CITY OF SAN ANTONIO

INFORMATION TECHNOLOGY SERVICES DEPARTMENT
& SAN ANTONIO POLICE DEPARTMENT

REQUEST FOR COMPETITIVE SEALED PROPOSAL
("RFCSP")

for

SAPD Body Worn Camera Technology Solution

RFCSP 6100005871, v3
LOG 2015-048
Release Date: April 6, 2015
Proposals Due: April 27, 2015

This solicitation has been identified as High-Profile.

Notice Regarding Prohibition on Campaign or Officeholder Contributions for Individuals and Entities Seeking High-Profile Contracts. Under Section 2-309 of the Municipal Campaign Finance Code, the following are prohibited from making a campaign or officeholder contribution to any member of City Council, candidate for City Council or political action committee that contributes to City Council elections from the 10th business day after a contract solicitation has been released until 30 calendar days after the contract has been awarded ("black out" period):

1 legal signatory of a high-profile contract;
2 any individual seeking a high-profile contract;
3 any owner or officer of an entity seeking a high-profile contract;
4 the spouse of any of these individuals;
5 any attorney, lobbyist or consultant retained to assist in seeking contract.

A high-profile contract cannot be awarded to the individual or entity if a prohibited contribution has been made by any of these individuals during the "black out" period.

002 TABLE OF CONTENTS

003 BACKGROUND

The San Antonio Police Department (SAPD) currently has COBAN mobile video and voice recording equipment installed in marked patrol vehicles. This equipment has the capability to gather video evidence as a recording of officer and citizen interaction from the perspective of the patrol vehicle. SAPD records approximately 1.5 terabytes of video evidence daily, resulting in an average of 2.5 hours of footage with 3 gigabytes of storage required per officer, per day.

Body worn cameras are a relatively new development in policing and the subject of significant discussion in the law enforcement and civil liberties communities. Current events across the nation have brought this issue to the forefront.

SAPD initiated a body camera feasibility test in March of 2014. During the test, six different models of body worn cameras were evaluated based on studies conducted by the:

- ***U.S. Department of Justice, Office of Justice Programs, National Institute for Justice, Body-Worn Cameras for Criminal Justice: Market Survey, March 2014***
- ***National Institute of Justice, Police Officer Body-Worn Cameras, Assessing The Evidence*, *2014***
- ***Department of Homeland Security (DHS) March 2012 System Assessment and Validation For Emergency Responds (SAVER) report***

Each vendor provided 25 models for testing and the equipment was issued to officers from the Downtown Bike Unit and the Westside Patrol Substation. The pilot was designed to gather data on the technology's effects on citizen and police behavior/accountability, evidentiary value, operation feasibility, program costs, compatibility with COBAN, and other factors.

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

004 SCOPE OF SERVICE

The City of San Antonio is requesting proposals for the purchase, implementation and support of wearable body cameras for the SAPD. No existing Body Worn Camera Systems are currently in use for SAPD. Body Worn Cameras will allow SAPD officers to video and audio record their daily activities while on duty, and for the recordings to be preserved and accessed by designated personnel in the SAPD. Body Worn Cameras will enhance the Department's ability to accurately capture events as they occur. The goal of the system is to provide for Officer's safety and to increase transparency with citizens.

SAPD is requesting a proposal to immediately implement **251** new Body Worn Cameras. Initial deployment will be to the Downtown Bike Patrol Unit (72 body cameras) and the Parks Police (179 body cameras). These Units have been selected since they currently do not have video support. The Downtown Bike Patrol does not utilize patrol vehicles and thus does not have access to the Coban in-car system. The Parks Police have not been issued Coban in-car systems, and a majority of their operations are on foot, ATV or bicycle. In addition, the City does not issue cellular devices to officers. Deployment of 2200 cameras to all patrol units is expected to be implemented over a 5 year period, contingent on funding availability.

Self-contained cameras will be worn on the outside of the Officer's uniform. Body Worn Cameras must utilize a backend IP based retrieval system available to multiple users. The Respondent will provide a warranty for the equipment. Applicable maintenance, upgrades and repair services must be fully described including estimated frequency thereof, and detailed pricing. Respondents may submit alternative approaches if they believe their proposed system will meet or exceed the capabilities described below.

SAPD desires to implement a best-practice process and solution that meets the business and technical requirements included within this document and corresponding attachments. The scope of work includes hardware and software with storage options.

The equipment supplied must be of new manufacture (not used or demo units), best quality, and installed in accordance with approved recommendations of the manufacturer thereof, and must conform to the equipment specifications listed in this RFCSP.

Services will include:

Camera

The body worn camera should:

1. Meet Military specifications (MIL-STD-810G) or equivalent for the following:
    a. Storage Temperature Range
    b. Vibration
    c. Thermal Shock
    d. Dust
    e. Solar Radiation
2. Provide operating temperature range specifications.
3. Drop Test rating of 6 ft
4. Be water-resistant to IPX Rating 4
5. Have flexible mounting options on the officer's uniform with a forward facing field of view:
    a. Chest
    b. Lapel
    c. Point of view/head
    d. Windshield Mount (Optional)
6. Have Video Recording Definition of 640x480 (30FPS)
7. Have Date and Time Stamp on video file
    a. Be capable of recording the devices geolocation via GPS locator
8. Be able to record at least 4 hours uninterrupted of continuous recording.
9. Be able to store a total of 8 hours of video
    a. Have 64GB preferred of internal memory. Enhancement.
10. Have a battery life of at least 12 hours.
11. Be able to synchronize time to an external time service.

12. Have industry standard security in place equal or greater than CJIS standards version 5.3 or later and policy standard dated 8/4/14 for minimum camera design.
13. Have color video.
14. Have a minimum field of view of 68 degrees.
15. Be compatible with Windows 7.
16. Have USB cable computer connectivity.
17. Have a noise canceling internal microphone.
18. Have a one touch recording activation button.
    a. Have Mute Functionality
    b. Have Play Functionality
    c. Have Resume Functionality
19. Have audio or visual or vibrating alert to confirm when it is turned off and on.
20. Have safeguards to prevent accidentally turning it on or off.
21. Have enhanced image quality and low-light capability to mirror the human eye.
22. Have the ability to be activated automatically via Department defined cue (overhead lights, vehicle door opening, etc.).
23. Allow for video categorization in the field.
24. Each Body Worn Camera Unit must have its own unique ID that can be registered to a specific Officer (i.e. by badge number, etc.)

System

The system should:

1. Capable of handling over 2000 user/Officer accounts
2. Must be able to create individual user accounts with varying degrees of access
    i. Administrator accounts
    ii. Basic user accounts
3. Record at a minimum HE-AAC (High-Efficiency Advance Audio Coding) Audio Format or MP3.
4. Allow officer to initiate video file transfer.
5. Allow officer to upload through docked video transfer via auto-upload to secured evidence database.
    a. Allow officer to upload through wireless video transfer via auto-upload to secured evidence database. Enhancement
6. Be able to integrate with Active Directory.
7. Be capable of categorizing a call for service or field activity categories.
8. Be customizable to allow for the minimum number of days that a recording shall be retained in the system.
9. Have capability of at least 15 seconds of Pre-Event video buffering.
10. Self-contained memory that cannot be modified or altered upon view.
    a. Have solid-state memory Enhancement
11. Have access control that requires security permission for viewing and copying a video file.
12. Provide safeguards to ensure that the camera cannot record over or delete video files.
13. Be able to burn expired videos or copies being requested to DVD and/or other means of export.
14. Be a secure and tamper-proof device.
15. Have standard software allowing for an officer to enter additional information to an existing video recording.
16. Have industry standard security in place equal or greater than CJIS standards version 5.3 or later and policy standard dated 8/4/14 for minimum camera design.
17. Ensure an unalterable chain-of-custody that records all access and activity of the system and video.
18. Be customizable to allow for Department retention schedules.
19. Have import, export, share, and record etc. functions for supervisory users to manage and share digital evidence.
20. Include video editing software that will: Enhancement not mandatory.
    a. Redact digital media.
    b. Render segments of digital media.
    c. Create event timelines and flags in digital media.
    d. Redact documents (similar to PDF Professional editor).
21. Provide a minimum of 2x or double redundancy for all stored digital media and associated entries.

Backend System

Backend System should be capable of:

1. Automatic Video transfers from Body Worn Camera Unit into Local On-Site Storage Solution and/or Vendor Hosted Cloud Storage Solution.
2. Automatic Video transfers must be performed via multi-charging/docking stations and/or USB cable via individual desktop computer.
    a. Be RJ45 Ethernet connection.
    b. USB/Multi-docking station software must have throttle control capability when connected to network so as to not overload network pipe and allow for seamless upload and charging of captured media and battery.
    c. Minimum 256bit AES Encryption in storage and transport.
3. Video Playback Backend System.
    a. Fast Forward and Rewind.
    b. Fast Forward and Rewind Slow.
    c. Advance forward and backward frame by frame.
    d. Must have Video Screen Capture capability.
    e. Must have Desktop Player compatibility with Windows Media Player, Quick Time, and VLC media player.
    f. Must have the ability to digitally enhance a captured image/video without altering the original.
4. For On-Site Backend System should have a recommended Disaster Recovery or Failover strategy that allows for periodic testing and validation.
5. Video and audio to record and export in a standard, open, non-proprietary format, including both Codec and Container, such that it can be replayed in freely available software (e.g. VLC player) without processing conversion.
6. Source code and encryption information to be held in escrow

Storage Options

Storage options should include but not be limited to the following recommendations:

1. Data network infrastructure for the uploading and retrieval of video data.
2. Cloud and/or Local server storage arrays and back-up storage solutions.
3. Original captured media file must not be able to be deleted or altered upon capture and upload to Local Server Storage/Hosted Cloud Storage.

Proposed Storage Option should:

1. Include management software allowing the Department to digitally manage all uploaded evidence.
2. Include scalable storage for users to upload and download.
3. Allow for the sole ownership of digital media and associated entries to reside with the Department.
4. Cloud or Vendor hosted storage solutions should include means for COSA to recover digital media and associated entries in a non-proprietary format. Upon termination or end of the contract
5. On-Site Storage solutions shall provide a means to export digital media and associated entries in a non-proprietary format upon termination or end of the contract

Training

Respondent should:

1. Be prepared to offer ongoing training support for their product upon the procurement of new units for Department
2. Ensure training is an appropriate blend of classroom instruction and hands-on practical training with the equipment to be used
3. Ensure course content include the theory of device; the technical knowledge required for backend software operations and actual deployment
4. Supply all technical training materials and handouts in sufficient quantities to cover the training of identified persons.
5. Provide the training at a City facility
6. Provide Department defined, on-site user training, system migration and system installation.
7. Provide a minimum of 4 hours per officer training class.
8. Provided training to officers in such a manner that officers are competent in operating the recording device and backend systems.

9. For On-Site solutions provide training to System and Application Administrators in the management and maintenance of the backend systems
10. Provide evidence that the officer has completed training and is competent in operating the recording device and backend systems shall be maintained and turned over to the Department once completed.
11. Included in the training the Department Standard Operating Procedure (SOP) and Body camera policies for recording
12. Ensure 100 percent of the Department's users have been trained.

Personnel Assignments And Access

All Respondent's, subcontractor, and other personnel assigned by the Respondent to the San Antonio Police Body Worn Camera Project shall be apprised of and must acknowledge their responsibilities with respect to the confidentiality of Police District and Headquarter installations, capabilities, work processes and data.

The Respondent's staff assignments shall be subject to the San Antonio Police Department review and approval.

The San Antonio Police Department reserve the right to approve all personnel assigned to the project and to explicitly authorize participation and facilities access for each assigned individual.

The San Antonio Police Department reserve the right to unilaterally request the replacement of any individual assigned to the project, and the Respondent must accomplish the replacement with a person of appropriate qualification for the assigned position in a timely manner.

All Respondent employees, subcontractors and other personnel requiring access to the San Antonio Police facilities maybe fingerprinted and subjected to a fingerprint-based background check conducted by the San Antonio Police Department.

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

004.1 BUSINESS REQUIREMENTS

A. Requirements

1. The solution must comply with the Detailed Business Requirements as outlined in “RFCSP Body Worn Cameras – Attachment G – Detailed Business Requirements”.
2. The solution must comply with the Information Technology Environment Description Standards.
3. The proposal must include cost proposal information.
4. The solution must be accessible to the user 24/7 via on-site or remotely, with or without internet access.
5. The solution must include Active Directory Synchronization log-in functionality.

B. Off-Premise vs. On-Premise Solution Costs

Provide costs estimates and options for off-premise and on-premise solutions.

Off-Premise Solution - If Vendor off-premise solution, in which users log on to the vendor's website, provide detailed breakdown of fee schedule (monthly charges, yearly charges, extra charges, etc.) in Price Schedule, RFCSP Body Worn Cameras – Attachment F.

On-Premise Solution - If CoSA on-premise solution, in which CoSA purchases the software and the solution runs on CoSA hardware servers, provide detailed breakdown of recommended server size and storage requirements based on historical data. Provide a list of all software involved and extent of license rights as requested in RFCSP Body Worn Cameras – Attachment F.

The CoSA prefers broad license rights for all software and other technology, including perpetual, fully-paid and royalty free use rights for commercial off the shelf (COTS) software. CoSA also strongly prefers ownership of all custom software and interfaces. CoSA will require a source code escrow agreement where applicable.

C. Maintenance and Support

Respondent must provide a plan for post- implementation maintenance and ongoing support of the Body Worn Camera System and related equipment, including but not limited to: Body Worn Camera Unit, USB/Docking Station unit, servers, storage arrays, and back-up storage solution.

The plan should include details related to:

1. Delivery method for future upgrades and product enhancements, including frequency of upgrades.
2. Problem reporting and resolution procedures.
3. Thresholds for support limitations.
5. Bug fixes and patches.
6. Performance tunings and incremental enhancement.
7. On-site and on-line support.

The plan should also address details to:

1. Provide the Department a 10 percent rolling stock for immediate replacement of inoperable units.
2. Provide telephone support (include toll-free support, hours of operation, availability of - at a minimum – 24X7 hotline, etc.).
3. Respond to all service calls within 24 hours.
4. Provide a replacement if a Body Worn Camera Unit and/or USB/Docking Station Unit or associated equipment become inoperative within 72 hours from the date that the equipment is deemed inoperable.

D. Replacement Plans

Respondent must propose and supply a current and supported product and certify that it is not at end of life cycle. Should equipment or technological upgrades become available during the course of the contract, the Respondent must provide the City the upgrade to their equipment as a replacement to the contracted product. Only equipment and/or product models that have been satisfactorily demonstrated to the City and that have a demonstrated record of successful deployment by other law enforcement agencies, in similar sized cities will be used.

The Replacement plan must include details related to:

1. Replacement cycle of the entire system, including but not limited to:
    a. Body worn camera.
    b. Body worn camera accessories.
    c. System associated accessories.
    d. System docking stations.
    e. System software and associated software.

E. Service Levels

Respondents must state their Service Level Agreements (SLAs) in the following areas (add any other SLAs included with your offering):

1. Site Availability (uptime with full functionality outside scheduled maintenance periods).
2. Maximum Scheduled Downtime (e.g. scheduled maintenance outages must not exceed 6 hours per quarter, and must not exceed 24 hours per year).
3. Video Retrieval Time must be 5 seconds or less, 99.5% of the time.
4. Support Request Acknowledgement Time (time to acknowledge receipt of a support request).
5. Support Request Mean Time to Resolution.

F. Third Party Products I Options Software

The Respondent must explicitly state the name of any third party products that Respondent would be providing, as part of the proposed solution. Respondent must possess and demonstrate upon request that it has authorization to transfer any rights of use and warranties for third-party products to CoSA. The Respondent will be responsible for interacting with third party product providers, on all third-party warranty claims. The chosen Respondent will ultimately be responsible for providing all services, rights of use, service levels and warranties on both components and the System as a whole regardless of whether subcontractors perform certain services or provide certain technologies.

G. Expansion

In the future, CoSA may choose to expand, by amendment or other procurement process, the use of the Body Worn Camera solution to within the agency or among other public safety agencies. Scaling this system could include the development of additional agency specific forms. While CoSA is not seeking a proposal or cost schedules for additional licenses from the Respondent, the City requires that respondents include a discussion of the scalability of their system to gain an understanding of what would be required to expand the infrastructure to incorporate a larger system across multiple agencies. The scalability of the System is therefore important to CoSA and will be evaluated, as criteria for vendor selection.

004.2 TESTING

A testing period may be performed on the devices that meet the minimum specifications and are identified after the initial evaluation of the Respondent's proposed plan.

During the testing period, the San Antonio Police Department will evaluate each camera to assess in a static and fluid environment based on the following:

a. Ease of Camera Use
b. Camera Functionality
c. Camera Sturdiness
d. Video Download Capability
e. Ease of Storage System

f. Data Distribution Capability
g. Account Administration/Storage Rights

Successful Respondents who pass the Business Requirements evaluation criteria will be required to attend an assigned testing date and will provide training to police officers who will test that proposer's camera.

Successful Respondents will be required to provide the following information prior to the testing date:

a. Each Respondent must identify network connectivity/docking requirements and preparation/delivery of equipment.
b. Each Respondent will indicate any pre set-up requirements needed from City staff or equipment required for training.

A. On the assigned training day, each proposer will provide five working test units and training at no cost to the City.
B. All units undergoing testing will be returned to the proposer at the proposer's expense following the testing and grading of the units.

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

005 ADDITIONAL REQUIREMENTS

Statutory Requirements. Exceptions to the following provisions and exhibits by Respondent and/or their agent will lead to automatic disqualification of Respondent's proposal from consideration.

Sections:

Venue, Jurisdiction and Arbitration
Intellectual Property
Undisclosed Features
Ownership and Licenses
Certifications
Acceptance Criteria (if required)

Exhibits:

Insurance Requirements
Indemnification Requirements

Venue, Jurisdiction and Arbitration. For any dispute or claim arising under the award of a contract for this proposal, venue shall be in Bexar County, Texas, and the laws of the State of Texas shall apply. The City will not contractually agree to engage in binding arbitration and will not contractually agree to relinquish its right to a trial by jury.

Intellectual Property. If selected, Respondent agrees to abide by the following regarding intellectual property rights:

Respondent shall pay all royalties and licensing fees. Respondent shall hold the City harmless and indemnify the City from the payment of any royalties, damages, losses or expenses including attorney's fees for suits, claims or otherwise, growing out of infringement or alleged infringement of copyrights, patents, trademarks, trade secrets, materials and methods used in the project. It shall defend all suits for infringement of any Intellectual Property rights. Further, if Respondent has reason to believe that the design, service, process or product specified is an infringement of an Intellectual Property right, it shall promptly give such information to the City.

Upon receipt of notification that a third party claims that the program(s), hardware or both the program(s) and the hardware or any other intellectual property infringe upon any United States or International patent, copyright or trademark, Respondent will immediately:

Either:

Obtain, at Respondent's sole expense, the necessary license(s) or rights that would allow the City to continue using the programs, hardware, both the programs and hardware or any other intellectual property as the case may be, or,

Alter the programs, hardware, or both the programs and hardware so that the alleged infringement is eliminated, and

Reimburse the City for any expenses incurred by the City to implement emergency backup measures if the City is prevented from using the programs, hardware, or both the programs and hardware while the dispute is pending.

Respondent further agrees to:

Assume the defense of any claim, suit, or proceeding brought against the City for infringement of any United States patent, copyright, trademark or any other intellectual property rights arising from the use and/or sale of the equipment or software under this Agreement,

Assume the expense of such defense, including costs of investigations, reasonable attorneys' fees, expert witness fees, damages, and any other litigation-related expenses, and

Indemnify the City against any monetary damages and/or costs awarded in such suit;

Provided that:

Respondent is given sole and exclusive control of all negotiations relative to the settlement thereof, but that Respondent agrees to consult with the City Attorney of the City during such defense or negotiations and make good faith effort to avoid any position adverse to the interest of the City,

The Software or the equipment is used by the City in the form, state, or condition as delivered by Respondent or as modified without the permission of Respondent, so long as such modification is not the source of the infringement claim,

The liability claimed shall not have arisen out of the City's negligent act or omission, and

The City promptly provide Respondent with written notice within 15 days following the formal assertion of any claim with respect to which the City asserts that Respondent assumes responsibility under this section.

Undisclosed Features. CONTRACTOR warrants that the code and software provided to the City of San Antonio under this agreement does not contain any undisclosed features or functions that would impair or might impair the CITY'S use of the equipment, code or software. Specifically, but without limiting the previous representation, CONTRACTOR warrants there is no "Trojan Horse," lock, "time bomb," backdoor or similar routine. This Agreement shall not now nor will it hereafter be subject to the self-help provisions of the Uniform Computer Information Transactions Act or any other law. CONTRACTOR specifically disclaims any unilateral self-help remedies.

