CITY OF PHOENIX

AVIATION DEPARTMENT

REQUEST FOR INFORMATION
AVN RFI 19-044 (NS)

ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEM(S) AT PHOENIX SKY HARBOR INTERNATIONAL AIRPORT

Nichol Shrum
Procurement Officer
2485 E. Buckeye Road
Phoenix, AZ 85034
602-273-4082
nichol.shrum@phoenix.gov

Please read before continuing to the offer document.

SOLICITATION RESPONSE CHECK LIST

Check off each of the following as the necessary action is completed.

- ☐ All Submittals are included.
- ☐ Included any required drawings or descriptive literature.
- ☐ Included the specified number of copies of the offer as indicated in Submittal section.
- ☐ Included signed addenda, if any.
- ☐ Addressed the mailing envelope to the Procurement Officer on the solicitation front page, at the address listed.
- ☐ The mailing envelope clearly shows your company name and address, the solicitation number, and the offer opening date.
- ☐ Mailed the response in time – City must receive offers no later than the date and time indicated in the Schedule of Events or addenda.

SECTION I – INSTRUCTIONS

The City of Phoenix Aviation Department ("City") is seeking information from qualified respondents who have experience with airport security systems that encompass access control, authorized access management and identity management. The purpose of this request is to obtain information about maintaining or replacing the Identity Management System ("IMS") and Access Control Systems ("ACS").

This Request for Information (RFI) is issued as a means of technical discovery and information gathering only. This RFI is for planning purposes only and should not be construed as a competitive solicitation nor should it be construed as an obligation on the part of the City to enter into any contracts or make any purchases. This RFI should not be construed as a means to pre-qualify vendors.

Participation in this RFI is voluntary. The City will not pay for the preparation of any information submitted by a respondent or for the City's use of that information. No purchases will be made as a result of this request. Any price information provided shall be used for comparison purposes only**.**

1. CITY'S VENDOR SELF-REGISTRATION AND NOTIFICATION

Vendors must be registered in the City's e-Procurement Self-Registration System at https://www.phoenix.gov/financesite/Pages/EProc-help.aspx in order to receive solicitation notices, respond to solicitations and access procurement information. The City may, at its sole discretion, reject any offer from an Offeror who has not registered in the City's e-Procurement system. The product category codes for this solicitation are 680020000 (Access Control and Identity Systems and Security Systems, 918280000 (Computer Hardware Consulting), 918290000 (Computer Software Consulting), and 918300000 (Computer Network Consulting).

2. SCHEDULE OF EVENTS:

ACTIVITY	DATE (All times are local Phoenix time)
Pre-Response Meeting	Friday, August 9, 2019 at 10:00 a.m.
Pre-Response Meeting Location	2485 E. Buckeye Road Phoenix, AZ 85034
Written Inquiries Due Date	**Friday, August 16, 2019 at 10:00 a.m.**
RFI Due Date	Friday, August 30, 2019 at 10:00 a.m.
RFI Submittal Location	2485 E. Buckeye Road Phoenix, AZ 85034

The City reserves the right to change dates and/or locations as necessary, and the City does not always hold a Pre-Offer Conference or Site visit.

3. OBTAINING A COPY OF THE SOLICITATION AND ADDENDA: Interested Respondents may download the complete solicitation and addenda from https://solicitations.phoenix.gov/. Internet access is available at all public libraries. Any interested respondents without internet access may obtain this solicitation by calling the Procurement Officer or picking up a copy during regular business hours at the City of Phoenix Aviation Department, 2485 E. Buckeye Road, Phoenix, AZ. It is the Respondent's responsibility to check the website and verify all required information is submitted with their offer.

4. SUBMISSION OF INFORMATION: Submittals shall be in the actual possession of the Contracts and Services Division on or prior to the exact time and date indicated in the Schedule of Events. Late submittals shall not be considered. The prevailing clock shall be the Aviation Department, reception desk clock.

Submittals shall be presented in a sealed envelope and the following information should be noted on the outside of the envelope/container:

Respondent's Name
Respondent's Address
RFI Number
RFI Title
Procurement Officer's Name

All submittals must be completed in ink or typewritten

5. **INQUIRIES:** All questions that arise relating to this solicitation should be directed via email to the Procurement Officer and must be received by the due date indicated in the Schedule of Events. The City will not consider questions received after the deadline.

