0	$ -	Included						
9					0	$ -	Included						
10					0	$ -	Included						
15	*** Add lines as required				0	$ -	Included						
					TOTAL SOFTWARE COSTS (A')	$ -		$ -	$ -	$ -	$ -	$ -	$ -
B	**Professional Services / Labor**												
1	Professional Services				1	$ -	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	Custom Development Services				1	$ -	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	Training (including user manuals) Trusted Agents (3 sessions)				3	$ -	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	Training (including user manuals) System Admins (1 session)				1	$ -	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	Training (including user manuals) Authorized Signatories (5 sessions provided by the IdMS vendor)				5	$ -	N/A	N/A	N/A	N/A	N/A	N/A	N/A
					TOTAL LABOR COSTS (B')	$ -							
C	**Hardware - Badging Equipment**												
1	Camera		1	6	7	$ -							
2	DL+Passport Scanner		1	6	7	$ -							
3	Document Scanner (Multi-page)		1	6	7	$ -							
4	Badge Printer with laminate, provide consumables for 1-st 6 months - ribbons,		2	3	5	$ -							
5	Livescan system		2	6	8	$ -							
6	USB hub as required to connect all peripherals		1	6	7	$ -							
	*** Add lines as required					$ -							
					TOTAL EQUIPMENT COSTS (C')	$ -		$ -	$ -	$ -	$ -	$ -	$ -

Software licenses *(excluding Airport provided licenses for OS, SQL database etc.)*	$ -
Professional Services / Labor *(IdMS Contractor staff resources only, excluding costs for Port staff and Port consultants)*	$ -
Hardware - Badging Equipment *(excluding Airport provided equipment - servers and workstation)*	$ -
Total Implementation Cost:	$ -
Maintenance (Years 1, 2 & 3):	$ -
Option 1 maintenance (Years 4 & 5):	$ -
Option 2 maintenance (Years 6 & 7):	$ -

RFP No.: 21-22/33, Identity Management System at Oakland International Airport

Oakland International Airport
ID Badging Office Acceptable Document List

(Attachment 14)

PORT OF OAKLAND

OAK I-9 Document

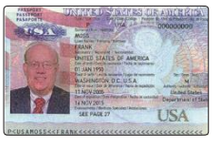
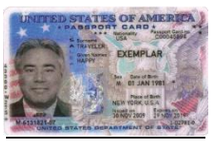
List of Acceptable Documents

All documents must be original and unexpired

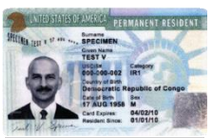
LIST A

Documents that Establish Both Identity and Employment Authorization*

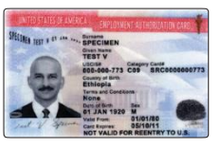
1. U.S. Passport or U.S. Passport Card.

2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551) or a foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa.


3. Employment Authorization Document that contains a photograph (Form I-766).




4. In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, as long as the period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitation identified on the form.

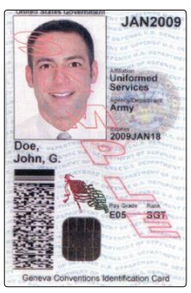
*Regardless if the identification in LIST A establishes identity and employment authorization applicants are required to present a second piece of identification from this form.

LIST B

Documents that Establish Identity

1. Driver license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address.

2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address.



NOTE:

The Aviation Security Manager or designee has the right to refuse acceptance of documents presented.

Port of Oakland Aviation Security
(510) 563-2895

LIST C

Documents that Establish Employment Authorization

1. Social Security Account Number card other than one that specifies on the face that the issuance of the card does not authorize employment in the United States.

2. Certification of Birth Abroad issued by the Department of State (Form DS-1350).

3. Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal.

4. Certificate of Naturalization.

I ✈ OAK

U.S. Born Citizen

Combination of Identification	LIST A	LIST B		LIST C	
	U.S. Passport	Driver License	Fed/State ID	Social Security Card	Birth Certificate
1	₱	₱			
2	₱		₱		
3	₱			₱	
4	₱				₱
5		₱		₱	
6		₱			₱
7			₱	₱	
8			₱		₱

U.S. Citizen Born Abroad

Combination of Identification	LIST A	LIST B		LIST C		
	U.S. Passport	Driver License	Fed/State ID	Social Security Card	Certificate of Birth Abroad	Naturalization Certificate
1	₱	₱				
2	₱		₱			
3	₱			₱		
4	₱					₱
5		₱			₱	
6		₱				₱
7			₱		₱	
8			₱			₱

Foreign Citizen

Combination of Identification	LIST A			LIST B		LIST C
	Permanent Resident Card	Employment Authorization	Visa + I-94 + Valid Foreign Passport	Driver License	Fed/State ID	Social Security Card
1	₱			₱		
2	₱				₱	
3	₱					₱
4		P		P		
5		P			P	
6		P				P
7			P	P		
8		✓	P	✓	P	
9		✓	P		✓	P