Ownership and Licenses.

In accordance with Texas law, Respondent acknowledges and agrees that all local government records created or received in the transaction of official business or the creation or maintenance of which were paid for with public funds are declared to be public property and subject to the provisions of Chapter 201 of the Texas Local Government Code and Subchapter J, Chapter 441 of the Texas Government Code. Thus, no such local government records produced by or on the behalf of Respondent pursuant to this Contract shall be the subject of any copyright or proprietary claim by Respondent.

The term “local government record” as used herein shall mean any document, paper, letter, book, map, photograph, sound or video recording, microfilm, magnetic tape, electronic medium, or other information recording medium, regardless of physical form or characteristic and regardless of whether public access to it is open or restricted under the laws of the state, created or received by local government or any of its officials or employees pursuant to law including an ordinance, or in the transaction of official business.

Respondent acknowledges and agrees that all local government records, as described in herein, produced in the course of the work required by any contract awarded pursuant to this RFCSP, will belong to and be the property of City. Respondent, if awarded this contract, will be required to turn over to City, all such records as required by said contract. Respondent, if awarded this contract, shall not, under any circumstances, release any records created during the course of performance of the contract to any entity without City’s written permission, unless required to do so by a Court of competent jurisdiction.

In accordance herewith, Respondent, if selected, agrees to comply with all applicable federal, state and local laws, rules and regulations governing documents and ownership, access and retention thereof.

Certifications. Respondent warrants and certifies that Respondent and any other person designated to provide services hereunder has the requisite training, license and/or certification to provide said services, and meets all competence standards promulgated by all other authoritative bodies, as applicable to the services provided herein.

006 TERM OF CONTRACT

A contract awarded in response to this RFCSP will be for a five (5) year period. The City shall have the option to renew for an additional three (3), one (1) year periods without additional City Council approval.

007 PRE-SUBMITTAL CONFERENCE

A Pre-Submittal Conference will be held at 111 Soledad, Suite 1100; San Antonio, TX 78205 at 8:00 a.m., Central Time, on Monday, April 13, 2015. Respondents are encouraged to prepare and submit their questions in writing 4 calendar days in advance of the Pre-Submittal Conference in order to expedite the proceedings. City's responses to questions received by this due date may be distributed at the Pre-Submittal Conference and posted with this solicitation. Attendance at the Pre-Submittal Conference is optional, but highly encouraged.

This meeting place is accessible to disabled persons. The 111 Soledad, Suite 1100; San Antonio, TX 78205 is wheelchair accessible. The accessible entrance is located at 111 Soledad, Riverview Towers, main entrance. Accessible parking spaces are located at Riverview Towers parking garage. Auxiliary aids and services are available upon request. Interpreters for the Deaf must be requested at least 48 hours prior to the meeting. For assistance, call (210) 207-7245 Voice/TTY.

Conference Bridge:
Local Dial-In Number: 210-207-8000
Toll Free Dial-In Number: 855-850-2672
Access Code: 6842

Any oral response given at the Pre-Submittal Conference that is not confirmed in writing and posted with this solicitation shall not be official or binding on the City. Only written responses shall be official and all other forms of communication with any officer, employee or agent of the City shall not be binding on the City. Respondents are encouraged to resubmit their questions in writing, to the City Staff person identified in the Restrictions on Communication section, after the conclusion of the Pre-Submittal Conference.

008 PROPOSAL REQUIREMENTS

Respondent's Proposal shall include the following items in the following sequence, noted with the appropriate heading as indicated below. If Respondent is proposing as a team or joint venture, provide the same information for each member of the team or joint venture.

Respondent shall submit one original hardcopy, signed in ink, and twelve (12) hardcopies of the proposal and one (1) compact disk (CD) also include one (1) flash drive containing an Adobe PDF version of the entire proposal in a sealed package clearly marked with the project name, "**SAPD WORN CAMERA TECHNOLOGY SOLUTION**", RFCSP 6100005871, on the front of the package.

TABLE OF CONTENTS

PROPOSAL. Prepare and submit the Proposal based on the requirements stated in the RFCSP and include as Attachment A.

RESPONDENT QUESTIONNAIRE. Use the Form found in this RFCSP as Attachment B.

CONTRACTS DISCLOSURE FORM. Use the Form in RFCSP Attachment C which is posted separately or Respondent may download a copy at:

https://www.sanantonio.gov/eforms/atty/ContractsDisclosureForm.pdf.

Instructions for completing the Contracts Disclosure form:

Download form and complete all fields. All fields must be completed prior to submitting the form.

Click on the "Print" button and place the copy in your proposal as indicated in the Proposal Checklist.

LITIGATION DISCLOSURE FORM. Complete and submit the Litigation Disclosure Form, found in this RFCSP as Attachment D. If Respondent is proposing as a team or joint venture, then all persons or entities who will be parties to the contract (if awarded) shall complete and return this form.

SMALL BUSINESS ECONOMIC DEVELOPMENT ADVOCACY (SBEDA) PROGRAM FORM(S). Complete, sign and submit any and all SBEDA form(s), found in this RFCSP as Attachment E.

PRICING SCHEDULE. Use the Pricing Schedule that is found in this RFCSP as Attachment F.

BUSINESS REQUIREMENTS-ADDITIONAL PROJECT DOCUMENTS. Complete and return as Attachment G.

SIGNATURE PAGE. Respondent must complete, sign and submit the Signature Page found in this RFCSP as Attachment H. The Signature Page must be signed by a person, or persons, authorized to bind the entity, or entities, submitting the proposal. Proposals signed by a person other than an officer of a corporate respondent or partner of partnership respondent shall be accompanied by evidence of authority.

VOSBPP TRACKING FORM.
Complete and return as Attachment I.

PROPOSAL CHECKLIST. Complete and submit the Proposal Checklist found in this RFCSP as Attachment J.

PROOF OF INSURABILITY. Submit a letter from insurance provider stating provider's commitment to insure the Respondent for the types of coverages and at the levels specified in this RFCSP if awarded a contract in response to this RFCSP. Respondent shall also submit a copy of their current insurance certificate. Exhibit 1.

FINANCIAL INFORMATION. Due to the anticipated investment and length of resultant contract between the parties, audited financial statements are preferred. In the event audited financial statements are not available, state the reason why. If audited financial statements are not available, respondents may submit other financial statement(s) or documentation, such as a Trial Balance Income Statement along with the most recent Annual Tax Submission, that validates and ensures the long term financial viability of the organization. Failure to provide requested information may impact your firm's final score.

Respondent is expected to examine this RFCSP carefully, understand the terms and conditions for providing the services listed herein and respond completely. FAILURE TO COMPLETE AND PROVIDE ANY OF THESE PROPOSAL REQUIREMENTS MAY RESULT IN THE RESPONDENT'S PROPOSAL BEING DEEMED NON-RESPONSIVE AND THEREFORE DISQUALIFIED FROM CONSIDERATION.

009 CHANGES TO RFCSP

Changes to the RFCSP, made prior to the due date for proposals shall be made directly to the original RFCSP. Changes are captured by creating a replacement version each time the RFCSP is changed. It is Respondent's responsibility to check for new versions until the proposal due date. City will assume that all proposals received are based on the final version of the RFCSP as it exists on the day proposals are due.

No oral statement of any person shall modify or otherwise change or affect the terms, conditions or specifications stated in the RFCSP.

010 SUBMISSION OF PROPOSALS

Proposals shall be submitted in hard copy format.

Submission of Hard Copy Proposals.

Respondent shall submit one original hardcopy, signed in ink, and twelve (12) hardcopies of the proposal and one (1) compact disk (CD) also include one (1) flash drive containing an Adobe PDF version of the entire proposal in a sealed package clearly marked with the project name, "**SAPD WORN CAMERA TECHNOLOGY SOLUTION**", RFCSP 6100005871, on the front of the package.

Proposals must be received in the City Clerk's Office no later than 2:00 p.m., Central Time, on Monday, April 27, 2015 at the address below. Any proposal or modification received after this time shall not be considered, and will be returned, unopened to the Respondent. Respondents should note that delivery to the P.O. Box address in a timely manner does not guarantee its receipt in the City Clerk's Office by the deadline for submission. Therefore, Respondents should strive for early submission to avoid the possibility of rejection for late arrival.

Mailing Address:
City Clerk's Office
Attn: IT Procurement Office (Finance Department)
P.O. Box 839966
San Antonio, Texas 78283-3966

Physical Address:
City Clerk's Office
Attn: IT Procurement Office (Finance Department)
100 Military Plaza
2nd Floor, City Hall San Antonio, Texas 78205

Proposals sent by facsimile or email will not be accepted.

Proposal Format. Each proposal shall be typewritten, single spaced and submitted on 8 ½" x 11" white paper. If submitting a hard copy, place proposal inside a three ring binder or other securely bound fashion. The use of recycled paper and materials is encouraged. Unnecessarily elaborate brochures, artwork, bindings, visual aides, expensive paper or other materials beyond that sufficient to present a complete and effective submission are not required. Font size shall be no less than 12-point type. All pages shall be numbered and, in the case of hard copy submissions, printed *two-sided.* Margins shall be no less than 1" around the perimeter of each page. A proposal response to RFCSP Attachment B – Respondent Questionnaire form may not exceed twenty-five (25) pages in length. Websites, or URLs shall not be submitted in lieu of the printed proposal. Each proposal must include the sections and attachments in the sequence listed in the RFCSP Section 008, Proposal Requirements, and each section and attachment must be indexed and, for hard copy submissions, divided by tabs and indexed in a Table of Contents page. For electronic submissions, on a CD and Flash Drive, each separate section should be attached as a separate file. Failure to meet the above conditions may result in disqualification of the proposal or may negatively affect scoring.

Correct Legal Name.

Respondents who submit proposals to this RFCSP shall correctly state the true and correct name of the individual, proprietorship, corporation, and /or partnership (clearly identifying the responsible general partner and all other partners who would be associated with the contract, if any). No nicknames, abbreviations (unless part of the legal title), shortened or short-hand, or local "handles" will be accepted in lieu of the full, true and correct legal name of the entity. These names shall comport exactly with the corporate and franchise records of the Texas Secretary of State and Texas Comptroller of Public Accounts. Individuals and proprietorships, if operating under other than an individual name, shall match with exact Assumed Name filings. Corporate Respondents and limited liability company Respondents shall include the 11-digit Comptroller's Taxpayer Number on the Respondent Questionnaire form found in this RFCSP as Attachment B.

If an entity is found to have incorrectly or incompletely stated its name or failed to fully reveal its identity on the General Information form, the Chief of Police and the Chief Technology Officer shall have the discretion, at any point in the contracting process, to suspend consideration of the proposal.

Firm Offer. All provisions in Respondent's proposal, including any estimated or projected costs, shall remain valid for one-hundred and eighty days (180) following the deadline date for submissions or, if a proposal is accepted, throughout the entire term of the contract.

Change Orders. In order to comply with Texas law governing purchases made by municipalities, the following rules shall govern all change orders made under this contract.

Any change orders that become necessary during the term of this contract as a result of changes in plans, specifications, quantity of work to be performed, materials, equipment or supplies to be furnished must be in writing and conform to the requirements of City Ordinance 2011-12-08-1014, as hereafter amended.

Any other change will require approval of the City Council, City of San Antonio.

Changes that do not involve an increase in contract price may be made by the City's Chief Technology Officer (CTO).

No oral statement of any person shall modify or otherwise change, or affect the terms, conditions or specifications stated herein.

Travel and Related Expenses. All proposed costs shall be inclusive of all Vendor's costs including, but not limited to, staffing, administrative overhead, travel, lodging, and any other expenses that may be incurred by the Vendor. The City of San Antonio will not separately reimburse the Vendor for any expenses beyond what the Vendor includes in their pricing proposal.

Confidential or Proprietary Information. All proposals become the property of the City upon receipt and will not be returned. Any information deemed to be confidential by Respondent should be clearly noted; however, City cannot guarantee that it will not be compelled to disclose all or part of any public record under the Texas Public Information Act, since information deemed to be confidential by Respondent may not be considered confidential under Texas law, or pursuant to a Court order. Respondent acknowledge that exemptions to Public Information Act requests may require a brief to be submitted to the Texas Attorney General explaining why the claimed exceptions apply to the information in issue. The City shall not be obligated to submit the brief supporting those claimed exceptions. Respondent shall be solely responsible for submitting the brief and the documents in issue to the Texas Attorney General.

Cost of Proposal. Any cost or expense incurred by the Respondent that is associated with the preparation of the Proposal, the Pre-Submittal conference, if any, or during any phase of the selection process, shall be borne solely by Respondent.

011 RESTRICTIONS ON COMMUNICATION

Respondents are prohibited from communicating with: 1) elected City officials and their staff regarding the RFCSP or proposals from the time the RFCSP has been released until the contract is posted as a City Council agenda item; and 2) City employees from the time the RFCSP has been released until the contract is awarded. These restrictions extend to "thank you" letters, phone calls, emails and any contact that results in the direct or indirect discussion of the RFCSP and/or proposal submitted by Respondent. Violation of this provision by Respondent and/or its agent may lead to disqualification of Respondent's proposal from consideration.

Exceptions to the Restrictions on Communication with City employees include:

Respondents may ask verbal questions concerning this RFCSP at the Pre-Submittal Conference.

Respondents may submit written questions concerning this RFCSP to the Staff Contact Person listed below until **2:00 p.m.**, Central Time, on **Thursday, April 16, 2015**. Questions received after the stated deadline will not be answered. All questions shall be sent by e-mail.

William Flint, Procurement Specialist III
City of San Antonio, IT Procurement Office
william.flint@sanantonio.gov

Questions submitted and the City's responses will be posted with this solicitation.

Respondents and/or their agents are encouraged to contact the Small Business Office of the Economic Development Department for assistance or clarification with issues specifically related to the City's Small Business Economic Development Advocacy (SBEDA) Program policy and/or completion of the SBEDA form. The point of contact is Irene Maldonado. Ms. Maldonado may be reached by telephone at 210) 207-8124 or by e-mail at Irene.maldonado@sanantonio.gov. *This exception to the restriction on communication does not apply, and there is no contact permitted to the Small Business Office regarding this solicitation, after the solicitation closing date.*

Respondents may provide responses to questions asked of them by the Staff Contact Person after responses are received and opened. During interviews, if any, verbal questions and explanations will be permitted. If interviews are conducted, Respondents shall not bring lobbyists. The City reserves the right to exclude any persons from interviews as it deems in its best interests.

Upon completion of the evaluation process, Respondents shall receive a notification letter indicating the recommended firm and anticipated City Council agenda date. Respondents desiring a review of the solicitation process may submit a written request no later than seven (7) calendar days from the date letter was sent. The letter will indicate the name and address for submission of requests for review.

012 EVALUATION CRITERIA

City will conduct a comprehensive, fair and impartial evaluation of all submissions received in response to this RFCSP. City may appoint a selection committee to perform the evaluation. Each submission will be analyzed to determine overall responsiveness and qualifications under this RFCSP. Criteria to be evaluated will include the items listed below. In accordance with §252.042, Texas Local Government Code, the selection committee may select all, some or none of the respondents who are judged to be reasonably qualified for award of the contract for interviews. Should the City elect to conduct interviews, selection for interviews will be based on initial scoring, prior to interviewing. Interviews are not an opportunity to change a submission. If the City elects to conduct interviews, respondents may be interviewed and re-scored based upon the same criteria. City may also request information from respondents at any time prior to final approval of a selected respondent, or seek best and final offers from respondents deemed reasonably qualified for award. Final approval of a selected respondent is subject to the action of the San Antonio City Council.

Evaluation criteria:

Proposed Solution (45 points)

Experience, Background, Qualifications (20 points)

Pricing (15 points)

SBE Prime Contract Program – 20 pts.

Certified SBE firms headquartered or having a Significant Business Presence within the San Antonio Metropolitan Statistical Area responding to this solicitation as Prime Contractors proposing at least 51% SBE participation (Prime and/or Subcontractor) will receive twenty (20) evaluation criteria percentage points.

No evaluation criteria percentage Points will be awarded to non-SBE or non-ESBE Prime Contractors through subcontracting to certified SBE or ESBE firms.

013 AWARD OF CONTRACT AND RESERVATION OF RIGHTS

City reserves the right to award one, more than one or no contract(s) in response to this RFCSP.

The Contract, if awarded, will be awarded to the Respondent(s) whose Proposal(s) is deemed most advantageous to City, as determined by the selection committee, upon approval of the City Council.

City may accept any Proposal in whole or in part. However, final selection of a Respondent is subject to City Council approval.

City reserves the right to accept one or more proposals or reject any or all proposals received in response to this RFCSP, and to waive informalities and irregularities in the proposals received. City also reserves the right to terminate this RFCSP, and reissue a subsequent solicitation, and/or remedy technical errors in the RFCSP process.

City will require the selected Respondent(s) to execute a contract with the City, prior to City Council award, incorporating the terms and conditions of this RFCSP. No work shall commence until City signs the contract document(s) and Respondent provides the necessary evidence of insurance as required in this RFCSP and the Contract. Contract documents are not binding on City until approved by the City Attorney. In the event the parties cannot execute a contract within the time specified, City reserves the right to terminate contract discussions with the selected Respondent and commence contract discussions with another Respondent.

This RFCSP does not commit City to enter into a Contract, award any services related to this RFCSP, nor does it obligate City to pay any costs incurred in preparation or submission of a proposal or in anticipation of a contract.

If selected, Respondent will be required to comply with the Insurance and Indemnification Requirements established herein. If Respondent takes exception to the terms and conditions of this RFCSP, the City may deem the Respondent non-responsive and not evaluate their proposal.

The successful Respondent must be able to formally invoice the City for services rendered, incorporating the SAP-generated contract and purchase order numbers that shall be provided by the City.

Conflicts of Interest. Respondent acknowledges that it is informed that the Charter of the City of San Antonio and its Ethics Code prohibit a City officer or employee, as those terms are defined in the Ethics Code, from having a financial interest in any contract with City or any City agency such as City-owned utilities. An officer or employee has a "prohibited financial interest" in a contract with City or in the sale to City of land materials, supplies or service, if any of the following individual(s) or entities is a party to the contract or sale: the City officer or employee; his parent, child or spouse; a business entity in which he or his parent, child or spouse owns ten (10) percent or more of the voting stock or shares of the business entity, or ten (10) percent or more of the fair market value of the business entity; or a business entity in which any individual or entity above listed is a subcontractor on a City contract, a partner or a parent or subsidiary business entity.

Respondent is required to warrant and certify that it, its officers, employees and agents are neither officials nor employees of the City, as defined in Section 2-42 of the City's Ethics Code. (Discretionary Contracts Disclosure – form may be found online at https://www.sanantonio.gov/eforms/atty/DiscretionaryContractsDisclosure.pdf.)

Independent Contractor. Respondent agrees and understands that, if selected, it and all persons designated by it to provide services in connection with a contract, are and shall be deemed to be an independent contractors, responsible for their respective acts or omissions, and that City shall in no way be responsible for Respondent's actions, and that none of the parties hereto will have authority to bind the others or to hold out to third parties, that it has such authority.

Effective January 1, 2006, Chapter 176 of the Texas Local Government Code requires that persons, or their agents, who seek to contract for the sale or purchase of property, goods, or services with the City, shall file a completed conflict of interest questionnaire with the City Clerk not later than the 7th business day after the date the person: (1) begins contract discussions or negotiations with the City; or (2) submits to the City an application, response to a request for proposals or bids, correspondence, or another writing related to a potential agreement with the City. The conflict of interest questionnaire form is available from the Texas Ethics Commission at http://www.ethics.state.tx.us/forms/CIQ.pdf. Completed conflict of interest questionnaires may be mailed or delivered by hand to the Office of the City Clerk. If mailing a completed conflict of interest questionnaire, mail to: Office of the City Clerk, P.O. Box 839966, San Antonio, TX 78283-3966. If delivering a completed conflict of interest questionnaire, deliver to: Office of the City Clerk, City Hall, 2nd floor, 100 Military Plaza, San Antonio, TX 78205. Respondent should consult its own legal advisor for answers to questions regarding the statute or form.

014 BONDS

This section left blank intentionally.

015 SOFTWARE ESCROW REQUIREMENT

To ensure that the City will have access to the Contractor's source code in the event that the Contractor is unable to support the software, a copy of the Contractor's source code shall be kept by a trusted third party agreeable to the City. A Software Escrow Agreement, attached as RFCSP EXHIBIT 3 shall be submitted to evidence the deposit of the source code and the maintenance of the escrow account. The Contractor may submit its own Software Escrow Agreement, provided it is in substantially similar form to the attached RFCSP EXHIBIT 3, in the determination of the City.