   No informal contact initiated by Respondent's on the proposed service will be allowed with members of City's staff from date of distribution of this solicitation until after City Council award. All questions concerning, or issues related to this solicitation must be presented **in writing**. The Procurement Officer will answer written inquiries in an addendum and publish any addendums on the Procurement Website.

6. **WITHDRAWAL OF SUBMITTAL:** At any time prior to the RFI due date and time, a Respondent (or designated representative) may withdraw the submittal by submitting a request in writing and signed by a duly authorized representative. Facsimiles, telegraphic or mailgram withdrawals shall not be considered.

7. **LATE OFFERS:** Late Offers must be rejected, except for good cause. If a late Offer is submitted, the Aviation Department will document the date and time of the submittal of the late Offer, keep the Offer, and notify Offeror that its Offer was disqualified for being a late Offer.

8. **PUBLIC RECORD:** All documents submitted in response to this solicitation will become the property of the City and become a matter of public record available for review pursuant to Arizona State law. If a Respondent believes that a specific section of its response is confidential, the Respondent will isolate the pages marked confidential in a specific and clearly labeled section of its response. A Respondent may request specific information contained within its Offer is treated by the Procurement Officer as confidential provided the Respondent clearly labels the information "confidential." To the extent necessary for the evaluation process, information marked as "confidential" will not be treated as confidential. Once the procurement file becomes available for public inspection, the Procurement Officer will not make any information identified by the Respondent as "confidential" available to the public unless necessary to support the evaluation process or if specifically requested in accordance with applicable public records law. When a public records request for such information is received, the Procurement Officer will notify the Respondent in writing of any request to view any portion of its respondent marked "confidential." The Respondent will have the time set forth in the notice to obtain a court order enjoining such disclosure. If the Respondent does not provide the Procurement Officer with a court order enjoining release of the information during the designated time, the Procurement Officer will make the information requested available for inspection.

9. **RESPONDENT EXPERIENCE:** The City encourages interested parties with a record of accomplishment in Access Control and/or Identity Management System planning, development, support, operation and maintenance of similar size systems to respond to this RFI.

SECTION II – SCOPE OF WORK

1. INTRODUCTION

The City invites responses to this RFI from the Access Control and Identity Management industry through qualified firms experienced in comprehensive deployment and support of Access Control and Identity Management solutions in medium to large hub airports, in accordance with the provisions contained in the RFI. The City is seeking responses for the requested services for both Access Control and Identity Management or a solution specific to one or the other system. Response to this RFI is not limited to Access Control and/or Identity Management vendors or solution providers.

The City of Phoenix Aviation Department (City) owns and operates three airports; Sky Harbor International Airport (PHX), Deer Valley (DVT) and Goodyear (GYR). PHX served over 44 million passengers through three terminals in calendar year 2018, putting it among the 10 busiest airports in the United States. DVT is the busiest general aviation airport in the country and GYR is in one of the fastest growing cities in Arizona. Securing various areas of the airports is not only critical in the day to day operations but is also mandated by the federal government.

2. BACKGROUND

Our airports are mandated by the Transportation Security Administration (TSA) to validate identity to protect passengers, staff, aircraft, and airport property. Currently PHX has separate systems to manage their Access Control (ACS) and Identity Management System (IMS) requirements. PHX's access control restricts admittance to a physical area while the IMS issues the mechanism (badge), to gain access to those areas. Bi-directional communication occurs between the two systems: 1) Badges are created in the IMS and transmitted to ACS upon issuance. 2) When an access level is created and/or changed in the access control system, a system operator prompts the IMS system to request the changes from the ACS so that the new access level may be assigned by the IMS.

3. CURRENT ENVIRONMENT

The following information provides an overview of the existing hardware and systems currently utilized by the City.

3.1. IMS: There are over 1,000 IMS users and approximately 25K+ cardholders at the three airport locations.

Specifications of existing IMS:

- Software: HID SAFE V4.5
- Company: HID
- Integrations: Telos ID (DAC designated aviation channeling solution), CROSSMATCH (fingerprint scanning), Honeywell EBI (Enterprise Buildings Integrator), Mindflash (Learning Management system)

Functionality provided by existing IMS:

- Track identities
- Control access
- Issues access media
- Track TSA-mandated security checks
- Track training
- Track privileges
- Payment management
- Violation tracking
- Send notifications (emails)

- Auditing and Reporting features

Peripherals utilized by existing IMS for 10 workstations:

- 3M AT9000 Document ID Scanner with Assure ID software
- HID Badge printer
- CROSSMATCH Fingerprint scanner
- ELO Touch screen monitor
- Topaz Electronic signature pad
- RF IDeas Card reader
- VALcam 8500-630 photo camera