016 ACCEPTANCE CRITERIA

All deliverables submitted to the City hereunder shall be submitted to a designated City employee for approval and that such deliverables comply in all material respects with the requirements as set forth in a Statement of Work.

The City will evaluate both On-Premise and Off-Premise solutions. Vendor may submit proposals for On-Premise, Off-Premise or both solutions. Each will be evaluated on its own merits. The City reserves the right to award based on a determination of what solution best meets the City's business need.

In the event of any nonconformity or nonfunctionality of deliverables, the City shall provide Respondent written notification within 14 days of delivery. Upon receipt of such notice of nonconformity or nonfunctionality, Respondent shall have 14 days to cure the nonconformity or nonfunctionality.

Upon delivery of the cure, the City will have 14 days to evaluate and determine if such cure is acceptable. In the event the Deliverable remains unacceptable, the City will provide a second notice of nonconformity or nonfunctionality of the

system within 30 days of delivery. Respondent shall have an additional 14 days to cure the nonconformity or nonfunctionality.

Upon delivery of the cure, the City will have 14 days to evaluate and determine if such cure is acceptable. In the event the Deliverable remains unacceptable the City will provide Respondent with a third notice of any nonconformity or nonfunctionality of the system and Respondent will forfeit 50% of retained balances on hold with the City at the time the third notice is provided to Respondent.

A retainage in the amount of 10% of the deliverable price shall be held by the City, to be paid upon final acceptance. The City Project Team will review, approve, and sign off on the deliverable. Upon acceptance of each milestone, the Contractor will be paid 90% of the agreed upon milestone.

Upon final acceptance, Contractor shall invoice the City for the 10% final acceptance hold-back payment.

017 SCHEDULE OF EVENTS

Following is a list of **projected dates/times** with respect to this RFCSP:

RFCSP Release	**Monday, April 6, 2015**
Pre-Submittal Conference	**Monday, April 13, 2015, 8:00 AM Central Time**
Final Questions Accepted	**Thursday, April 16, 2015, 2:00 PM Central Time**
Proposal Due	**Monday, April 27, 2015, 2:00 PM Central Time**

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

018 RFCSP EXHIBITS

RFCSP EXHIBIT 1

INSURANCE REQUIREMENTS

If selected to provide the services described in this RFCSP, Respondent shall be required to comply with the insurance requirements set forth below:

INSURANCE

If selected to provide the services described in this RFCSP, Respondent shall be required to comply with the insurance requirements set forth below:

A) Prior to the commencement of any work under this Agreement, Respondent shall furnish copies of all required endorsements and completed Certificate(s) of Insurance to the City's Finance Department, which shall be clearly labeled "**SAPD BODY WORN CAMERA TECHNOLOGY SOLUTION**" in the Description of Operations block of the Certificate. The Certificate(s) shall be completed by an agent and signed by a person authorized by that insurer to bind coverage on its behalf. The City will not accept a Memorandum of Insurance or Binder as proof of insurance. The certificate(s) must have the agent's signature and phone number, and be mailed, with copies of all applicable endorsements, directly from the insurer's authorized representative to the City. The City shall have no duty to pay or perform under this Agreement until such certificate and endorsements have been received and approved by the City's Finance Department. No officer or employee, other than the City's Risk Manager, shall have authority to waive this requirement.

B) The City reserves the right to review the insurance requirements of this Article during the effective period of this Agreement and any extension or renewal hereof and to modify insurance coverages and their limits when deemed necessary and prudent by City's Risk Manager based upon changes in statutory law, court decisions, or circumstances surrounding this Agreement. In no instance will City allow modification whereby City may incur increased risk.

C) A Respondent's financial integrity is of interest to the City; therefore, subject to Respondent's right to maintain reasonable deductibles in such amounts as are approved by the City, Respondent shall obtain and maintain in full force and effect for the duration of this Agreement, and any extension hereof, at Respondent's sole expense, insurance coverage written on an occurrence basis, unless otherwise indicated, by companies authorized to do business in the State of Texas and with an A.M Best's rating of no less than A- (VII), in the following types and for an amount not less than the amount listed below:

TYPE	AMOUNTS
1. Workers' Compensation 2. Employers' Liability	Statutory $500,000/$500,000/$500,000
3. Broad form Commercial General Liability Insurance to include coverage for the following: a. Premises/Operations *b. Independent Contractors c. Products/Completed Operations d. Personal Injury e. Contractual Liability f. Damage to property rented by you	For Bodily Injury and Property Damage of $1,000,000 per occurrence; $2,000,000 General Aggregate, or its equivalent in Umbrella or Excess Liability Coverage f. $100,000
4. Business Automobile Liability a. Owned/leased vehicles b. Non-owned vehicles c. Hired Vehicles	Combined Single Limit for Bodily Injury and Property Damage of $1,000,000 per occurrence
5. Professional Liability (Claims-made basis) To be maintained and in effect for no	$1,000,000 per claim, to pay on behalf of the insured all sums which the insured shall

less than two years subsequent to the completion of the professional service.	become legally obligated to pay as damages by reason of any act, malpractice, error, or omission in professional services.
*if applicable	

D) Respondent agrees to require, by written contract, that all subcontractors providing goods or services hereunder obtain the same insurance coverages required of Respondent herein, and provide a certificate of insurance and endorsement that names the Respondent and the CITY as additional insureds. Respondent shall provide the CITY with said certificate and endorsement prior to the commencement of any work by the subcontractor. This provision may be modified by City's Risk Manager, without subsequent City Council approval, when deemed necessary and prudent, based upon changes in statutory law, court decisions, or circumstances surrounding this agreement. Such modification may be enacted by letter signed by City's Risk Manager, which shall become a part of the contract for all purposes.

E) As they apply to the limits required by the City, the City shall be entitled, upon request and without expense, to receive copies of the policies, declaration page, and all endorsements thereto and may require the deletion, revision, or modification of particular policy terms, conditions, limitations, or exclusions (except where policy provisions are established by law or regulation binding upon either of the parties hereto or the underwriter of any such policies). Respondent shall be required to comply with any such requests and shall submit a copy of the replacement certificate of insurance to City at the address provided below within 10 days of the requested change. Respondent shall pay any costs incurred resulting from said changes.

City of San Antonio
SAPD BODY WORN CAMERA TECHNOLOGY SOLUTION
Attn: IT Procurement Office (Finance Department)
P.O. Box 839966
San Antonio, Texas 78283-3966

F) Respondent agrees that with respect to the above required insurance, all insurance policies are to contain or be endorsed to contain the following provisions:

- Name the City, its officers, officials, employees, volunteers, and elected representatives as additional insureds by endorsement, as respects operations and activities of, or on behalf of, the named insured performed under contract with the City, with the exception of the workers' compensation and professional liability policies;

- Provide for an endorsement that the "other insurance" clause shall not apply to the City of San Antonio where the City is an additional insured shown on the policy;

- Workers' compensation, employers' liability, general liability and automobile liability policies will provide a waiver of subrogation in favor of the City.

- Provide advance written notice directly to City of any suspension, cancellation, non-renewal or material change in coverage, and not less than ten (10) calendar days advance notice for nonpayment of premium.

G) Within five (5) calendar days of a suspension, cancellation or non-renewal of coverage, Respondent shall provide a replacement Certificate of Insurance and applicable endorsements to City. City shall have the option to suspend Respondent's performance should there be a lapse in coverage at any time during this contract. Failure to provide and to maintain the required insurance shall constitute a material breach of this Agreement.

H) .In addition to any other remedies the City may have upon Respondent's failure to provide and maintain any insurance or policy endorsements to the extent and within the time herein required, the City shall have the right to order Respondent to stop work hereunder, and/or withhold any payment(s) which become due to Respondent hereunder until Respondent demonstrates compliance with the requirements hereof.

I) Nothing herein contained shall be construed as limiting in any way the extent to which Respondent may be held responsible for payments of damages to persons or property resulting from Respondent's or its subcontractors' performance of the work covered under this Agreement.

J) It is agreed that Respondent's insurance shall be deemed primary and non-contributory with respect to any insurance or self insurance carried by the City of San Antonio for liability arising out of operations under this Agreement.

K) It is understood and agreed that the insurance required is in addition to and separate from any other obligation contained in this Agreement and that no claim or action by or on behalf of the City shall be limited to insurance coverage provided..

L) Respondent and any Subcontractors are responsible for all damage to their own equipment and/or property.

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

RFCSP EXHIBIT 2

INDEMNIFICATION REQUIREMENTS

If selected to provide the services described in this RFCSP, Respondent shall be required to comply with the indemnification requirements set forth below:

INDEMNIFICATION

RESPONDENT covenants and agrees to FULLY INDEMNIFY, DEFEND and HOLD HARMLESS, the CITY and the elected officials, employees, officers, directors, volunteers and representatives of the CITY, individually and collectively, from and against any and all costs, claims, liens, damages, losses, expenses, fees, fines, penalties, proceedings, actions, demands, causes of action, liability and suits of any kind and nature, including but not limited to, personal or bodily injury, death and property damage, made upon the CITY directly or indirectly arising out of, resulting from or related to RESPONDENT'S activities under this Agreement, including any acts or omissions of RESPONDENT, any agent, officer, director, representative, employee, consultant or subcontractor of RESPONDENT, and their respective officers, agents employees, directors and representatives while in the exercise of the rights or performance of the duties under this Agreement. The indemnity provided for in this paragraph shall not apply to any liability resulting from the negligence of CITY, its officers or employees, in instances where such negligence causes personal injury, death, or property damage. IN THE EVENT RESPONDENT AND CITY ARE FOUND JOINTLY LIABLE BY A COURT OF COMPETENT JURISDICTION, LIABILITY SHALL BE APPORTIONED COMPARATIVELY IN ACCORDANCE WITH THE LAWS FOR THE STATE OF TEXAS, WITHOUT, HOWEVER, WAIVING ANY GOVERNMENTAL IMMUNITY AVAILABLE TO THE CITY UNDER TEXAS LAW AND WITHOUT WAIVING ANY DEFENSES OF THE PARTIES UNDER TEXAS LAW.

The provisions of this INDEMNITY are solely for the benefit of the parties hereto and not intended to create or grant any rights, contractual or otherwise, to any other person or entity. RESPONDENT shall advise the CITY in writing within 24 hours of any claim or demand against the CITY or RESPONDENT known to RESPONDENT related to or arising out of RESPONDENT's activities under this AGREEMENT and shall see to the investigation and defense of such claim or demand at RESPONDENT's cost. The CITY shall have the right, at its option and at its own expense, to participate in such defense without relieving RESPONDENT of any of its obligations under this paragraph.

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

RFCSP EXHIBIT 3

ESCROW AGREEMENT

Account Number _____

This agreement ("Agreement") is effective _____ , 20__ among _____ ("Custodian"), _____ ("Depositor") and the Beneficiary, the City of San Antonio ("City"), who collectively may be referred to in this Agreement as the parties ("Parties").

A. Depositor and City have entered or will enter into a license agreement, development agreement, and/or other agreement regarding certain proprietary technology of Depositor (referred to in this Agreement as "the License Agreement").

B. Depositor desires to avoid disclosure of its proprietary technology except under certain limited circumstances.

C. The availability of the proprietary technology of Depositor is critical to City in the conduct of its business and, therefore, City needs access to the proprietary technology under certain limited circumstances.

D. Depositor and City desire to establish an escrow with Custodian to provide for the retention, administration and controlled access of the proprietary technology materials of Depositor.

E. The parties desire this Agreement to be supplementary to the License Agreement pursuant to 11 United States [Bankruptcy] Code, Section 365(n).

ARTICLE 1 -- **DEPOSITS**

1.1 Obligation to Make Deposit. Upon the signing of this Agreement by the parties, Depositor shall deliver to Custodian the proprietary technology and other materials ("Deposit Materials") required to be deposited by the License Agreement or, if the License Agreement does not identify the materials to be deposited with Custodian, then such materials will be identified on Exhibit A. If Exhibit A is applicable, it is to be prepared and signed by Depositor and City. Custodian shall have no obligation to either party with respect to the preparation, accuracy, execution or delivery of Exhibit A.

1.2 Identification of Tangible Media. Prior to the delivery of the Deposit Materials to Custodian, Depositor shall conspicuously label for identification each document, magnetic tape, disk, or other tangible media upon which the Deposit Materials are written or stored. Additionally, Depositor shall complete a copy of Exhibit B to this Agreement by listing each such tangible media by the item label description, the type of media and the quantity. Each Exhibit B shall be signed by Depositor and delivered to Custodian with the Deposit Materials. Unless and until Depositor makes the initial deposit with Custodian, Custodian shall have no obligation with respect to this Agreement, except the obligation to notify the parties regarding the status of the account as required in Section 2.2 below.

1.3 Acceptance of Deposit. Custodian will conduct a deposit inspection upon receipt of any Deposit Material and associated Exhibit B by visually matching the labeling of the tangible media containing the Deposit Materials to the item descriptions and quantity listed on Exhibit B. Depositor shall provide notice by electronic mail, telephone, or regular mail to the Depositor and Beneficiary of all Deposit Material that is accepted and deposited into the escrow account under this Agreement. If Custodian determines that the Deposit Material does not match the description provided by Depositor represented in Exhibit B attached hereto, Custodian will provide Depositor with notice by electronic mail, telephone, or regular mail of such discrepancies. Custodian will work directly with the Depositor to resolve any such discrepancies prior to accepting Deposit Material. Other than Custodian's

inspection of the Deposit Materials, Custodian shall have no obligation to the accuracy, completeness, functionality, performance or non-performance of the Deposit Materials.

1.4 Depositor's Representations. Depositor represents as follows:

a. Depositor lawfully possesses all of the Deposit Materials deposited with Custodian;

b. With respect to all of the Deposit Materials, Depositor has the right and authority to grant to Custodian and City the rights as provided in this Agreement;

c. As of the effective date of this Agreement, the Deposit Materials are not the subject of a lien or encumbrance, however, any liens or encumbrances made after the execution of this Agreement will not prohibit, limit, or alter the rights and obligations of Custodian under this Agreement;

d. The Deposit Materials consist of the proprietary technology and other materials identified either in the License Agreement or Exhibit A, as the case may be; and

e. The Deposit Materials are readable and useable in the appropriate technical environment their current form or, if any portion of the Deposit Materials is encrypted, the decryption tools and decryption keys have also been deposited.

f. The Deposit Materials include the source code corresponding to the computer software licensed by Depositor to City under the License Agreement, except for third-party software that Depositor has no right to provide to Custodian or to City in source code form. Either the License Agreement or Exhibit A properly identifies all third-party software embedded in or associated with the computer software licensed by Depositor to City under the License Agreement that is not included in the Deposit Materials. The Deposit Materials include any pertinent commentary or explanation that may be necessary to render the source code understandable and useable by a trained computer-programming expert who is generally familiar with _____ systems and _____ program code. The Deposit Materials include system documentation, statements of principles of operation and schematics, all as necessary or useful for the effective understanding and use of the source code. Insofar as the “development environment” employed by Depositor for the development, maintenance, and implementation of the Source Code includes any device, programming, or documentation not commercially available to City on reasonable terms through readily known sources other than Depositor, the Deposit Materials shall include all such devices, programming, or documentation. The foregoing reference to such “development environment” is intended to apply to any programs, including compilers, “workbenches,” tools, and higher-level (or “proprietary”) languages, used by Depositor for the development, maintenance and implementation of the Source Code.

1.5 Deposit Updates. Unless otherwise provided by the License Agreement, Depositor shall update the Deposit Materials within sixty (60) days of each release of a new version, release, addition, modification or update of the licensed software, which is subject to the License Agreement; provided that Depositor shall not be required to make updates more often than once every six (6) months, nor less frequently than once per year. Such updates will be added to the existing deposit. All deposit updates shall be listed on a new Exhibit B and Depositor shall sign the new Exhibit B. Each Exhibit B will be held and maintained separately within the escrow account. An independent record will be created which will document the activity for each Exhibit B. The processing of all deposit updates shall be in accordance with Sections 1.2 and 1.3 above. All references in this Agreement to the Deposit Materials shall include the initial Deposit Materials and any updates.

1.6 Removal of Deposit Materials. The Deposit Materials may be removed and/or exchanged only on written instructions signed by Depositor and City, or as otherwise provided in this Agreement.

1.7 Verification. City shall have the right to cause a verification of any Deposit Materials once within the first 90 days after the end of the warranty period, and thereafter once in any 12-month period, at Depositor’s expense,. City shall notify Depositor and Custodian of City's request for verification. Depositor shall have the right to be present at the verification. A verification determines, in different levels of detail, the accuracy, completeness, sufficiency and quality of the Deposit Materials as well as to confirm that it compiles to the pertinent object code of the licensed software. If a verification is elected after the Deposit Materials have been delivered to Custodian, then Custodian, or at City's election, an independent person or company selected by City who is reasonably acceptable to Depositor will perform the verification. The Depositor shall be responsible

for all costs of the verification, including, without limitation, Custodian's fees associated with the verification, the costs incurred by Depositor relating to such verification (including, without limitation, travel and living expenses for Depositor personnel required to assist with the verification and fees for the services of such personnel, at Depositor's standard daily rates, as applicable).

ARTICLE 2 -- **CONFIDENTIALITY AND RECORD KEEPING**

2.1 Confidentiality. Custodian shall have the obligation to reasonably protect the confidentiality of the Deposit Materials by maintaining the Deposit Materials in a secure, environmentally safe, locked facility which is accessible only to authorized representatives of Custodian. Except as provided in this Agreement or any subsequent agreement between the Parties, Custodian shall not disclose, transfer, make available to any party, or use the Deposit Materials. Custodian shall not disclose the terms of this Agreement to any third party. If Custodian receives a subpoena or any other order from a court or other judicial tribunal pertaining to the disclosure or release of the Deposit Materials, Custodian will immediately notify the parties to this Agreement of same in writing, unless prohibited by law. It shall be the responsibility of Depositor to challenge any such order; provided, however, that Custodian does not waive its rights to present its position with respect to any such order. Custodian will not be required to disobey any order from a court or other judicial tribunal, including, but not limited to, notices delivered pursuant to Section 7.6 below. Custodian will not be required to disobey any order from a court or other judicial tribunal.

2.2 Status Reports. Custodian shall provide to Depositor and City access to the Custodian's real-time, on-line portal to view data and documentation relative to this Agreement. Upon request, Custodian will provide ad hoc status reports to Depositor and City.

2.3 Audit Rights. During the term of this Agreement, Depositor and City shall each have the right to inspect the written records of Custodian pertaining to this Agreement. Any such inspection shall occur during normal business hours and following reasonable prior notice.

ARTICLE 3 -- **RIGHT TO MAKE COPIES**

Custodian may make copies of the Deposit Materials as necessary to meet its obligations under this Agreement, while retaining a copy to carry out its obligations for other licensees who may benefit from the same arrangement. Custodian shall include in any copies all copyright, non-disclosure and other proprietary notices and titles contained on the Deposit Materials. With all Deposit Materials submitted to Custodian, Depositor shall provide any and all instructions as may be necessary to duplicate the Deposit Materials, including, without limitation, instructions as to necessary hardware or software. In all other respects, Custodian shall not make copies of the Deposit Materials except to fulfill an order of a court of competent jurisdiction (see Section 2.1).

If for any reason Custodian should make any copy of the Deposit Materials, Custodian shall promptly give written notice to Depositor of such action and shall explain the reason for such copying in the notice.

ARTICLE 4 -- **RELEASE OF DEPOSIT**

4.1 Release Conditions. As used in this Agreement, “Release Condition” shall mean the occurrence and continuance of any of the following:

a. Entry of an order for relief regarding Depositor under Title 11 (bankruptcy) of the United States Code, the making by Depositor of a general assignment for the benefit of its creditors, the appointment of a general receiver or trustee in bankruptcy of Depositor's business or property, or the commencement of similar proceedings under the bankruptcy, insolvency, liquidation or reorganization laws of any state or any other country or province (except that were entry of an order, appointment of a receiver or trustee in bankruptcy, or

commencement of bankruptcy or insolvency proceedings is effected on an involuntary basis, then Depositor shall have 60 days to have such case or proceeding dismissed);

b. Depositor's failure to continue to do business in the ordinary course;

c. Any decision by Depositor to withdraw maintenance services in support of the Depositor software licensed by Depositor to City under the License Agreement;

d. The occurrence of a material breach *(or a series of related breaches that collectively are material)* under the implementation, maintenance and support terms of the License Agreement, which Depositor fails to cure within thirty (30) days (or such longer period of time as may be reasonable under the circumstances) after written notice of such breach;

e. The occurrence of any condition *(whether or not qualifying as a breach)* having a critical impact on necessary business functions *(such as a continuing loss of service or data)*, which Depositor cannot or will not assure City will be corrected so to restore necessary business functions using all reasonable means, and the release of the Deposit Materials is reasonably believed to enable City to remedy such condition critically impacting City's use of the licensed software to meet necessary business functions; and, for purposes of this Agreement, if a Release Condition is claimed by City to exist on this basis, then, notwithstanding Sections 4.2 and 4.3 hereof, Custodian will, without delay, release the Deposit Materials to City immediately upon Custodian's receipt of written notice of such Release Condition in which City shall explain why it believes the Deposit Materials will enable City to resolve such critical impact condition and why an immediate release is required, but City shall commit to surrender the Deposit Materials to Custodian or Depositor promptly after the correction has occurred to restore necessary business functions.

4.2 Filing For Release. If City believes in good faith that a Release Condition has occurred and is continuing, then City, at any time, may provide to Custodian written notice of the occurrence of the Release Condition and a request for the release of the Deposit Materials. Within five (5) business days of receipt of a written notice, Custodian shall provide a copy of the notice to Depositor. Custodian will promptly notify the Parties unless Custodian acknowledges or discovers independently, or through the Parties, its need for additional documentation or information in order to comply with this Section. Such need for additional documentation or information may extend the time period for Custodian's performance under this section.

4.3 Contrary Instructions. From the date Custodian mails the notice by overnight express mail requesting release of the Deposit Materials, Depositor shall have ten (10) business days to deliver to Custodian contrary instructions (“Contrary Instructions”). Contrary Instructions shall mean the written representation by Depositor that a Release Condition has not occurred or has been cured. Upon receipt of Contrary Instructions, Custodian shall send a copy of Contrary Instructions to City by overnight commercial express mail. Additionally, Custodian shall notify both Depositor and City that there is a dispute to be resolved pursuant to Section 7.4 of this Agreement. Subject to Section 5.2 and 4.1(e) of this Agreement, Custodian will continue to store the Deposit Materials without release pending (a) joint instructions from Depositor and City; or (b) dispute resolution pursuant to Section 7.4; or (c) an order from a court of competent jurisdiction.

4.4 Release of Deposit. If Custodian does not receive Contrary Instructions from the Depositor, or if the Preferred Beneficiaries request to release is based on 4.1(e), Custodian is authorized to release the Deposit Materials to the City. However, Custodian is entitled to receive any fees due Custodian before making the release. This Agreement will terminate upon the release of the Deposit Materials held by Custodian.

4.5 Right to Use Following Release. Unless otherwise provided in the License Agreement, upon release of the Deposit Materials in accordance with this Article 4, City shall have the right to use the Deposit Materials for the sole purpose of continuing the benefits afforded to City by the License Agreement. City shall be obligated to maintain the confidentiality of the released Deposit Materials. In the event that the Deposit Materials shall be delivered out of escrow to City pursuant to the terms hereof, City shall be entitled to request and obtain immediately from Depositor any modifications, updates, new releases or new documentation (including source code for any such software) related to the software then licensed by City from Depositor, insofar as the same have not been included in any previous deposit.

ARTICLE 5 -- **TERM AND TERMINATION**

5.1 Term of Agreement. The initial term of this Agreement is for a period of one year. Thereafter, this Agreement shall automatically renew from year-to-year unless (a) Depositor and City jointly instruct Custodian in writing that the Agreement is terminated; (b) Custodian instructs Depositor and City in writing ninety (90) days after its renewal date, that the Agreement is terminated for nonpayment in accordance with Section 5.2; or (c) Custodian reserves the right to terminate this Agreement, for any reason, other than for nonpayment, by providing Depositor and City sixty (60) days written notice of its intent to terminate this Agreement. If the Deposit Materials are subject to another escrow agreement with Custodian, Custodian reserves the right, after the initial one year term, to adjust the anniversary date of this Agreement to match the then prevailing anniversary date of such other escrow arrangements.

5.2 Termination for Nonpayment. In the event of the nonpayment of fees owed to Custodian, Custodian shall provide written notice of delinquency to all parties to this Agreement. Any party to this Agreement shall have the right to make the payment to Custodian to cure the default. If the past due payment is not received in full by Custodian within one (1) month of the date of such notice, then Custodian shall have the right to terminate this Agreement at any time thereafter by sending written notice of termination to all parties. Custodian shall have no obligation to take any action under this Agreement so long as any payment due to Custodian remains unpaid.

5.3 Disposition of Deposit Materials Upon Termination. Subject to the foregoing termination provisions, and upon termination of this Agreement, Custodian shall destroy, return to Depositor, or otherwise deliver the Deposit Materials in accordance with Depositor's instructions. If there are no instructions, Custodian may, at its sole discretion, destroy the Deposit Materials or return them to Depositor. Custodian shall have no obligation to destroy or return the Deposit Materials if the Deposit Materials are subject to another escrow agreement with Custodian or have been totally released to the City in accordance with Section 4.4.

5.4 Survival of Terms Following Termination. Upon termination of this Agreement, the following provisions of this Agreement shall survive:

a. Depositor's Representations (Section 1.4);

b. The obligations of confidentiality with respect to the Deposit Materials;

c. The obligation to pay Custodian any fees and expenses due;

d. The provisions of Article 7;

e. Section 4.5 to the extent applicable; and

f. Any provisions in this Agreement which specifically state they survive the termination of this Agreement.

ARTICLE 6 -- **CUSTODIAN'S FEES**

6.1 Fee Schedule. Custodian is entitled to be paid its agreed fees and expenses applicable to the services provided by Depositor. Custodian shall notify the Depositor for payment of Custodian's fees at least sixty (60) days prior to any increase in fees. For any service not listed on Custodian's standard fee schedule, Custodian will provide a quote prior to rendering the service, if requested.

6.2 Payment Terms. Custodian shall not be required to perform any service, including release of any Deposit Materials under Article 4, unless the payment for such service and any outstanding balances owed to Custodian are paid in full. Fees are due upon receipt of a signed contract or receipt of the Deposit Materials whichever is earliest. If invoiced fees are not paid, Custodian may terminate this Agreement in accordance with Section 5.2.

ARTICLE 7 -- **LIABILITY AND DISPUTES**

7.1 Right to Rely on Instructions. Custodian may act in reliance upon any instruction, instrument, or signature reasonably believed by Custodian to be genuine. Custodian may assume that any employee of a party to this Agreement who gives any written notice, request, or instruction has the authority to do so. Custodian will not be required to inquire into the truth or evaluate the merit of any statement or representation contained in any notice or document. Custodian shall not be responsible for failure to act as a result of causes beyond the reasonable control of Custodian.

7.2 Indemnification. Depositor agrees to indemnify, defend and hold harmless Custodian from any and all claims, actions, damages, arbitration fees and expenses, costs, reasonable attorney's fees and other liabilities ("Liabilities") incurred by Custodian directly resulting from this escrow arrangement, except where it is adjudged that Custodian acted with gross negligence or willful misconduct.

7.3 Limitation of Liability and Waiver of Consequential Damages.

(a) Notwithstanding anything else herein, all liability, if any, whether arising in contract, tort (including negligence) or otherwise, of Custodian under this Agreement shall be limited to the amount equal to ten times the then annual fees owed or paid to Custodian under this Agreement. If claim or loss is made in relation to a specific deposit or deposits, such liability shall be limited to the fees related specifically to such deposits. This limit shall not apply for: (I) any claims of infringement of any patent, copyright, trademark or other proprietary right; (II) liability for death or bodily injury; (III) damage to tangible property (excluding the Deposit Material); (IV) theft; or (V) proven gross negligence or willful misconduct.

(b) In no event will Custodian be liable for any incidental, indirect, special, exemplary, punitive or consequential damages, including, but not limited to, damages (including loss of data, revenue, and/or profits) costs or expenses (including legal fees and expenses), whether arising in contract, tort (including negligence) or otherwise even if the possibility thereof may be known in advance to one or more parties and whether foreseeable or unforeseeable, that may arise out of or in connection with this Agreement.

7.4 Controlling Law. This Agreement is to be governed and construed in accordance with the laws of the State of Texas, without regard to its conflict of law provisions.

7.6 Notice of Requested Order. If any party intends to obtain an order from the arbitrator or any court of competent jurisdiction, which may direct Custodian to take, or refrain from taking any action, that party shall:

a. Give notice to Custodian at least five (5) business days prior to the hearing; and

b. Include in any such order that, as a precondition to Custodian's obligation, Custodian be paid in full for any past due fees and be paid for the reasonable value of the services to be rendered pursuant to such order.

ARTICLE 8 -- **GENERAL PROVISIONS**

8.1 Entire Agreement. This Agreement, which includes Exhibits described herein, embodies the entire understanding among the parties with respect to its subject matter and supersedes all previous communications, representations or understandings, either oral or written. Custodian is not a party to the License Agreement between Depositor and City and has no knowledge of any of the terms or provisions of any such License Agreement. Custodian's only obligations to Depositor or City are as set forth in this Agreement. No amendment or modification of this Agreement shall be valid or binding unless signed by all the parties hereto, except that Exhibit A need not be signed by Custodian, Exhibit B need not be signed by City and Exhibit C need not be signed.

8.2 Notices. All notices, invoices, payments, deposits and other documents and communications shall be given to the parties at the addresses specified in the attached Exhibit C. It shall be the responsibility of the parties to notify each other as provided in this Section in the event of a change of address. The parties shall have the right to rely on the last known address of the other parties. Any correctly addressed notice or last

known address of the other parties that is relied on herein that is refused, unclaimed, or undeliverable because of an act or omission of the party to be notified as provided herein shall be deemed effective as of the first date that said notice was refused, unclaimed, or deemed undeliverable by the postal authorities by registered mail, or through messenger or commercial express delivery services. Unless otherwise provided in this Agreement, all non-critical documents (such as invoices) and non-critical communications may be delivered by First Class mail.

8.3 Severability. In the event any provision of this Agreement is found to be invalid, voidable or unenforceable, the parties agree that unless it materially affects the entire intent and purpose of this Agreement, such invalidity, voidability or unenforceability shall affect neither the validity of this Agreement nor the remaining provisions herein, and the provision in question shall be deemed to be replaced with a valid and enforceable provision most closely reflecting the intent and purpose of the original provision.

8.4 Successors and Assigns. This Agreement shall be binding upon and shall inure to the benefit of the successors and assigns of the parties. However, Custodian shall have no obligation in performing this Agreement to recognize any successor or assign of Depositor or City unless Custodian receives clear, authoritative and conclusive written evidence of the change of parties.

8.5 Waiver. Any term of this Agreement may be waived by the party entitled to the benefits thereof, provided that any such waiver must be in writing and signed by the party against whom the enforcement of the waiver is sought. No waiver of any condition, or breach of any provision of this Agreement, in any one or more instances, shall be deemed to be a further or continuing waiver of such condition or breach. Delay or failure to exercise any right or remedy shall not be deemed the waiver of that right or remedy.

8.6 Regulations. Depositor and City are responsible for and warrant compliance with all applicable laws, rules and regulations, including but not limited to customs laws, import, export, and reexport laws and government regulations of any country from or to which the Deposit Materials may be delivered in accordance with the provisions of this Agreement.

8.7 Attorney's Fees. Each party shall be responsible for its own attorney fees to enforce this agreement.

8.8 No Third Party Rights. This Agreement is made solely for the benefit of the Parties to this Agreement and their respective permitted successors and assigns, and no other person or entity shall have or acquire any right by virtue of this Agreement unless otherwise agreed to by all the parties hereto.

8.9 Authority to Sign. Each of the Parties herein represents and warrants that the execution, delivery, and performance of this Agreement has been duly authorized and signed by a person who meets statutory or other binding approval to sign on behalf of its business organization as named in this Agreement.

8.10 Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be an original, but all of which together shall constitute one instrument.

_____	_____
Depositor	City
By:	By:
_____	
Name:	Name:
_____	_____
Title:	Title:
_____	_____
Date:	Date:
_____	_____

Custodian

By: _____

Name: _____

Title: _____

Date: _____

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

EXHIBIT 3-A

MATERIALS TO BE DEPOSITED

Account Number _____

Depositor represents to City that Deposit Materials delivered to Custodian shall consist of the following:

_____	_____
Depositor	City of San Antonio
By:	By:
_____	_____
Name:	Name:
_____	_____
Title:	Title:
_____	_____
Date:	Date:
_____	_____

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

EXHIBIT 3-B

DESCRIPTION OF DEPOSIT MATERIALS

Depositor Company Name _____

Account Number _____

Product Name _____

(Product Name will appear as the Exhibit B Name on Account History report)

DEPOSIT MATERIAL DESCRIPTION:

Quantity	Media Type & Size	Label Description of Each Separate Item
_____	Disk 3.5" or _____	
_____	DAT tape _____ mm	
_____	CD-ROM	
_____	Data cartridge tape _____	
_____	TK 70 or _____ tape	
_____	Magnetic tape _____	
_____	Documentation	
_____	Other _____	

PRODUCT DESCRIPTION:

Environment _____

DEPOSIT MATERIAL INFORMATION:

Is the media or are any of the files encrypted? If yes, please include any passwords and the decryption tools.

Encryption tool name_____ Version _____

Hardware required_____

Software required_____

Other required information_____

I certify for **Depositor** that the above described **Custodian** has accepted the above.	
Deposit Materials have been transmitted to Custodian: _____	
Materials	*(any exceptions are noted above)*:

INTERLOCAL PARTICIPATION

The City may, from time to time, enter into Interlocal Cooperation Purchasing Agreements with other governmental entities or governmental cooperatives (hereafter collectively referred to as “Entity” or “Entities”) to enhance the City’s purchasing power. At the City’s sole discretion and option, City may inform other Entities that they may acquire items listed in this Request for Offer (hereafter “RFCSP”). Such acquisition(s) shall be at the prices stated herein, and shall be subject to vendor’s acceptance. Entities desiring to acquire items listed in this RFCSP shall be listed on a rider attached hereto, if known at the time of issuance of the RFCSP. City may issue subsequent riders after contract award setting forth additional Entities desiring to utilize this contract. VENDOR shall sign and return any subsequently issued riders within ten calendar days of receipt.

In no event shall City be considered a dealer, remarketer, agent or other representative of Vendor or Entity. Further, City shall not be considered and is not an agent; partner or representative of the Entity making purchases hereunder, and shall not be obligated or liable for any such order.

Entity purchase orders shall be submitted to Vendor by the Entity.

Vendor authorizes City’s use of Vendor’s name, trademarks and Vendor provided materials in City’s presentations and promotions regarding the availability of use of this contract. The City makes no representation or guarantee as to any minimum amount being purchased by City or Entities, or whether Entity will purchase utilizing City’s contract.

CITY WILL NOT BE LIABLE OR RESPONSIBLE FOR ANY OBLIGATIONS, INCLUDING, BUT NOT LIMITED TO, PAYMENT, AND FOR ANY ITEM ORDERED BY AN ENTITY OTHER THAN CITY.

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

RFCSP EXHIBIT 5

SMALL BUSINESS ECONOMIC DEVELOPMENT ADVOCACY (SBEDA) PROGRAM

A. Solicitation Response and Contract Requirements and Commitment

Respondent understands and agrees that the following provisions shall be requirements of this solicitation and the resulting contract, if awarded, and by submitting its Response, Respondent commits to comply with these requirements. In the absence of a waiver granted by the SBO, failure of a Prime Contractor to commit in its response, through fully-documented and signed SBO-promulgated Subcontractor/Supplier Utilization Plan form, to satisfying the SBE subcontracting goal shall render its response NON-RESPONSIVE. [*****NOTE:** The following provisions shall only be added to the solicitation document {BUT NOT THE CONTRACT.]

Exception Request - A Respondent may, for good cause, request an Exception to the application of the SBEDA Program if the Respondent submits the *Exception to SBEDA Program Requirements Request* form *(available at http://www.sanantonio.gov/SBO/Forms.aspx)* with its solicitation response. The Respondent's Exception request must fully document why: (1) the value of the contract is below the $50,000 threshold for application of the SBEDA Program; or (2) no commercially-useful subcontracting opportunities exist within the contract scope of work; or (3) the type of contract is outside of the scope of the SBEDA Ordinance. **Late Exception Requests will not be considered.**

Include the following provisions to the solicitation document and resulting contract:

B. SBEDA Program

The CITY has adopted a Small Business Economic Development Advocacy Ordinance (Ordinance No. 2010-06-17-0531 and as amended, also referred to as "SBEDA" or "the SBEDA Program"), which is posted on the City's Economic Development (EDD) website page and is also available in hard copy form upon request to the CITY. The SBEDA Ordinance Compliance Provisions contained in this section of the Agreement are governed by the terms of this Ordinance, as well as by the terms of the SBEDA Ordinance Policy & Procedure Manual established by the CITY pursuant to this Ordinance, and any subsequent amendments to this referenced SBEDA Ordinance and SBEDA Policy & Procedure Manual that are effective as of the date of the execution of this Agreement. Unless defined in a contrary manner herein, terms used in this section of the Agreement shall be subject to the same expanded definitions and meanings as given those terms in the SBEDA Ordinance and as further interpreted in the SBEDA Policy & Procedure Manual.

C. Definitions

Affirmative Procurement Initiatives (API) – Refers to various Small Business Enterprise, Minority Business Enterprise, and/or Women Business Enterprise ("S/M/WBE") Program tools and Solicitation Incentives that are used to encourage greater Prime and subcontract participation by S/M/WBE firms, including bonding assistance, evaluation preferences, subcontracting goals and joint venture incentives. (For full descriptions of these and other S/M/WBE program tools, see Section III. D. of Attachment A to the SBEDA Ordinance.)

Certification or "Certified" – the process by which the Small Business Office (SBO) staff determines a firm to be a bona-fide small, minority-, women-owned, or emerging small business enterprise. Emerging Small Business Enterprises (ESBEs) are automatically eligible for Certification as SBEs. Any firm may apply for multiple Certifications that cover each and every status category (e.g., SBE, ESBE, MBE, or WBE) for which it is able to satisfy eligibility standards. The SBO staff may contract these services to a regional Certification agency or other entity. For purposes of Certification, the City accepts any firm that is certified by local government entities and other organizations identified herein that have adopted Certification standards and procedures similar to those followed by the SBO, provided the prospective firm satisfies the eligibility requirements set forth in this Ordinance in Section III.E.6 of Attachment A.

Centralized Vendor Registration System (CVR) – a mandatory electronic system wherein the City requires all prospective Respondents and Subcontractors that are ready, willing and able to sell goods or services to the City to register. The CVR system assigns a unique identifier to each registrant that is then required for the purpose of submitting solicitation responses and invoices, and for receiving payments from the City. The CVR-assigned identifiers are also used

by the Goal Setting Committee for measuring relative availability and tracking utilization of SBE and M/WBE firms by Industry or commodity codes, and for establishing Annual Aspirational Goals and Contract-by-Contract Subcontracting Goals.

Commercially Useful Function – an S/M/WBE firm performs a Commercially Useful Function when it is responsible for execution of a distinct element of the work of the contract and is carrying out its responsibilities by actually performing, staffing, managing and supervising the work involved. To perform a Commercially Useful Function, the S/M/WBE firm must also be responsible, with respect to materials and supplies used on the contract, for negotiating price, determining quantity and quality, ordering the material, and installing (where applicable) and paying for the material itself. To determine whether an S/M/WBE firm is performing a Commercially Useful Function, an evaluation must be performed of the amount of work subcontracted, normal industry practices, whether the amount the S/M/WBE firm is to be paid under the contract is commensurate with the work it is actually performing and the S/M/WBE credit claimed for its performance of the work, and other relevant factors. Specifically, an S/M/WBE firm does not perform a Commercially Useful Function if its role is limited to that of an extra participant in a transaction, contract or project through which funds are passed in order to obtain the appearance of meaningful and useful S/M/WBE participation, when in similar transactions in which S/M/WBE firms do not participate, there is no such role performed. The use of S/M/WBE firms by CONTRACTOR to perform such "pass-through" or "conduit" functions that are <u>not</u> commercially useful shall be viewed by the CITY as fraudulent if CONTRACTOR attempts to obtain credit for such S/M/WBE participation towards the satisfaction of S/M/WBE participation goals or other API participation requirements. As such, under such circumstances where a commercially useful function is not actually performed by the S/M/WBE firm, the CONTRACTOR shall not be given credit for the participation of its S/M/WBE subcontractor or joint venture partner towards attainment of S/M/WBE utilization goals, and the CONTRACTOR and S/M/WBE firm may be subject to sanctions and penalties in accordance with the SBEDA Ordinance.

Evaluation Preference – an API that may be applied by the Goal Setting Committee ("GSC") to Construction, Architectural & Engineering, Professional Services, Other Services, and Goods and Supplies contracts that are to be awarded on a basis that includes factors other than lowest price, and wherein responses that are submitted to the City by S/M/WBE firms may be awarded additional Points in the evaluation process in the scoring and ranking of their proposals against those submitted by other prime CONTRACTORs or Respondents.