3.2. ACS: There are 100+ users and approximately 25K+ cardholders at the three airport locations.

Specifications of existing Access Control system:

- Software: (Honeywell Enterprise Buildings Integrator R500, video alarm monitoring software (Honeywell Digital Video Manager R600)
- Company: Honeywell
- Integrations: HID SAFE

Functionality provided by existing Access Control system:

- Access control with two factor authentications (doors, gates, etc.)
- Alarm monitoring
- Device status monitoring (escalators, elevators, AED, etc)
- Video monitoring and integration with alarms
- Covert alarm monitoring
- Reporting
- Visitor Management
- Time clock

Access Control hardware utilized:

- Client workstations – quantity 35
- Video cameras – quantity 600
- Covert alarm buttons
- Badge printers – quantity 12
- Servers (redundant application and video recording) – quantity 25
- Badge readers with keypads (Essex Electronics) – quantity 900
- Door locks and sensors – quantity 550+
- Access control units (Security Electronics Star II, PCSC Fault Tolerant) – quantity 150
- eLocks (Assa Abloy) – quantity 15
- Innovation Center – test environment
- Onsite / on-call technical support

4. PROJECT OVERVIEW

The purpose of this RFI is to obtain information about maintaining or replacing the IMS and Access Control systems at the three city owned airports to determine the direction and for an upcoming procurement. The current maintenance contracts are due to expire June 2023.

To reduce cost, risk, project time and duration, as well as migration efforts, the City requests respondents consider maximum re-use of current IMS and Access Control investments, where possible. Where vendors have an IMS or Access Control component or solution they believe is superior to an existing component or provides an advantage to our airports, they should explain why and how their proposed solution or solution component would better meet the goals and objectives in the City's initiative. Respondents are reminded, however, that it is the goal of the RFI to understand what IMS and Access Control vendors have to offer that will complement the existing environment, where possible, and replace only where needed and justified.

The objectives of this RFI are to obtain information regarding:

4.1. Option 1 - Support and maintain existing system(s)

Provide support and on-going maintenance of existing hardware and software for:

- Access Control System
- Identity Management System
- Both

This option explores the possibility of continuing with existing systems but leveraging service providers other than current providers for on-going maintenance and support.

4.2. Option 2 – A solution that integrates with existing hardware infrastructure

Keep existing hardware, replace software and provide support and maintenance for:

- Access Control System
- Identity Management System
- Both

This option explores the possibility of keeping existing hardware in both systems but replacing the software component(s) through a backend software solution provider.

4.3. Option 3 - Solution to replace some hardware/software

Retain existing hardware/software where possible and provide support and maintenance for:

- Access Control System
- Identity Management System
- Both

This option explores the possibility of retaining hardware and software of one or both systems where possible and replacing with new hardware and software where needed. This option could result in either continuing with existing maintenance and support provider after such changes or transition to new service providers.

4.4. Option 4 – Solution to replace all hardware/software

Replace all components and provide support and maintenance for:

- Access Control
- Identity Management
- Both

4.5. Other options in the industry

Possible solutions that have not already been discussed, for:

- Access Control
- Identity Management
- Both

5. DESIRED FUNCTIONALITY

PHX wants the Identity Management System to provide/allow for:

- A single point of information entry for authorized users and signatory authorities
- The ability to modify requested badge types, assess fees, and access privileges for designated functions/work areas
- The ability to input biographic information and attach supporting documents
- Paperless signatures and paperless applications
- Integration with TSA approved Designated Aviation Channeling (DAC) for TSA/STA vetting, FBI CHRC profile evaluation
- Integration with Security training capabilities (Learning Management System)
- Access to credentialing inputs (photos, eventual hologram implementation)
- Physical access control management (door access profiles)
- Asset management/tracking (perimeter keys, cypher codes)
- Infraction management (fines, notices, retraining)
- Financial management (billing, refunding)
- Audit capabilities
- Dashboard capabilities (analytics /trend analysis); and
- Incorporating existing data
- Ability to run on virtual server infrastructure
- The ability to use existing peripherals where applicable
- Electronic Communication/Notification (mass emails, status change and renewal emails to badge holder and authorized signer)
- Calculation of expiration
- Do Not Issue
- Reporting functions
- Insurance tracking
- Sponsoring other companies (letters of verification)
- No size limitations on uploading or scanning documents