Good Faith Efforts – documentation of the CONTRACTOR's or Respondent's intent to comply with S/M/WBE Program Goals and procedures including, but not limited to, the following: (1) documentation within a solicitation response reflecting the Respondent's commitment to comply with SBE or M/WBE Program Goals as established by the GSC for a particular contract; or (2) documentation of efforts made toward achieving the SBE or M/WBE Program Goals (e.g., timely advertisements in appropriate trade publications and publications of wide general circulation; timely posting of SBE or M/WBE subcontract opportunities on the City of San Antonio website; solicitations of bids/proposals/qualification statements from all qualified SBE or M/WBE firms listed in the Small Business Office's directory of certified SBE or M/WBE firms; correspondence from qualified SBE or M/WBE firms documenting their unavailability to perform SBE or M/WBE contracts; documentation of efforts to subdivide work into smaller quantities for subcontracting purposes to enhance opportunities for SBE or M/WBE firms; documentation of a Prime Contractor's posting of a bond covering the work of SBE or M/WBE Subcontractors; documentation of efforts to assist SBE or M/WBE firms with obtaining financing, bonding or insurance required by the Respondent; and documentation of consultations with trade associations and consultants that represent the interests of SBE and/or M/WBEs in order to identify qualified and available SBE or M/WBE Subcontractors.) The appropriate form and content of CONTRACTOR's Good Faith Efforts documentation shall be in accordance with the SBEDA Ordinance as interpreted in the SBEDA Policy & Procedure Manual.

HUBZone Firm − a business that has been certified by U.S. Small Business Administration for participation in the federal HUBZone Program, as established under the 1997 Small Business Reauthorization Act. To qualify as a HUBZone firm, a small business must meet the following criteria: (1) it must be owned and Controlled by U.S. citizens; (2) at least 35 percent of its employees must reside in a HUBZone; and (3) its Principal Place of Business must be located in a HUBZone within the San Antonio Metropolitan Statistical Area. [See 13 C.F.R. 126.200 (1999).]

Independently Owned and Operated – ownership of an SBE firm must be direct, independent and by Individuals only. Ownership of an M/WBE firm may be by Individuals and/or by other businesses provided the ownership interests in the M/WBE firm can satisfy the M/WBE eligibility requirements for ownership and Control as specified herein in Section III.E.6. The M/WBE firm must also be Independently Owned and Operated in the sense that it cannot be the subsidiary of another firm that does not itself (and in combination with the certified M/WBE firm) satisfy the eligibility requirements for M/WBE Certification.

Individual − an adult person that is of legal majority age.

Industry Categories – procurement groupings for the City of San Antonio inclusive of Construction, Architectural & Engineering (A&E), Professional Services, Other Services, and Goods & Supplies (i.e., manufacturing, wholesale and retail distribution of commodities). This term may sometimes be referred to as "business categories."

Minority/Women Business Enterprise (M/WBE) – firm that is certified as a Small Business Enterprise and also as either a Minority Business Enterprise or as a Women Business Enterprise, and which is at least fifty-one percent (51%) owned, managed and Controlled by one or more Minority Group Members and/or women, and that is ready, willing and able to sell goods or services that are purchased by the City of San Antonio.

M/WBE Directory – a listing of minority- and women-owned businesses that have been certified for participation in the City's M/WBE Program APIs.

Minority Business Enterprise (MBE) – any legal entity, except a joint venture, that is organized to engage in for-profit transactions, which is certified a Small Business Enterprise and also as being at least fifty-one percent (51%) owned, managed and controlled by one or more Minority Group Members, and that is ready, willing and able to sell goods or services that are purchased by the CITY. To qualify as an MBE, the enterprise shall meet the Significant Business Presence requirement as defined herein. Unless otherwise stated, the term "MBE" as used in this Ordinance is not inclusive of women-owned business enterprises (WBEs).

Minority Group Members – African-Americans, Hispanic Americans, Asian Americans and Native Americans legally residing in, or that are citizens of, the United States or its territories, as defined below:

> African-Americans: Persons having origins in any of the black racial groups of Africa as well as those identified as Jamaican, Trinidadian, or West Indian.
>
> Hispanic-Americans: Persons of Mexican, Puerto Rican, Cuban, Spanish or Central and South American origin.
>
> Asian-Americans: Persons having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent or the Pacific Islands.
>
> Native Americans: Persons having no less than $1/16^{th}$ percentage origin in any of the Native American Tribes, as recognized by the U.S. Department of the Interior, Bureau of Indian Affairs and as demonstrated by possession of personal tribal role documents.

Originating Department – the CITY department or authorized representative of the CITY which issues solicitations or for which a solicitation is issued.

Payment – dollars actually paid to CONTRACTORS and/or Subcontractors and vendors for CITY contracted goods and/or services.

Points – the quantitative assignment of value for specific evaluation criteria in the vendor selection process used in some Construction, Architectural & Engineering, Professional Services, and Other Services contracts (e.g., up to 10 points out of a total of 100 points assigned for S/M/WBE participation as stated in response to a Request for Proposals).

Prime Contractor – the vendor or contractor to whom a purchase order or contract is issued by the City of San Antonio for purposes of providing goods or services for the City. For purposes of this agreement, this term refers to the CONTRACTOR.

Relevant Marketplace – the geographic market area affecting the S/M/WBE Program as determined for purposes of collecting data for the MGT Studies, and for determining eligibility for participation under various programs established by the SBEDA Ordinance, is defined as the San Antonio Metropolitan Statistical Area (SAMSA), currently including the counties of Atascosa, Bandera, Bexar, Comal, Guadalupe, Kendall, Medina and Wilson.

Respondent – a vendor submitting a bid, statement of qualifications, or proposal in response to a solicitation issued by the City. For purposes of this agreement, CONTRACTOR is the Respondent.

Responsible – a firm which is capable in all respects to fully perform the contract requirements and has the integrity and reliability which will assure good faith performance of contract specifications.

Responsive – a firm's submittal (bid, response or proposal) conforms in all material respects to the solicitation (Invitation for Bid, Request for Qualifications, or Request for Proposal) and shall include compliance with S/M/WBE Program requirements.

San Antonio Metropolitan Statistical Area (SAMSA) – also known as the Relevant Marketplace, the geographic market area from which the CITY's MGT Studies analyzed contract utilization and availability data for disparity (currently including the counties of Atascosa, Bandera, Bexar, Comal, Guadalupe, Kendall, Medina and Wilson).

SBE Directory - a listing of small businesses that have been certified for participation in the City's SBE Program APIs.

Significant Business Presence – to qualify for this Program, a S/M/WBE must be headquartered or have a *significant business presence* for at least one year within the Relevant Marketplace, defined as: an established place of business in one or more of the eight counties that make up the San Antonio Metropolitan Statistical Area (SAMSA), from which 20% of its full-time, part-time and contract employees are regularly based, and from which a substantial role in the S/M/WBE's performance of a Commercially Useful Function is conducted. A location utilized solely as a post office box, mail drop or telephone message center or any combination thereof, with no other substantial work function, shall not be construed to constitute a significant business presence.

Small Business Enterprise (SBE) – a corporation, partnership, sole proprietorship or other legal entity for the purpose of making a profit, which is Independently Owned and Operated by Individuals legally residing in, or that are citizens of, the United States or its territories, and which meets the U.S. Small Business Administration (SBA) size standard for a small business in its particular industry(ies) and meets the Significant Business Presence requirements as defined herein.

Small Business Office (SBO) – the office within the Economic Development Department (EDD) of the CITY that is primarily responsible for general oversight and administration of the S/M/WBE Program.

Small Business Office Manager – the Assistant Director of the EDD of the CITY that is responsible for the management of the SBO and ultimately responsible for oversight, tracking, monitoring, administration, implementation and reporting of the S/M/WBE Program. The SBO Manager is also responsible for enforcement of contractor and vendor compliance with contract participation requirements, and ensuring that overall Program goals and objectives are met.

Small Minority Women Business Enterprise Program (S/M/WBE Program) – the combination of SBE Program and M/WBE Program features contained in the SBEDA Ordinance.

Subcontractor – any vendor or contractor that is providing goods or services to a Prime Contractor or CONTRACTOR in furtherance of the Prime Contractor's performance under a contract or purchase order with the City. A copy of each binding agreement between the CONTRACTOR and its subcontractors shall be submitted to the CITY prior to execution of this contract agreement and any contract modification agreement.

Suspension – the temporary stoppage of the SBE or M/WBE firm's beneficial participation in the CITY's S/M/WBE Program for a finite period of time due to cumulative contract payments the S/M/WBE firm received during a fiscal year that exceed a certain dollar threshold as set forth in Section III.E.7 of Attachment A to the SBEDA Ordinance, or the temporary stoppage of CONTRACTOR's and/or S/M/WBE firm's performance and payment under CITY contracts due to the CITY's imposition of Penalties and Sanctions set forth in Section III.E.13 of Attachment A to the SBEDA Ordinance.

Subcontractor/Supplier Utilization Plan – a binding part of this contract agreement which states the CONTRACTOR's commitment for the use of Joint Venture Partners and / or Subcontractors/Suppliers in the performance of this contract agreement, and states the name, scope of work, and dollar value of work to be performed by each of CONTRACTOR's Joint Venture partners and Subcontractors/Suppliers in the course of the performance of this contract, specifying the S/M/WBE Certification category for each Joint Venture partner and Subcontractor/Supplier, as approved by the SBO Manager. Additions, deletions or modifications of the Joint Venture partner or Subcontractor/Supplier names, scopes of work, of dollar values of work to be performed requires an amendment to this agreement to be approved by the EDD Director or designee.

Women Business Enterprises (WBEs) - any legal entity, except a joint venture, that is organized to engage in for-profit transactions, that is certified for purposes of the SBEDA Ordinance as being a Small Business Enterprise and that is at least fifty-one percent (51%) owned, managed and Controlled by one or more non-minority women Individuals that are lawfully residing in, or are citizens of, the United States or its territories, that is ready, willing and able to sell goods or services that are purchased by the City and that meets the Significant Business Presence requirements as defined herein. Unless otherwise stated, the term "WBE" as used in this Agreement is not inclusive of MBEs.

D. <u>SBEDA Program Compliance – General Provisions</u>

As CONTRACTOR acknowledges that the terms of the CITY's SBEDA Ordinance, as amended, together with all requirements, guidelines, and procedures set forth in the CITY's SBEDA Policy & Procedure Manual are in furtherance of the CITY's efforts at economic inclusion and, moreover, that such terms are part of CONTRACTOR's scope of work as referenced in the CITY's formal solicitation that formed the basis for contract award and subsequent execution of this Agreement, these SBEDA Ordinance requirements, guidelines and procedures are hereby incorporated by reference into this Agreement, and are considered by the Parties to this Agreement to be material terms. CONTRACTOR voluntarily agrees to fully comply with these SBEDA program terms as a condition for being awarded this contract by the CITY. Without limitation, CONTRACTOR further agrees to the following terms as part of its contract compliance responsibilities under the SBEDA Program:

1. CONTRACTOR shall cooperate fully with the Small Business Office and other CITY departments in their data collection and monitoring efforts regarding CONTRACTOR's utilization and payment of Subcontractors, S/M/WBE firms, and HUBZone firms, as applicable, for their performance of Commercially Useful Functions on this contract including, but not limited to, the timely submission of completed forms and/or documentation promulgated by SBO, through the Originating Department, pursuant to the SBEDA Policy & Procedure Manual, timely entry of data into monitoring systems, and ensuring the timely compliance of its Subcontractors with this term;

2. CONTRACTOR shall cooperate fully with any CITY or SBO investigation (and shall also respond truthfully and promptly to any CITY or SBO inquiry) regarding possible non-compliance with SBEDA requirements on the part of CONTRACTOR or its Subcontractors or suppliers;

3. CONTRACTOR shall permit the SBO, upon reasonable notice, to undertake inspections as necessary including, but not limited to, contract-related correspondence, records, documents, payroll records, daily logs, invoices, bills, cancelled checks, and work product, and to interview Subcontractors and workers to determine whether there has been a violation of the terms of this Agreement;

4. CONTRACTOR shall immediately notify the SBO, in writing on the Change to Utilization Plan form, through the Originating Department, of any proposed changes to CONTRACTOR's Subcontractor / Supplier Utilization Plan for this contract, with an explanation of the necessity for such proposed changes, including documentation of Good Faith Efforts made by CONTRACTOR to replace the Subcontractor / Supplier in accordance with the applicable Affirmative Procurement Initiative. All proposed changes to the Subcontractor / Supplier Utilization Plan including, but not limited to, proposed self-performance of work by CONTRACTOR of work previously designated for performance by Subcontractor or supplier, substitutions of new Subcontractors, terminations of previously designated Subcontractors, or reductions in the scope of work and value of work awarded to Subcontractors or suppliers, shall be subject to advanced written approval by the Originating Department and the SBO.

5. CONTRACTOR shall immediately notify the Originating Department and SBO of any transfer or assignment of its contract with the CITY, as well as any transfer or change in its ownership or business structure.

6. CONTRACTOR shall retain all records of its Subcontractor payments for this contract for a minimum of four years or as required by state law, following the conclusion of this contract or, in the event of litigation concerning this contract, for a minimum of four years or as required by state law following the final determination of litigation, whichever is later.

7. In instances wherein the SBO determines that a Commercially Useful Function is not actually being performed by the applicable S/M/WBE or HUBZone firms listed in a CONTRACTOR's Subcontractor / Supplier Utilization Plan, the CONTRACTOR shall not be given credit for the participation of its S/M/WBE or HUBZone subcontractor(s) or joint venture partner(s) toward attainment of S/M/WBE or HUBZone firm utilization goals, and the CONTRACTOR and its listed S/M/WBE firms or HUBZone firms may be subject to sanctions and penalties in accordance with the SBEDA Ordinance.

8. CONTRACTOR acknowledges that the CITY will not execute a contract or issue a Notice to Proceed for this project until the CONTRACTOR and each of its Subcontractors for this project have registered and/or maintained active status in the CITY's Centralized Vendor Registration System, and CONTRACTOR has represented to CITY which primary commodity codes each registered Subcontractor will be performing under for this contract.

E. SBEDA Program Compliance – Affirmative Procurement Initiatives

The CITY has applied the following contract-specific Affirmative Procurement Initiatives to this contract. CONTRACTOR hereby acknowledges and agrees that the selected API requirement shall also be extended to any change order or subsequent contract modification and, absent SBO's granting of a waiver, that its full compliance with the following API terms and conditions are material to its satisfactory performance under this Agreement:

SBE Prime Contract Program. In accordance with the SBEDA Ordinance, Section III. D. 9. (c), this contract is being awarded pursuant to the SBE Prime Contract Program, and as such, CONTRACTOR affirms that if it is presently certified as an SBE, CONTRACTOR agrees not to subcontract more than 49% of the contract value to a non-SBE firm.

F. Commercial Nondiscrimination Policy Compliance

As a condition of entering into this Agreement, the CONTRACTOR represents and warrants that it has complied with throughout the course of this solicitation and contract award process, and will continue to comply with, the CITY's Commercial Nondiscrimination Policy, as described under Section III. C. 1. of the SBEDA Ordinance. As part of such compliance, CONTRACTOR shall not discriminate on the basis of race, color, religion, ancestry or national origin, sex, age, marital status, sexual orientation or, on the basis of disability or other unlawful forms of discrimination in the solicitation, selection, hiring or commercial treatment of Subcontractors, vendors, suppliers, or commercial customers, nor shall the company retaliate against any person for reporting instances of such discrimination. The company shall provide equal opportunity for Subcontractors, vendors and suppliers to participate in all of its public sector and private sector subcontracting and supply opportunities, provided that nothing contained in this clause shall prohibit or limit otherwise lawful efforts to remedy the effects of marketplace discrimination that have occurred or are occurring in the CITY's Relevant Marketplace. The company understands and agrees that a material violation of this clause shall be considered a material breach of this Agreement and may result in termination of this Agreement, disqualification of the company from participating in CITY contracts, or other sanctions. This clause is not enforceable by or for the benefit of, and creates no obligation to, any third party. CONTRACTOR's certification of its compliance with this Commercial Nondiscrimination Policy as submitted to the CITY pursuant to the solicitation for this contract is hereby incorporated into the material terms of this Agreement. CONTRACTOR shall incorporate this clause into each of its Subcontractor and supplier agreements entered into pursuant to CITY contracts.

G. Prompt Payment

Upon execution of this contract by CONTRACTOR, CONTRACTOR shall be required to submit to CITY accurate progress payment information with each invoice regarding each of its Subcontractors, including HUBZone Subcontractors, to ensure that the CONTRACTOR's reported subcontract participation is accurate. CONTRACTOR shall pay its Subcontractors in compliance with Chapter 2251, Texas Government Code (the "Prompt Payment Act") within ten days of receipt of payment from CITY. In the event of CONTRACTOR's noncompliance with these prompt payment provisions, no final retainage on the Prime Contract shall be released to CONTRACTOR, and no new CITY contracts shall be issued to the CONTRACTOR until the CITY's audit of previous subcontract payments is complete and payments are verified to be in accordance with the specifications of the contract.

H. Violations, Sanctions and Penalties

In addition to the above terms, CONTRACTOR acknowledges and agrees that it is a violation of the SBEDA Ordinance and a material breach of this Agreement to:

1. Fraudulently obtain, retain, or attempt to obtain, or aid another in fraudulently obtaining, retaining, or attempting to obtain or retain Certification status as an SBE, MBE, WBE, M/WBE, HUBZone firm, Emerging M/WBE, or ESBE for purposes of benefitting from the SBEDA Ordinance;

2. Willfully falsify, conceal or cover up by a trick, scheme or device, a material fact or make any false, fictitious or fraudulent statements or representations, or make use of any false writing or document, knowing the same to contain any false, fictitious or fraudulent statement or entry pursuant to the terms of the SBEDA Ordinance;

3. Willfully obstruct, impede or attempt to obstruct or impede any authorized official or employee who is investigating the qualifications of a business entity which has requested Certification as an S/M/WBE or HUBZone firm;

4. Fraudulently obtain, attempt to obtain or aid another person fraudulently obtaining or attempting to obtain public monies to which the person is not entitled under the terms of the SBEDA Ordinance; and

5. Make false statements to any entity that any other entity is, or is not, certified as an S/M/WBE for purposes of the SBEDA Ordinance.

Any person who violates the provisions of this section shall be subject to the provisions of Section III. E. 13. of the SBEDA Ordinance and any other penalties, sanctions and remedies available under law including, but not limited to:

1. Suspension of contract;

2. Withholding of funds;

3. Rescission of contract based upon a material breach of contract pertaining to S/M/WBE Program compliance;

4. Refusal to accept a response or proposal; and

5. Disqualification of CONTRACTOR or other business firm from eligibility for providing goods or services to the City for a period not to exceed two years (upon City Council approval).

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

RFCSP EXHIBIT 6

CITY TECHNICAL STANDARDS

FOLLOW ON DOCUMENT ATTACHED AS SEPARATE DOCUMENT

City of San Antonio
Information Technology Environment Description

The City of San Antonio Information Technology Services Department (ITSD) will provide computing and infrastructure services for the selected hardware and software solution in one or both of two datacenters that are currently in operation. The two datacenters are interconnected by redundant high-speed Dense Wavelength Division Multiplexing (DWDM) links with servers and storage hosted in both environments. ITSD will manage the Data Center Layer, Networking Layer, Device Layer, Operating System Layer, and Application Infrastructure Layer for the information technology components of the proposed System in accordance with a SLA to be jointly developed by ITSD, the system provider, and the business owner of the System. Management of the Application Layer (business logic) will be determined by SLA.

To the extent that information technology equipment necessary to support the System must be deployed outside of the City's managed datacenter environment, the respondent must include in their response the scope necessary to provide appropriate environmental and compliance controls for the proposed System.

THE REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Information Management

***S=*Standard* Product(s), P=*Preferred* Product(s), G=*Guidance* Info Only.**

If the Information Technology Standards & Guidelines does not address a specific technical area, the user should seek guidance from the Director, Information Technology.

Information Management: Section 1	**Policy or Product**	S/P/G *	**Remarks**
Directory Services	Microsoft Server 2008 R2 Active Directory	S	The City is currently evaluating LDAP-based alternatives
Enterprise Backup	Symantec NetBackup 7.x	S	The City does not utilize tape media for backups The City uses a disk based backup solution for all backup operations.
Relational Database Management Systems	Oracle 11.2.x MS SQLServer 2008 Oracle 11.2.x MS SQLServer 2008	P S G	Enterprise and large-scale systems with high capacity, complex design and/or high volume transactional requirements Mid-scale systems with moderate capacity and/or transactional volume requirements
Database Access	SQL*Plus OCI-compliant client ODBC	S G G	
File Formats	IT guidance	G	Follow IT guidance for recommended file extensions
Data Administration Implementation	IT guidance	G	IT is currently evaluating the use of tools in this area
Data Warehousing and Mining	SAP BI 7.01 / NW 7.01 (EHP1) non-unicode / SP16	S	For SAP-based data
Messaging	Microsoft Exchange 2007 SP3	S	
Presentation and Interface Standards • Application Standard Interfaces • Mobile Devices	 Web Services: .Net 3.5 or higher Web Applications: .Net 4.0 or higher API	 P P G G	 Follow IT guidance

Information Distribution

***S=*Standard* Product(s), P=*Preferred* Product(s), G=*Guidance* Information Only**

If the Information Technology Standards and Guidelines policy does not address a specific technical area, the user should seek guidance from the Director, Information Technology.

Information Distribution: Section 2	**Policy or Product**	S/P/G *	**Remarks**
E-Mail with Attachments			
• SMTP	MS Exchange with outbound SMTP	S,G	See IT for guidance
• Active Sync	Supported for use with smartphones and mobile devices	G	See IT for guidance
File Transfer Service			
• HTTPS		S	
• SFTP	SFTP Client (Core FTP LE 2.1 or higher)	S	

Applications

***S=*Standard* Product(s), P=*Preferred* Product(s), G=*Guidance* Information Only**

If the Information Technology Standards and Guidelines policy does not address a specific technical area, the user should seek guidance from the Director, Information Technology.

Applications: Section 3	**Policy or Product**	S/P/G *	**Remarks**
Enterprise Resource Planning	SAP ECC6 / EHP7 / NW 7.01 (EHP1) non-unicode / SP5	S	• Production implementation date was April 2004. • ECC6 upgrade completed April 2009. • SAP Enterprise Portal completed 2010 Core modules include: HR FI MM SD PS PM GM The application is accessible from any site or client VPN within the corporate network Current access methods include: client server run-time objects, Citrix, and SAP Enterprise Portal.
Procurement	SAP SRM 7.0 / NW 7.01 (EHP1) unicode / SP14	S	SAP Enterprise Portal completed 2010 Current access methods include: client server run-time objects, Citrix, and SAP Enterprise Portal.
Document Management	FileNet P8 v4.5.x	S	The City has plans to upgrade to v5.1 in 2015
Cooperative Work Applications			
• Collaborative Processing (internal use only)	MS Exchange 2007 MS SharePoint 2003	S	
• Workflow	SAP IBM FileNet	G G	See IT for guidance
• External File Sharing	Globalscape EFT Server	S	
Content Management	FileNet P8 v4.5.x	G	See IT for guidance
Web Server	IIS 7.0	S	
Web Content Management	DotNetNuke Enterprise Edition 7.0.x	S	

Applications: Section 3	**Policy or Product**	S/P/G *	**Remarks**
Web Portal	Citrix XenApp 5.0 DotNetNuke Enterprise Edition 7.0.x	P,G G	 See IT for guidance
Office Automation	MS Office 2007 MS Internet Explorer 9 MS Internet Explorer 10 Firefox 15.x (or higher) Safari 6.x (or higher) Chrome 22.x (or higher) MS Outlook 2007 Adobe Reader 10.x MS Project 2007 MS Visio 2007 Std.	S S,G P S,G S,G S,G S S G G	Excludes MS Access See IT for guidance on “extensions” See IT for guidance
GIS Mapping	ESRI ArcGIS Desktop v10.x ESRI ArcGIS Server v10.x ESRI ArcSDE v10.x	S S S	Using Windows OS Using IIS with SSL if external Using MS SQL Server
GIS Web Development	MS Visual Studio 2013	S	
Web Development Tools	MS Visual Studio 2013 MS Visual Studio 2010 MS Visual Studio 2008	S G G	Follow IT guidance in extending legacy systems to the Web and Service-Oriented Architecture
Digital Signature	Pending	G	
Application Development Tools	MS Visual Studio 2013 Netweaver 7.x PL SQL	S S S	Follow IT guidance for configuration
Application Integration	Web Services Netweaver XI 7.11 SP13	S G	Follow IT guidance
Report Writers	Business Objects 3.1 Crystal Reports 2008 Xcelsius Dashboards	S G G	Follow IT guidance for data integrity and access

Computing Resources

***S=*Standard* Product(s), P=*Preferred* Product(s), G=*Guidance* Information Only**

If the Information Technology Standards and Guidelines policy does not address a specific technical area, the user should seek guidance from the Director, Information Technology.

Computing Resources: Section 4	**Policy or Product**	S/P/G *	**Remarks**
Workstation • Tier 1 • Tier 2 • Tier 3	 2.5GHz Intel Core i5 Two 2.5GHz Intel Core i7 	 S P G	In general, current IT standards provide a minimum baseline. IT will provision best value desktops that efficiently support the Refresh Policy. For specialized requirements seek IT guidance
Bus Standards	PCI	G	
Memory (RAM) Standards (EDO, SDRAM, DRAM) • Tier 1 • Tier 2 • Tier 3	 4GB 6GB 8GB (or higher)	 S P G	In general, current IT standards provide a minimum baseline. IT will provision best value desktops that efficiently support the Refresh Policy. For specialized requirements seek IT guidance
Server Hardware Configuration	SUN SPARC64 VI UltraSPARC T1 AMD Opteron Intel Xeon	P S	Solaris Database Server: M5000 Solaris Application Server: M4000, Blade 6000 Windows: 8 core Xeon E5-2665 (or higher) Processor, 20MB Cache, 2.40GHz (or higher), 1600 MHz FSB Virtual Hosts: Cisco UCS w/B-Series Blade Servers
Virtual Server Environment	VMWare Vsphere 5.1	S	The City uses a virtualization first approach when provisioning servers.
Mainframe Environment	IBM z890 z/OS 1.10 Software AG Natural 4.2.4 Software AG Adabas 8.1.4	G	The IBM z-series mainframe platform is being twilighted by the City
Disk Storage	FC SAN (HDS, Cisco) iSCSI (HDS, Nimble) NTFS ZFS CIFS/SMB (HDS\BlueArc)	S S S S S	IT guidance for application specific requirements
Workstation Operating Systems	Windows 7 SP1 Mac OSX 10.x	S G	

Computing Resources: Section 4	**Policy or Product**	S/P/G *	**Remarks**
Server Operating Systems			
• General File & Print Servers	Windows Server 2008	S	
• Application Servers	Windows Server 2008	S	
	Windows Server 2008 R2	P	
	Windows Server 2008 EE	G	Follow IT guidance
	Windows Server 2012	G	
	Solaris 10 Zones	S	
	Solaris 10	G	
• Database Servers	Windows Server 2008	S	
	Solaris 10	P	
Telephony			
• IVR	Cisco Unified Communications Manager 9.1.x	P	
• VoIP	Cisco	S	
• ACD	Cisco	S	

RFCSP EXHIBIT 7

CITY SECURITY POLICIES

FOLLOW ON DOCUMENT ATTACHED AS SEPARATE DOCUMENT

CITY OF SAN ANTONIO

Administrative Directive	**7.3a Data Security**
Procedural Guidelines	Regarding the use of Public and Confidential Data
Department/Division	Information Technology Services Department (ITSD)
Effective Date	April 1, 2014
Originator	Patsy Boozer, CISO

Purpose

This Administrative Directive (AD) provides guidance for compliance, confidentiality, privacy, security, and the associated governance for City of San Antonio's (COSA) three data categories of confidential, agency-sensitive, and public. Data must be classified into one of the three categories when stored, processed, or transmitted on COSA resources or other resources where COSA business occurs. This AD establishes and identifies responsibility for such data and provides a framework for maintaining compliance with applicable laws, regulations, and/or standards. Security standards, which define these security controls, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures. This directive supersedes the provisions of AD 7.3.

Overview

This directive establishes guidance for developing, maintaining, publishing, and administering comprehensive data governance and information technology system security. This directive references applicable local, state, and federal codes, directives, laws, ordinances, and/or statutes among other regulations.

Departmental data owners are responsible for the classification and protection of data under this directive. Precautions shall be taken to reasonably assure the confidentiality, integrity and availability of the protected data. Access to protected data shall be based on legitimate business need. COSA data shall be disseminated in accordance with this directive.

Policy

Adherence to this directive will help reasonably assure the confidentiality, integrity, and availability of COSA data:

- COSA data shall be classified as public, agency-sensitive, or confidential
- Baseline security controls for COSA Information Systems shall be based on the data owner's data classification as governed by this directive
- The National Institute of Standards and Technology (NIST) 800-53a Security and Privacy Controls has been adopted by COSA to provide a data protection framework for maintaining the confidentiality, integrity and availability of data.

Applicability

This directive applies to:

- All data processed, stored and/or transmitted by a COSA Information Technology System(s).
- All COSA data processed, stored and/or transmitted on personally-owned devices also referred to as "Bring Your Own Device" (BYOD).
- All data collected or maintained by or on behalf of COSA in any form (electronic or hardcopy).

Policy Applies To

☒ External & Internal Applicants	☒ Current Temporary Employees
☒ Current Full-Time Employees	☒ Current Volunteers
☒ Current Part-Time Employees	☒ Current Grant-Funded Employees
☒ Current Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	☒ Vendors, Contractors and Other Third Parties

Roles and Responsibilities

1. COSA departmental data owners are responsible for data classification and identification of data protection requirements.
2. All applicable parties as defined above have the responsibility of protecting COSA data.
3. COSA Information Technology Services Department (ITSD) is responsible for publishing, disseminating, and maintaining this directive.

Data Classification and Open Records

All data shall be classified as public, agency-sensitive, or confidential for the purpose of establishing dissemination guidelines and protective security measures. AD 1.31 Open Records (Texas Public Information Act) places responsibility for developing and updating the Municipal Open Records Policy with The City Attorney's Office. This requirement includes any response to Open Record Requests (ORR) whether the records are or are not public under the Open Records/Texas Public Information Act of 1993. All open records shall be reviewed by the department data owners prior to dissemination to reasonably assure that open records do not contain confidential data or sensitive Personally Identifiable Information (PII).

1. *Confidential Data*
   - Confidential data is specifically exempted from federal regulation(s) and/or Texas Open Record Law and other constitutional, statutory, judicial, and legal agreements.
   - This type of data may not be freely disseminated. As mandated by local, state and federal statutes, ordinances, directives and/or court orders, distribution and dissemination of this data is restricted.
   - Confidential data requires the highest level of protection. Accidental or intentional disclosure of this type of sensitive data could cause damage and/or serious harm to COSA and/or its citizens. Confidential data is normally prohibited from disclosure by legislative measures.

   Examples of "Confidential" data may include but are not limited to:

   - Sensitive PII, such as: a name in combination with Social Security Number (SSN), drivers

license number, and/or financial account numbers
- Uniformed personnel files
- Medical information
- Credit Card data

2. *Agency-Sensitive*
- Sensitive data that **may** be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection.

Examples of "Agency-Sensitive" data may include but are not limited to:
- COSA operational information
- COSA personnel records
- COSA proprietary data, research data, network diagrams, server names and configurations
- COSA information security configurations, data, and procedures
- Vendor bids and/or contract cost estimates among other sensitive data types

3. *Public*
- All data and information not classified as confidential or agency-sensitive.
- The data owner, or designated employee of the data owner, may disseminate and disclose the data or information derived from the data to anyone upon request. ORR fees have been established for extracting and delivering this type of data.

Regulation and industry standards that protect confidential data including but not limited to:
- The U.S. Privacy Act of 1974 (5 U.S.C.A. 552a)
- U.S. Electronic Communications Privacy Act of 1986 (ECPA)
- The Open Records / Texas Public Information Act of 1993 (TPIA)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Texas Business and Commerce Act, Section 521.053
- Texas Medical Privacy Act of 2001 (TMPA)
- Texas Identity Theft Enforcement and Protection Act of 2007 (ITEPA)
- Payment Card Industry Security Standards (PCI)
- Criminal Justice Information Services Security Policy (CJIS)

Sensitive PII

Sensitive PII is any combination of information or data that permits the identity of an individual to be directly or indirectly inferred, traceable, linked and/or linkable to a specific individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, or visitor to the U.S. In addition, sensitive PII combinations if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, and/or unfairness to an individual.

Below is a list of data that is always Sensitive PII:
- Social Security Numbers
- Alien Registration Numbers (A-numbers)
- Passport Numbers
- Drivers license Numbers or state identification numbers
- Biometric Identifiers (fingerprint, iris scan, voice print)
- Genetic Data

The following information is Sensitive PII when linked with the person's name or other unique identifier, such as an address or phone number:

- Citizenship or Immigration status
- Criminal History
- Medical Information
- Bank Account or Routing/Transit Numbers
- Credit Card Numbers
- Income Tax Records
- Full Date of Birth
- Financial or Bank Account Numbers
- Fingerprint Identification Number (FIN) or Student and Exchange

Protection of Confidential Data

1. **All Departmental Data Owners must:**
   - Implement cost effective internal controls, safeguards and/or countermeasures to protect data. All preventative, detective and/or corrective controls shall be risk based. The cost of all management, operational and/or technical controls shall be commensurate with the value of the data.
   - Preserve citizen privacy and respect individuals choice to consent when collecting, using, sharing, and/or disclosing of customer, partner, or employee personal information.
   - Limit the use and storage of confidential data and sensitive PII to what is only necessary.
   - Determine encryption requirements based on regulatory requirements.
   - Not store confidential and/or sensitive data longer than is absolutely necessary.
   - Only collect data when COSA has the legal authority to do so, and if required have a Privacy Act System of Records Notice (SORN) in place that describes the information.
   - Minimize the distribution and proliferation of protected data.
   - Keep protected data relevant, accurate, timely and not excessive in relation to the purpose such data is processed, stored and/or transmitted.
   - Establish departmental procedures for dissemination of protected data in compliance with AD 1.31 and Open Records as well as establish and enforce departmental procedures and protections in addition to this Directive to reasonably assure the security of the specific data owned.
   - Annually review data protection procedures, controls, and safeguards to reasonably assure that internal controls, countermeasures and/or safeguards are working as intended.

2. **COSA Information Systems must:**
   - Use security controls to protect against unauthorized access, disclosure, modification and destruction to reasonably assure the confidentiality, integrity, availability of data.
   - Follow NIST encryption and security protocol standards for protected data as required.

3. **Employee and Third Parties shall:**
   - Safeguard COSA's data resources and comply with the provisions of relevant COSA Security ADs.
   - Comply with all COSA procedures regarding protected data.
   - Receive written approval from both his/her department director to store sensitive data.
   - Report suspected violations to supervisor or manager, department head, and the Chief Information Security Officer (CISO).
   - Only store protected data on COSA owned device(s).
   - Personal devices shall not be used to store, process and/or transmit unencrypted protected data.
   - Unencrypted confidential data and sensitive PII shall not be transmitted outside of the COSA

network.

- Physically secure hardcopy protected data in a locked drawer, file cabinet, desk and/or safe.

Data Destruction

Electronic records shall be destroyed in accordance with Section 441.185 Government Code and COSA record retention policies. All data storage device(s) and/or information system(s) containing protected data shall be sanitized or the storage device destroyed. COSA shall arrange for destruction of protected data by shredding, degaussing, erasing and/or otherwise modifying the sensitive data in the records to make the information unreadable or indecipherable. Additional information on sanitization tools and methods of destruction based on Department of Defense 5220.22-M data destruction standards (available at http://www.dir.state.tx.us). Documentation shall also be maintained that documents the data, description of device, data destruction process and sanitization tools used to remove or destroy data.

Data Breach and Incident Reporting

In compliance with applicable federal, state, and local laws and regulations, COSA shall disclose any breach of system security.

Definitions

City of San Antonio (COSA)	The City of San Antonio, its departments and agencies.
City-administered information technology system(s)	Any technology or equipment that is used and/or managed by COSA even if COSA does not own the technology or equipment. COSA-managed information technology system(s) includes technology or equipment owned by COSA, on loan to COSA, funded by grants, leased by COSA.
Criminal Justice Information Services (CJIS) Security Policy	CJIS Security Policy represents the shared responsibility between Federal Bureau of Investigation CJIS and the CJIS Systems Agency and State Identification Bureaus.
Federal Statutes	The laws of the United States and its territories.
Information Technology Services Department (ITSD)	COSA's Information Technology Services Department or successor agencies.
Local Statutes	The ordinances, statutes, and laws of COSA, Bexar County and/or the municipality or county where the user is located.
Local Government Record Retention Schedules	Publications issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter 441 of the Government Code which establish the mandatory minimum retention period for a local government record.
Network	A group of two or more computers linked together to facilitate communication, data sharing, and processing among other computer-based activities.
National Institute of Standards and Technology (NIST)	Recommended Security Controls for Federal Information Systems and Organizations

Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.
Records Management Officer	The person who administers the records management program established in each local government under section 203.026, chapter 203 of Local Government Code.
Retention Period	The minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record, before it is eligible for destruction.
Sensitive PII	Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
State Statutes	The statutes and laws of the state of Texas and/or the state where the user is located. Where statutes from two states conflict, the statutes of Texas and federal government shall take precedence.

This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the Information Technology Services Department at 207-8888.

CITY OF SAN ANTONIO

Administrative Directive	**7.4A Acceptable Use of Information Technology**
Procedural Guidelines	Regarding use of electronic communications systems
Department/Division	Information Technology Services Department (ITSD)
Effective Date	April 1, 2014
Originator	Patsy Boozer, CISO

Purpose

This Administrative Directive (AD) provides guidance for the acceptable use of information technology systems including electronic devices, electronic mail, Internet access, and/or software among other City systems. This includes acceptable use of City-owned computers, mobile devices and/or personal devices reimbursed through City stipends (A.D. 7.9). This directive establishes and identifies responsibility for the acceptable use of technology to help ensure the confidentiality, integrity and availability of City systems. This directive supersedes the use provisions previously in AD 7.4, 7.5, 7.6, 7.8.1 and 7.8F.

Overview

The City of San Antonio (COSA or City) provides access and use of its information technology systems to help users efficiently and effectively perform their business-related activities. All users of the City's information technology systems are responsible for using that technology in an appropriate and lawful manner.

Inappropriate use of information technology exposes the City to additional internal and/or external vulnerabilities that may reduce the reliability, confidentiality, integrity and/or availability of those systems.

The Information Technology Services Department (ITSD) shall be responsible for developing, maintaining, publishing and administering the acceptable use of information technology assets and systems. All unauthorized access to City data is strictly prohibited.

Policy

Adherence to this directive will help assure the City's acceptable use of technology.

1. There shall be no expectation of privacy when using any City-administered information technology system.
2. COSA is required to protect public assets and resources, and it has an obligation to manage information technology systems to comply with Chapter 552 of the Texas Public Information Act (open public records), Sections 7.71-7.79 of the Texas Administrative Code and 205.001-205.009 of the Local Government Code, among other regulations.
3. All information generated, processed, stored, or entrusted on any City-provided information technology system is the property of COSA.
4. Externally transmitted email and attachments that contain non-public data shall use FIPS 140-2 encryption.
5. COSA email may not be automatically forwarded or redirected to email addresses outside of COSA.
6. Email messages not essential to the fulfillment of statutory obligations or to the documentation of the

City's functions may be deleted. **Note:** These messages may include personal messages, internal meeting notices, letters of transmittal, and general FYI announcements.

7. Email messages that fulfill statutory obligations or document the City's functions are subject to retention as established by the Texas Administrative Code.
8. Individual COSA email accounts may not be used to send to more than 50 recipients of the same email message.
9. Distribution list must be maintained to remove invalid email addresses.
10. The City's information technology systems are shared resources that serve all of its users and provide the general public with access to its website. Inappropriate uses of information system assets reduce the usefulness of these resources.
11. City-managed information technology systems shall be used for official business only, which may include personal communications, including telephone calls during business hours, that are necessary and in the interest of the City. While some incidental use (as defined below) of City-managed technology is unavoidable, such incidental use is not a right, and should never interfere with the performance of duties or service to the public.
12. The National Institute of Standards of Technology (NIST) and industry best practices have been adopted by the City to help maintain the confidentiality, integrity and availability of COSA systems.