PHX wants the Access Control system to provide/allow for:

- Physical access control of doors, gates and elevators with multi-factor authentication (badge/pin, biometrics, etc)
- Alarm monitoring (able to monitor alarm events from multiple locations)
- Device status monitoring (escalators, moving walk-ways, AEDs, etc)
- Real time alarm event video display (video monitoring)
- Integration with wireless covert alarm systems
- Ability to analyze and report on historical event data for three previous years
- Ability to run on virtual server infrastructure
- Server/system redundancy
- Temporary/visitor badge creation and tracking (Visitor Management)
- System operability in off-line mode (power and network failure)
- Ability to configure base and extended door-open times

- Interoperability with other systems via open architecture
- Ability to support a variety of hardware including door locks, card readers and video cameras

SECTION III: RESPONSE REQUIREMENTS

1. COMPANY BACKGROUND AND EXPERIENCE

Respondent to provide history of the company, including the date established, the type of ownership and the length of time that the business has been operating. Please discuss the area of expertise and list the following:

A. Describe your experience as it relates to Access Control and/or Identity Management systems. List similar project that you have previously worked on. Provide detailed information (i.e. when, where, with whom, number of users, scope, your role, etc.).

B. What is your experience working with biometrics-based solutions as it relates to Identity Management and/or Access Control?

C. Based on your experience, provide information regarding best strategies, practices for customer preparedness, common mistakes and/or lessons learned (i.e. unplanned costs or delays, etc.) when acquiring a new Identity Management and/or Access Control solution.

D. Based on your experience, provide information on Access Control and Identity Management solution providers with national or international presence. Offer examples where such systems are supported by vendors with local engineering, product development, and technical support as well as where such functions are based outside of the United State. In your opinion, which model is best for an airport and explain why?

2. System Information

Based on the options listed in Project Overview, which option do you recommend and provide an explanation.

Respond to the following for each option recommended:

A. How do you propose to implement? What is your recommended system architecture?

B. What are the benefits?

C. Describe any potential risks with this approach.

D. What is the estimated implementation time?

E. How will you implement and integrate with the existing system, if applicable?

F. Describe the most advantageous integration architecture between Access Control and/or Identity Management. What are the benefits such integration architecture provides?

G. What additional capabilities would a new system provide to the airport?

H. Would the proposed system use on-premises virtual servers or cloud-based systems? What are the benefits and risks associated with each?

I. Provide a Rough Order Magnitude (ROM) for your recommended solution:

   a. One-time implementation costs for software and hardware

   b. On-going annual maintenance and support costs for hardware

   c. On-going annual maintenance and support costs for software

   d. Projected increases over the life of the contract, including allowances for system growth

J. Describe any self-service options with your recommendation.

K. Based on your experience, what are the post implementation staffing requirements for your recommendation?

L. Explain the possible migration path to use any of the existing field devices, peripherals, etc.

M. What are your plans to have a local presence and/or technical support?

N. Include any additional information not already provided that will be helpful to the City in determination of the best option and architecture for the on-going operation of the two systems.

3. Access Control and Identity Management General Information

In addition to written responses to this RFI, is there any additional information you can provide in response to information gathering or market research (i.e. product brochures, marketing materials, technical manuals or diagrams, etc.)?

SECTION IV – SUBMITTALS

1. **COPIES:** Please submit one (1) original, six (6) copies, and one (1) electronic copy (CD or portable drive) of RFI response. RFI response must include the name of the organization, contact name, title, address, direct phone number and email address of the person who is authorized to respond to questions regarding the submittal.

The City shall not be responsible for any costs associated with preparing or responding to this RFI.

Please submit only the Submittal Section and all other required documentation, do not submit a copy of the entire solicitation document.

2. **SUBMITTAL FORMAT:** Respondent shall organize and submit their response (printed and electronic) in the following tabbed order with a 12-point font.

Submittals should be:

- Typewritten;
- Submitted in a binder, preferably using double-sided copying;
- Submitted with a one-page cover letter prepared on the company's letterhead and signed by an authorized employee of the company. Provide a brief summary in the cover letter that provides the company's expertise as relates to this RFI.
- Submitted with a table of contents and tabbed accordingly reflecting the information requested in the corresponding section of this RFI and organized in the same manner:
    - **Tab 1 Company Background and Experience**
    - **Tab 2 System Information**
    - **Tab 3 Access Control and Identity Management General Information**
    - **Tab 4 Signed Addenda, if applicable**