Applicability

This directive applies to:

- All information technology assets and systems, procured with City funds and/or used in the conduct of City business.
- All access to the City's facilities and networks, data, and/or applications among other systems including employees, contractors, vendors, and other third parties of City information assets, systems.
- All electronic messaging, equipment, or technology that is owned or administered by the City including City-owned computers, mobile devices, and/or personal devices reimbursed through CoSA stipends (*A.D. 7.9*) is included within the scope of this Directive.
- All software, information systems and/or other documents developed by City personnel with City funds or licensed to the City of San Antonio.
- All data processed, stored, and/or transmitted by any City information technology system.
- All devices that use the COSA network, including any "Bring Your Own Device" (BYOD).
- This directive applies to all information collected or maintained by or on behalf of the City and all information assets used or operated by the City, a City contractor, a City vendor, or any other organization on behalf of the City.

Policy Applies To

☒ External & Internal Applicants	☒ Current Temporary Employees
☒ Current Full-Time Employees	☒ Current Volunteers
☒ Current Part-Time Employees	☒ Current Grant-Funded Employees
☒ Current Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	☒ Vendors, Contractors and Other Third Parties

Roles and Responsibilities	
Information Technology Services Department (ITSD)	1. ITSD is responsible for the development, implementation, maintenance, and compliance monitoring of this directive is placed with ITSD and the City Clerk's Office. 2. ITSD and Human Resources will provide City departments with initial communication and training regarding application of this directive. However, City Department Directors are ultimately responsible for communicating the policies and standards established in this AD to all personnel in their respective departments and for ensuring compliance within their respective departments with those policies and standards. 3. ITSD is responsible for publishing and disseminating the standards and procedures established in this directive to all relevant personnel, third-party users including (contractors, consultants, vendors, business partners etc.) and for ensuring their compliance. City departments who work with third-party users are responsible for identifying the third-party users to ITSD. 4. ITSD is responsible for ordering, inventorying, managing, and supporting all of the City's information technology assets, which includes, but not limited to, desktops, laptops, tablets, mobile phones, servers, software, networking equipment, and printers. 5. Any computer-based device may be disconnected from the City network at any time, if continued connectivity constitutes a threat to the City or any City-administered information technology system. ITSD will attempt to contact the business owner responsible for the computer prior to disconnecting as long as such notification does not allow further degradation of the City-administered information technology systems. Such notification will be made after the disconnection, if prior coordination was not possible. 6. User's access may be terminated if he/she is found in breach of this directive. Service may be restored to the user following a written request by the user's Department Director or sponsor. 7. ITSD may isolate a sender's email message from reaching a user's City e-mail account. The following process must be followed in order to isolate email messages sent to the City's email system: • A user who receives repeated or multiple unsolicited, unacceptable annoying, alarming, abusive, embarrassing or offensive e-mail messages from a sender outside of the City must request the sender to stop sending such messages and inform the sender that any emailed requests for City records or documents must be sent to the City's Officer for Public Information at: http://www.sanantonio.gov/opengovernment/. • The user must provide copies of the messages and all correspondence between the user and sender, to the user's Department Director or appropriate Executive Leadership Team (ELT) member along with a written request to have ITSD isolate the sender's e-mails. • The Department Director or ELT member and the Office of the City Attorney will review the request and determine if the request is warranted. • It the request is deemed warranted and subsequently approved, it will be submitted to ITSD Customer Service for email isolation. 8. ITSD shall have acceptable use of technology training at least annually for all relevant personnel as part of their security awareness training program.

Office of the City Clerk	1. In accordance with AD 1.34 *Paper, Microfilm, and Electronic Records Management* the Records Management Officer will, in cooperation with ITSD, ensure that appropriate training and communication, retention, maintenance, and disposition requirements for applicable information. In addition, the Office of the City Clerk is responsible for the creation, maintenance and administration of all rules regarding the classification and protection of applicable information stored on City-administered information technology systems.
Department Directors and their Designees	1. Departments are responsible for implementation, training, and enforcement of the data classification standards defined by the Texas State Attorney General's Office as they apply to information created, stored, or processed on City-administered technology or equipment including data retention and disposition. 2. Department Directors are responsible for any disciplinary actions taken against employees who violate this policy. The Human Resources Department will provide guidance as required to City departments regarding appropriate disciplinary actions to be taken against employees who violate this policy. 3. Upon the voluntary or involuntary termination of any user with system access, or upon notification of such termination, the business owner will ensure all access authorizations are revoked and will take custody of, or ensure the safe return, modification, or destruction of all of the following items assigned, or relating, to the terminating or notified person: • Keys, change lock combinations, and identification badges. • Change system passwords. • Collect confidential data and documentation, along with operator procedures, and other program documentation and manuals. • COSA owned computers, software, assets and property.
Human Resources	1 . Human Resources Department is responsible for providing accurate job descriptions and security responsibilities shall be addressed in the terms and conditions of employment. All candidates for employment will be adequately screened, especially for positions of trust. Furthermore, management will require employees, contractors and other users, to apply security in accordance with established policies and procedures of the COSA. 2. Human Resources will provide guidance to departments for disciplinary actions associated with violations of the directive. 3. Human Resources will assist ITSD in providing training regarding this directive to current and future employees. Following implementation of this directive, Human Resources will ensure that all new employees are provided a copy of this directive and complete the attached acknowledgement form (Attachment A) regarding the acceptable use of COSA technology. 4. The Chief Human Resources Officer will consult with the Chief Technology Officer (CTO) or his/her designee in approving any monitoring of systems for personnel administration purposes.
Users	1. In accordance with AD 1.34 Paper, Microfilm, and Electronic Records Management users shall, with guidance and training from the Records Management Officer, manage the City's information technology systems in accordance with the City's approved retention periods. 2. Users should be aware that all information created, stored, or processed by City information technology systems is the property of the City of San Antonio. There should be no expectation of user privacy or confidentiality with regard to any files, including email, stored on City computers. Any materials stored on City information systems may be monitored and reviewed by City management at any time. In addition, users should be aware that much information generated and/or stored on any City information technology

	system is subject to applicable open records laws. 3. All lost equipment must be reported to the ITSD Service Desk. All stolen IT equipment shall be reported to the San Antonio Police Department (SAPD) and the associated case numbers reported to the ITSD Service Desk. COSA IT equipment can be any City-owned device, mobile device, and/or personal device reimbursed through COSA stipends in accordance with A.D. 7.9 among other City IT systems. In addition, all COSA capital assets that are lost or stolen shall be reported to the Finance Department in accordance with A.D. 8.7. 4. Users who voluntarily terminate employment or contract, retire, or are transferred, will be required to review their e-mail accounts with their supervisor or sponsor. The user's supervisor or sponsor is responsible for ensuring that e-mail records are properly classified and stored. All unnecessary working or convenience copies shall be disposed of appropriately.

Personal Use Policy

Personal use of technology must not interfere with the performance of assigned duties, must not have a detrimental effect on any City information technology system, and not be prohibited by this policy.
This includes the personal use of City-owned or managed technology that:

- does not cause any additional expense to the City
- is infrequent and brief
- does not have a negative impact on overall user productivity
- does not interfere with the normal operations of the a user's department or work unit
- does not compromise the City in anyway
- does not embarrass either the City or the user
- does not contravene other elements of this policy and
- serves the interest of the City in allowing employees to address personal matters which cannot be addressed outside of work hours without leaving the workplace.

Examples of personal communications that can be in the interest of the City include:

- communications to alert household members about working late or other schedule changes
- communications to make alternative child care arrangements, communications with doctors, hospital staff or day care providers
- communications to determine the safety of family or household members, particularly in an emergency
- communications to reach businesses or governmental agencies that only can be contacted during work hours
- and communications to arrange emergency repairs to vehicles or residences. City departments may consult with the Human Resources Department to determine whether a use is personal or business and if the usage is personal, whether it is incidental.

Security and Proprietary Information

1. Information stored on any City-administered information technology system should be classified in accordance with federal, state and local statues, ordinances, regulations, and/or policies among other directives regarding the confidentiality of the information. Users shall take the necessary steps or follow the prescribed processes to prevent unauthorized access to confidential information. Unclassified information should not be released to non-City entities without authorization and approval by the City Manager's Office. Users must comply with all City Directives regarding use of information technology, including:
    - Electronic Communications (e-mail, voice and Internet)

- Password Management
- Security
- Data Management and Classification
- Monitoring
- Remote Access

2. All personal computers, laptops, and workstations should be protected from unauthorized access when the system is unattended. The recommended method of security for City devices is with a password-protected screensaver (with the automatic activation feature set to 15 minutes or less) or by manually locking the device (Ctrl-Alt-Delete for most Microsoft Operating Systems). Devices that cannot be locked as described above should be secured by logging off the devices or turning them off.
3. Users must take reasonable and necessary precautions to secure and protect electronic devices.
4. ITSD regularly maintains operating systems, updates security software, and applies security patches by sending those updates during non-business hours to computers attached to the network. When a user leaves for the day, he/she should log off from his/her computer, but should leave the computer turned on and attached to the network. If laptops are secured during non-business hours and are not connected to the network, it is possible that updates were sent; as such users should work with their business owner to ensure updates to portable devices are installed in a timely manner.
5. All technology devices used by a technology user to connect to the City's networks shall continually execute approved security software with a current virus definition file. This includes user-owned equipment attached to the City's networks through remote access technologies. The City is not responsible for providing the required security software for user-owned computers
6. E-mail attachments that may constitute a risk to the City's technology environment will be removed from e-mail messages passing through the City's mail servers. Removed attachments are replaced by a message indicating that they have been removed and the header and text of the original message delivered normally.
7. A spam message filter is used to reduce the transmission of chain letters, broadcast announcements, general advertisement postings, or any other message via e-mail to a group of persons not requesting the message.

Password Management

Passwords are an important element of the acceptable use of technology and associated information security. A poorly chosen password may result in the compromise of the City's network. All technology users are responsible for taking appropriate steps to select and secure passwords. Users shall take reasonable and necessary care to prevent unauthorized access to workstations, laptops, applications, mobile and/or other devices.

City Password requirements (at a minimum):

1. No departmental personnel, including administrative staff, shall request access to or maintain lists of other user passwords.
2. Use of "strong" passwords. Strong passwords that:
   - are at least eight characters in length
   - are not based on words in any language, slang, dialect or jargon
   - are not based on personal information, such as family names
   - use at least one (1) each English uppercase (A through Z), lowercase (a through z), digit (0 to 9) and non-alphanumeric character (!,$,#,%)
   - are not common usage words like family, pets, friends, COSA, birthdays, phone numbers, addresses, computer terms, fantasy characters and/or common patterns like aaabbb, qwerty, zyxwvuts, 123321 or any derivation followed by a digit.
3. All users' passwords will expire at intervals of ninety (90) days. Users will be prompted to change passwords beginning 10 days before the next expiration date. Passwords may not be re-used.
4. Passwords will be changed immediately after a security breach has been detected to the affected COSA

systems.

5. As the COSA system software permits, an initial or reset password issued to a user will be valid only for the user's next log in. After that, the user must be prompted to change their password.
6. Users should register for password management self-service on the COSA intranet.
7. Password Protection Guidelines:
    - Do not write passwords down, store them on-line, or reveal them in any electronic format.
    - Do not use the same password for COSA accounts as for other accounts (i.e. social media, personal email account, banking sites, etc).
    - Passwords must be treated as sensitive and confidential information thus do not share City passwords with anyone.
    - ITSD support personnel may require a user's password to resolve a problem however, the user be present to enter the required password. If a password must be revealed to the ITSD technician then the password must be changed as soon as is practical.
    - Do not talk about a password in the presence of others.
    - Do not hint at the format of a password ("my family name").
    - Do not click on links in emails from unknown sources and provide account information that includes personal information and/or password.
    - Do not reveal a password on questionnaires or security forms.
    - Do not use the "remember password" feature.
    - Do not store passwords in a file on ANY computer system without encryption.
8. Technology users shall report any suspected security violations or threat to the ITSD Service Desk immediately. Any activity performed under a user-id/password combination is presumed to have been performed by that user and is the responsibility of that technology user.

Retention and Disposition of E-mail

The City's approved Declaration of Compliance with the Local Government Records Retention Schedules establishes record series and the retention period for each series. It is the content and function of an e-mail message that determines the retention period for that message. All e-mail sent or received by a government is considered a government record. Therefore, all e-mail messages must be retained and disposed of according to the City's retention requirements. E-mail systems must meet the retention requirement found in chapter 7, section 7.77 of the Texas Administrative Code.

Users and their supervisors or sponsor should seek guidance from the City's Records Management Officer if there is a question concerning whether an electronic message should be deleted.

Acceptable Use of Electronic Signatures and Electronic Records

Electronic signatures, an automated function that replaces a handwritten signature with a system generated signature statement, and electronic records can be utilized as a means for authentication of City documents, computer generated City documents and/or electronic City entries among other uses. System generated electronic signatures are considered legally binding as a means to indentify the author of record for entries and confirm that the contents of what the author intended. City departments and staff will be allowed to utilize electronic signature in accordance with this directive, City, State, and/or Federal regulations regarding such.

Acceptable Use of Electronic Records and Electronic Signatures are allowed:

1. Where policies, laws, regulations, and rules require a signature and that requirement is met if the document contains an electronic signature.
2. Where policies, laws, regulations, and/or rules require a written document, and that requirement is met if the document is an electronic record.
3. Each party to a transaction must agree to conduct the transaction electronically in order for the electronic

transaction to be valid and binding. Consent may be implied from the circumstances, except with respect to any electronic records used to deliver information for which consumers are otherwise entitled by law to receive in paper or hardcopy form.

4. If a law prohibits a transaction from occurring electronically, the transaction must occur in the manner specified by law.
5. If a law requires an electronic signature to contain specific elements, the electronic signature must contain the elements specified by law.
6. If a law requires that a record be retained, that requirement is satisfied by retaining an electronic record of the information in a record that accurately reflects the information set forth in the original record and shall remain accessible for later reference. When the requirements for retention require an original form, retention by an "electronic form" shall provide and satisfy the retention requirement.

Procedures, Forms, Guidelines and Resources for electronic signatures:

1. Procedures for electronic signatures can be found under the *Texas Uniform Electronic Transactions Act*
2. United States governance can be found in 18 USC 2510, *Electronic Communications Privacy Act*
3. Record management for COSA is established by Local Government Code: 201 through 205. The Texas State legislature requires local governments to establish a records program by Ordinance.
    - City of San Antonio adopted Ordinance 70508 and 72054
    - Ordinance 70508 (11-02-1989) names the City Clerk as the City's Record Management Officer
    - Ordinance 72054 (August 9, 1990) establishes the City's Records Management program
    - The charter of the City of San Antonio mandates that the City Clerk shall keep the records of the Council and of the City
    - Pursuant to Article II, Section 10 of the Chart for the City of San Antonio, the City Clerk shall keep the records of the Council and of the City. Pursuant to City Ordinance 72054 which establishes the City's records management program in compliance with the Local Government Records Act and reaffirms City Ordinance 70508 naming the City Clerk as the City's Records Management Officer, both ordinances filed with the Texas State Library and Archives Commission, the Records Management Officer shall develop policies and procedures in the administration of the City's records management program. This policy does not supersede any local, state or federal laws regarding records management, confidentiality, information dissemination or standards of conduct.

Electronic Transactions and Signed Records:

1. Electronic Records - The Uniform Electronic Transactions Act (UETA) was enacted into law in Texas by the 77th Legislature (Senate Bill 393) in May 2001, and became effective on January 1, 2002. UETA provides definitions for several key terms that pertain to this policy. These terms are listed in the "Definition" section of this directive.
2. Electronic Signatures - Texas law (Government Code, Section 2054.60, provides a definition for the term "digital signature," which is sometimes used interchangeably with "electronic signature" (see Section II, C, 3).

Unacceptable Use of COSA Resources and the Internet

The following activities are prohibited unless performed in the course of legitimate job responsibilities. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable uses of COSA information technology systems:

1. Engaging in any activity that is illegal under local, state and/or federal statutes as well as any activity that violates COSA policies and Administrative Directives.
2. Accessing, displaying, storing or transmitting material that is offensive in nature, including sexually explicit materials, or any text or image that can be considered threatening, racially offensive, or hate

speech. This includes any images, text, files, etc. sent via email to co-workers or outside parties. Accessing, storing, displaying, or transmitting pornographic materials using City-owned and managed technology is strictly forbidden.

3. Engaging in any form of harassment, whether sexual or otherwise, or sending any unwelcome personal communication. It is the perception of the recipient that prevails in most instances, not the intent of the sender.
4. Any personal use that interrupts City business and that keeps an employee from performing his/her work. Users should not use their City e-mail account as a personal email address or to register with a non-work related social network. City systems shall also not be used to chat online, "blog", or shop online.
5. Extensive personal use of the Internet for any non work-related purpose during working hours which decreases the employees productivity or results in decreased performance of the City's Internet facilities.
6. Violating any copyright, trade secret, patent and/or other intellectual property or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City.
7. Unauthorized downloading of and/or distributing of copyrighted materials.
8. Revealing a City account password to others or allowing use of a City account by others. This includes household members and visitors when work is being done at home. Revealing a City account password to an authorized technician during a troubleshooting procedure is not a violation of this policy. In such a situation, a new password should be established as soon as possible, after the problem is resolved.
9. Requesting a password to another users network or application account.
10. Unauthorized reading, deleting, copying, modifying, printing and/or forwarding of electronic communications of another, or accessing electronic files of another without authorization.
11. Unauthorized duplication of copyrighted material including, but not limited to, text and photographs from magazines, books or other copyrighted sources, copyrighted music and/or copyrighted movies. Copying or installing copyrighted software for which the City or the end user does not have an active license is not permitted.
12. Sending SPAM to either internal or external parties. Individual email accounts will be limited by technical controls as a preventive measure to detect SPAM originating from a City email account. Large volume emails to recipients will not be allowed from individual email accounts. Request for approved email accounts designated for such business purposes will be submitted to ITSD Customer Service.
13. Approved email accounts must not regularly send bulk emails unless distribution lists are maintained. All undeliverable or invalid addresses from distribution lists must be regularly removed to prevent the City from not being able to send email through Internet Service Providers and/or mail hosts.
14. Downloading and/or copying music, photographs or video material, including such material that has been obtained legally, onto City computers or servers.
15. Downloading and/or installing executable program files from external media or the Internet without the approval of ITSD.
16. Exporting software, technical information, encryption software and/or technology, in violation of international or regional export control laws.
17. Using the City's electronic mail or Internet systems for private gain or profit.
18. Using unauthorized personal software which allows peer-to-peer communications between two workstations (Yahoo Messenger, AIM, Google Talk, KaZAA, etc.).
19. Using instant messaging through public service providers.
20. Using City systems for non work-related access to online auctions or ecommerce sites (such as e-Bay, Amazon).
21. Maliciously introducing malware or similar programs into the network or server.
22. Soliciting for political, religious, and/or other non-business uses not authorized by COSA.
23. Making fraudulent offers of products or services originating from any City account.
24. Accessing non-business related streaming media, including Internet-based radio.

25. Accessing any non-business related application which maintains a persistent application connection to the Internet, such as streaming videos or media, such as Pandora, YouTube, Netflix, and/or Google Video, among others.
26. Using City technology, electronic mail and/or Internet facilities for political activity including voting, private gain, gambling, shipping, games, entertainment or other non-business function unless permitted by this directive.
27. Including email "tag lines" or personal quotations other than ones that state the mission of the City or the user's Department.
28. Using the COSA email system to automatically forward COSA email to a personal email account is prohibited.
29. Sending or forwarding junk e-mail, chain letters, or other mass mailings.
30. Causing security breaches or disruptions of City communications. Security breaches or disruptions can include, but are not limited to:
    - Accessing data which the user is not authorized to access or logging into a server or user account that the user is not expressly authorized to access
    - Causing network disruptions for malicious purposes including, but not limited to, network sniffing, ping floods, packet spoofing, denial of service of any kind, and forged routing information for malicious purposes
    - Port scanning or vulnerability scanning for malicious purposes is prohibited. Non-malicious scanning that is part of a City-sanctioned security process is allowed. ITSD should be notified prior to any such scanning
    - Circumventing user authentication or security of any device, network or account
    - Maliciously interfering with or denying service through a denial of service attack, or by other means
    - Using any program/script/command, or sending messages of any kind, with the intent to interfere with, and/or disable, another user's device or session, via any means, locally or via the City's network
    - Adding/removing hardware components, attaching external devices, and/or making configuration changes to information technology devices without the explicit approval by ITSD
    - Storing confidential data on personally owned devices.

Privacy and Monitoring

1. City systems may be monitored by ITSD to support operational, maintenance, auditing, security and/or investigative activities including enforcement of this Directive, legal requests, and public records requests or for other business purpose.
2. Only Department Directors or higher may request monitoring of City administered IT systems for employees under their supervision for administrative purposes. Unauthorized monitoring or reading of electronic communications systems or their contents violates this Directive.
    - Any request to monitor must be approved by the CTO or his/her designees as well as the Chief Human Resources Officer (CHRO) or higher.
    - To obtain the necessary authorization, a written request from the requestor's Department Director to the CHRO must include subject employee information (i.e. name, employee number), a specific description of request (e.g. Email, share drives, web usage etc.) and name and phone number of the employee in the requesting department who is responsible for coordination of the request.
    - The CHRO will forward the request to the CTO or designees for concurrence as well as to assign staff from ITSD to assist as necessary with any monitoring activities.

Definitions

City-administered information technology systems	Any technology or equipment that is used and/or managed by the City even if the City does not own the technology or equipment. City-managed information technology systems include technology or equipment owned by the City, on loan to the City, funded by grants, leased by the City, etc. Information Technology systems includes but, are not limited to computers, mobile communication devices, telecommunication devices, servers, networks, software, databases and email messages, among other physical and virtual infrastructure.
Digital Signature	An electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature.
Electronic mail record	An electronic government record sent and received in the form of a message on an electronic mail system of a government, including any attachments, transmitted with the message.
Electronic Record	Record created, generated, sent, communicated, received, or stored by electronic means.
Electronic Signature	An electronic sound, symbol, or process attached to, or logically associated with a record and executed or adopted by a person with the intent to sign the record.
Incidental Use	Personal use of technology that does not interfere with the performance of assigned duties, does not have a detrimental effect on City information technology systems, and is not prohibited by this policy.
Local Government Record Retention Schedules	Publications issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter 441 of the Government Code which establish the mandatory minimum retention period for a local government record.
Malware	Malicious software designed to impact the confidentiality, integrity and/or availability of an information technology system. Malware can include viruses, worm, Trojan horse, or adware among other malicious programs.
Network	A group of two or more computers linked together to facilitate communication, data sharing and processing among other computer activities.
Records Management Officer	The person who administers the records management program established in each local government under section 203.026, chapter 203 of Local Government Code.
Retention Period	The minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record before it is eligible for destruction.
Sponsor	Departmental representative responsible for authorizing non-employee access to COSA assets and/or systems.
User	Any employee or non-employee who uses COSA-administered information assets and/or systems, exclusive of COSA's web pages
Discipline	

Compliance with COSA administrative directives, security policies, and/or procedures is the responsibility of all COSA employees, contractors and/or other third parties. The City can temporarily or permanently suspend, block, and/or restrict access to information or physical assets, independent of such procedures, when it is reasonable and associated probable cause exists to do so in order to protect the confidentiality, integrity or availability of City resources as well as protect the City from liability, and/or to comply with applicable federal, state, and municipal laws, regulations, statutes, court orders, or other contractual obligations. Violations of any of these directives shall result in disciplinary actions in accordance with section 2 of Rule XVII of the Municipal Civil Service Rules of the City of San Antonio. Administrative action may range from reprimand and loss of access privileges to suspension to separation of employment. Violations may also result in civil and/or criminal prosecution.

CITY OF SAN ANTONIO

EMPLOYEE ACKNOWLEDGMENT FORM FOR

ADMINISTRATIVE DIRECTIVE 7.4A
Acceptable Use of Information Technology

Employee:

I acknowledge that on _____, 20____, I received a copy of Administrative Directive 7.4A, Acceptable Use of Information Technology. I understand if I should have any questions I should contact my Human Resources Representative.

_____ _____
Employee Name (Print) Department

_____ _____
Employee Signature Employee SAP ID Number

Attachment A
Personnel File (original)

Exhibit 7

CITY OF SAN ANTONIO

Administrative Directive	**7.5a Establishing IT-Related Directives**
Procedural Guidelines	Guidelines to implement and enforce Citywide IT-related directives and standards.
Department/Division	Information Technology Services Department (ITSD)
Effective Date	April 1, 2014
Originator	Patsy Boozer, CISO

Purpose

This Administrative Directive (AD) establishes a framework for the City of San Antonio's (COSA or City) information security program and process for creating or updating and communicating City-administered information technology (IT) system – related directives, standards and procedures. It establishes and identifies responsibilities to help ensure the confidentiality, integrity and availability of City system(s). This directive supersedes 7.8.1 Information Security Program and 7.5a dated December 23, 2008.

Overview

The COSA information security program is a framework based on the National Institute of Standards of Technology (NIST) and industry best practices to help maintain the confidentiality, integrity and availability of COSA systems and meet applicable federal, state, and municipal laws, administrative codes, regulations, and/or statutes that apply to City assets. In order to implement COSA IT-related ADs, ITSD will need to develop, update and communicate standards and/or procedures designed to provide reasonable assurance that risk-based system and application security controls and/or countermeasures are commensurate with the value of the asset(s) they protect.

Note: Any definition, provision, directive, standard, procedure or requirement of this information security program, or any referenced or related documents, shall be presumed valid and in effect unless it becomes superseded or conflicts with any:
Federal Law
State Statute
San Antonio Municipal Ordinance or Charter Provision, Federal or State administrative code, or Federal or State regulation.

Updates for compliance shall be made if necessary.

Policy

Adherence to this directive will help reasonably assure the security of City assets.

1. The Information Technology Services Department (ITSD) has primary responsibility for the security management program and the security of the City's electronic systems. ITSD will establish administrative directives, standards and/or policies to help ensure the security of City system(s).
2. Organizational responsibility for the development, implementation, maintenance and/or compliance monitoring of this directive is placed with ITSD.
3. ITSD will maintain the security management program and monitor its compliance.
4. COSA is required to protect public assets and resources and it has an obligation to manage

information technology systems to comply with Chapter 552 of the Texas Public Information Act (open public records), Sections 7.71-7.79 of the Texas Administrative Code, and 205.001-205.009 of the Local Government Code among other regulations.

5. All information created, processed, or stored in City-provided information technology systems are the property of COSA.
6. IT-related Standards may include specifications for acceptable hardware, acceptable versions of software, and acceptable performance of technology, service level agreements, and other categories.

Applicability

This directive applies to:

- All information technology systems, procured with City funds, and/or used in the conduct of City business
- All electronic messaging, equipment and/or technology that are owned or administered by the City including City-owned computers and/or mobile devices
- Personal devices when used to access City systems, applications or data
- All software, information system(s) and/or other documents developed by City personnel with City funds or licensed to the City of San Antonio
- All data processed, stored and/or transmitted by any City Information Technology System(s)
- All devices that use the COSA network including any "Bring Your Own Device" (BYOD)
- All information collected or maintained by or on behalf of the City and all information assets used or operated by the City, a City contractor, a City vendor, or any other organization on behalf of the City
- All IT-related directives standards and procedures required to protect information technology systems, procured with City funds, residing on City property and/or used in the conduct of City business.

Policy Applies To

☒ External & Internal Applicants	☒ Current Temporary Employees
☒ Current Full-Time Employees	☒ Current Volunteers
☒ Current Part-Time Employees	☒ Current Grant-Funded Employees
☒ Current Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	☒ Vendors, Contractors and Other Third Parties

Information Security Management Program

The COSA Security Management Program Framework is designed to create a continuous cycle for assessing and validating risk by developing and implementing entity wide security policies and procedures as well as monitoring and periodically testing their effectiveness. Assessing and validating risk defines the management, operational, and/or technical controls necessary to protect COSA asset(s). Security Management includes risk-based countermeasures and safeguards as well as preventative, detective, and corrective security controls over remote and local access, contingency and backup planning, change and log management, cryptography, network security, patch and configuration management, physical access, and secure system development among other controls.

COSA information assets represent a significant investment by the City. As such, all City information assets must be protected from unauthorized access, use, disclosure, duplication, modification, diversion, and/or destruction whether accidental or intentional. Access to all City, non-public, information assets must be limited to what is necessary for the performance of required business tasks.

COSA's City-wide security program includes (at a minimum):

- Periodic risk and vulnerability assessments, security evaluation and testing as well as continuous monitoring that validate risk and internal control effectiveness.
- Coordinating development and distribution of security policies and procedures to reasonably assure cost-effective risk reduction and compliance.
- Subordinate information security plans for networks, facilities, systems and software among other plans.
- Security awareness training for City employees, contractors, officials and other third parties as well as planning and coordinating security-related activities within COSA.
- Periodic testing and evaluation that includes testing of all major risk-based systems on the COSA network as well as providing results to senior management on policy and control.
- Maintaining a remedial action process to address deficiencies.
- Monitoring vendor activity to help ensure compliance with the COSA security program requirements.
- Coordinating Security Incident Response activities for detecting, reporting and/or responding to incidents.
- Maintaining continuity of mission-essential systems including operational and contingency plans.
- Representing COSA in the security community.

Roles and Responsibilities

1. Organizational responsibility for the development, implementation, maintenance, and/or compliance monitoring of this directive is placed with ITSD.
2. ITSD Security Personnel shall have sufficient authority, training and resources to:
    - Obtain data needed to monitor compliance with directives, policies/standards and procedures
    - Establish an IT and Physical Security Awareness Program
    - Execute responsibilities including staff and tools.
3. ITSD Security Personnel & system/application owner will develop procedures to ensure system/application security is addressed throughout the procurement process and/or development lifecycle.
4. System/application owners are responsible for defining security-related business requirements.
5. ITSD is responsible for publishing, disseminating and communicating the policies/standards and procedures established in this directive to all relevant personnel, third-party users including (contractors, consultants, vendors, business partners etc.).
6. City departments who work with third-party users are responsible for identifying the third-party users to ITSD.
7. A final security review must be approved by the system/application owner, Chief Information Security Officer (CISO) and the Chief Technology Officer (CTO), or their respective designees, before a being placed into production.
8. The system/application maintenance process shall include reviews of security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.
9. Documentation shall be maintained by the system/application owner and be available to ITSD.
10. All software applications obtained, purchased, leased, or developed provide appropriate security controls to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other information technology resources.

Definitions	
COSA/City	The City of San Antonio, its departments and/or agencies.
Confidentiality	Ensuring that the information and processing capabilities of City information assets are protected from unauthorized disclosure or use.
Integrity	Ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably.
Information Security Program	A framework designed to provide reasonable assurance that risk-based system and application security controls and/or countermeasures are commensurate with the value of the asset(s) they protect; are in place and working as intended to protect City information asset(s).
Information Technology Services Department (ITSD)	The City's Information Technology Services Department of successor agencies.
User	Any employee or non-employee who uses COSA-administered information assets and/or system(s), exclusive of COSA's web pages.

This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the Information Technology Services Department at 207-8888.

Exhibit 7

CITY OF SAN ANTONIO

Administrative Directive	**7.8d Access Control**
Procedural Guidelines	Controlling Access to City Systems
Department/Division	Information Technology Services Department (ITSD)
Effective Date	April 1, 2014
Originator	Patsy Boozer, CISO

Purpose

This Administrative Directive (AD) provides a framework for controlling access to the City of San Antonio's (COSA) information assets. It identifies requirements and responsibilities needed to properly manage access control, helping to ensure the confidentiality, integrity and availability of City system(s). This directive supersedes 7.8c on Remote Access, 7.8d on Account Access Management and 7.8e on User Account Management.

Overview

This directive is designed to help control logical and/or physical access to COSA information assets. CoSA is subject to federal and state regulations and/or requirements that govern access control requirements (i.e. tax record laws/regulations, public records, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Criminal Justice Information Services (CJIS) policy for Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA), Payment Card Industry (PCI), etc).

Controlling access to COSA systems prevents unauthorized access; limits access to sensitive resources; and restricts users to performing functions that are within the scope of their authority and/or responsibility. Access controls also assist in controlling the kinds of data, transactions, operations and activities that may be performed on COSA IT Systems. Appropriate access controls provide reasonable assurance and user accountability that access attempts, actions taken and transactions committed may be associated with a specific individual. Access Controls also pertain to the proper classification and protection of physical and logical diagrams, personnel listings, operations manuals, and IT system configuration information among other data. Improper access controls within units and departments can reduce the reliability and integrity of computerized data as well as increase the risk of data destruction, unauthorized program changes and/or other inappropriate disclosure of data. Should confidential information be disclosed, it could result in unnecessary vulnerabilities to the COSA environment.

Policy

Adherence to this directive takes into account

- Federal and state laws/regulations, as well as industry standards that require COSA to implement, access and apply security controls, including access control(s) to protect sensitive and regulated data.
- The National Institute of Standards and Technology (NIST) 800-53 Security Controls and industry best practices have been adopted by COSA to provide a protection framework for maintaining the confidentiality, integrity and availability of COSA systems and data.
- Organizational responsibility for the development, implementation, maintenance and/or compliance monitoring of this directive is placed with the Information Technology Services

Department (ITSD).

- All information generated by and/or stored in COSA information technology systems are the property of COSA.
- Access to COSA's information and IT resources must conform to all administrative directives and ITSD security requirements.
- Access authorization should be formal, well-defined, documented and an auditable process.
- Access to COSA assets is based on an individual's membership in a group, job function and/or role in their assigned City department. Access permissions will use the principle of least privilege. All other access requires justification and approval.
- Logical and physical access controls implemented should be risk-based. Once access controls are implemented, they must be audited at least on an annual basis.
- A unique identifier and authenticator must be established for each individual (i.e., user ID) or process requesting access to COSA IT Systems.
- Where technically feasible and appropriate, access controls will enforce segregation of duties.
- COSA departments are responsible for non-employee and special account sponsorship and compliance with ITSD established provisioning and de-provisioning procedures.
- Remote access to COSA resources must comply with Human Resource (HR) and ITSD established provisioning and de-provisioning procedures.
- COSA Departments are responsible for ensuring compliance to this Directive.
- ITSD is responsible for monitoring compliance with this Directive.

Applicability

This directive applies to:

- All information technology systems procured with COSA funds and/or used in the conduct of COSA business.
- All technology users who access COSA networks, data and/or applications including employees, contractors, consultants, vendors, partners and/or other third parties.
- All electronic messaging, equipment and technology that are owned or administered by the City including computers, mobile devices or personal devices reimbursed through COSA stipends (*A.D. 7.9*).
- All software, applications and/or, information system(s) developed by City personnel with City funds or licensed to the City.
- All data processed, stored and/or transmitted by a City Information Technology System(s).
- All City data residing on 'Bring Your Own Devices' (BYOD) that use the COSA network.
- All remote access to the COSA network.
- All information collected or maintained by or on behalf of the City as well as all information assets used or operated by a City employee, a City contractor, a City vendor, or any other organization on behalf of the City.

Policy Applies To

☒ External & Internal Applicants	☒ Current Temporary Employees
☒ Current Full-Time Employees	☒ Current Volunteers
☒ Current Part-Time Employees	☒ Current Grant-Funded Employees
☒ Current Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	☒ Vendors, Contractors, Partners and Other Third Parties

Roles and Responsibilities

1. The Department Business System Owner is responsible for ensuring that appropriate access controls have been developed and documented in accordance with this AD.
2. ITSD is responsible for developing and maintaining an implementation standard and monitoring compliance for this directive for business systems under management control.
3. ITSD is responsible for publishing and disseminating the policies, standards and procedures which implement and enforce this directive.

Business Requirements for Access Control

1. Users requesting physical access to a City facility controlled by an access control system or logical access to an information system must have completed the Human Resources new employee or COSA third party sponsorship, background check, and attestation process.
2. Local, physical and/or remote access to information resources must be explicitly approved through the user provisioning and de-provisioning, account access and/or the COSA ID request process.
3. All access to the COSA network shall utilize ITSD approved technologies.
4. Local, physical and/or remote access controls will be periodically reviewed for validity by ITSD, COSA department(s) and or application owners.

Non-Employee Access Requirements

To obtain local, physical and/or remote access to COSA IT resources, all non-employees (contractors, vendors, partners and consultants) must:

- Be sponsored by a City Departmental Business Owner through submission of the Access Control Sponsorship process
- Utilize defined user accounts that are only active during the individual's expected period of work or 90 days, whichever is shorter. At the end of 90 days if the account is still required, the sponsor must request that the account be renewed. Third party accounts not used for 60 days without prior notification will be suspended.
- The sponsor is responsible for notifying ITSD customer service when a non-employee is no longer supporting their department. If the sponsor separates from COSA or transfers within the City, the responsible COSA Department must designate a new sponsor and ensure that the required ITSD access control forms are updated and submitted to ITSD for that user account.

User Access Management and Responsibility

1. No individual shall engage in any activity which attempts to compromise COSA information assets or data regardless of intent.
2. Any attempt to bypass or disable security controls or measures to gain unauthorized access to COSA IT assets or data is expressly forbidden.
3. Departmental Data Owners are responsible for authorizing access to information.
4. Access to COSA IT assets must be disabled upon separation of the employee.
5. Accounts for individuals who are in a Leave of Absence (LOA) status must be disabled on the first date of absence and for the duration of the leave.
6. All COSA Information Systems must be periodically screened for inactive accounts. Accounts will be disabled after 90 days of continuous inactivity or as soon thereafter as technically feasible.

ITSD is Responsible for:

- Maintaining the user processes required for physical access and COSA domain user accounts
- Provisioning and deprovisioning access based on COSA Departmental Business Owner authorization and approval
- Reviewing and monitoring data center access and domain user accounts
- Support review process for Departmental physical and logical access controls.

Definitions	
Access	The ability to do something with a computer resource (use, change, or view).
Access controls	A manual or automated mechanism by which a system grants or revokes the right to access some data, or perform some action. Access controls are the means by which the access ability is explicitly enabled or restricted in some way and they enforce segregation of duties. Access controls can be onsite via local network, offsite via remote network and/or physical access by token or badge.
Authorization	The mechanism by which a system determines what level of access a particular authenticated user should have to sensitive resources or data controlled by the system.
Availability	The mechanism whereby systems and networks provide adequate capacity in order to perform in a predictable manner with an acceptable level of performance.
COSA	The City of San Antonio, its departments and/or agencies.
Confidentiality	Ensuring that the information and processing capabilities of City information assets are protected from unauthorized disclosure or use.
Identification	The process whereby a network element recognizes a valid user's identity.
Information Systems	Computer(s), hardware, software, storage media, and network(s); the procedures and processes used to collect, process, store, share or distribute information by and through the City's computing and network infrastructure.
Integrity	Ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably.
ITSD	The City's Information Technology Services Department of successor agencies.
Least Privilege	An access control principle requiring that a computer user be given only the level of access needed to perform their job duties.
Network	A group of two or more computers linked together to facilitate communication, data sharing and processing among other computer activities.
Segregation of duties	The process of segregating work responsibilities to help ensure critical stages of a process is not under the control of a single individual.
User	Any employee or non-employee who uses COSA-administered information assets and/or system(s), exclusive of COSA's web pages.

This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the Information Technology Services Department at 207-8888.

RFCSP EXHIBIT 8

NON-DISCRIMINATION

Non-Discrimination. As a party to this contract, {Contractor or Vendor} understands and agrees to comply with the Non-Discrimination Policy of the City of San Antonio contained in Chapter 2, Article X of the City Code and further, shall not discriminate on the basis of race, color, national origin, sex, sexual orientation, gender identity, veteran status, age or disability, unless exempted by state or federal law, or as otherwise established herein.

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

019 RFCSP ATTACHMENTS

RFCSP ATTACHMENT A

PROPOSED PLAN

Provide a detailed but concise description of your approach to this project. Include a description of the task required for each area and the time required for their completion. This description should address but is not limited to the following:

SYSTEM ARCHITECTURE AND OPERATION - Describe the technical architecture necessary to support the proposed solution. The technical architecture proposal should address all components necessary to support the video upload, the video management solution software, and the storage platform itself.

Your response should include but not be limited to the following:

- All hardware, peripherals and client software necessary to catalog and upload videos and their associated meta data
- Data network infrastructure to support the upload and retrieval of videos and their associated meta data
- Data storage configuration to support the City's anticipated storage volume and retention including data backup
- All hardware and software necessary to manage, edit, download, or otherwise use the videos

Your response should include a detailed description of how officers will catalog, manage, and upload video to the proposed system with minimal disruption and impact to their other duties, include a breakdown of the estimated interaction time required from an officer during and after a duty shift.

Your response should include a detailed description of how videos and their meta data are transported from the camera to the back end system, including what connections, transports, and protocols are necessary.

Your response should include an explanation of the portability of videos and their associated meta data once they have been uploaded including your capabilities to integrate with external systems (eg, web services or APIs to third-party systems).

Your response should include an explanation of how you will collect geo location information and how you will manage system-wide date/time synchronization with the cameras.

IMPLEMENTATION PLAN – Describe your master implementation approach, plan and timeline for the San Antonio Police Department body worn camera system to include the distribution of units, training, testing, network configuration, and server and storage platform deployment. The plan should include a description of the proposed project organization structure, key personnel assignments, and roles and responsibilities. The response should also include a draft work plan to include all payment milestones and their associated tasks necessary to develop and deliver the system beginning with project initiation through final acceptance by the City.

TRAINING PLAN - Describe your approach to providing initial and ongoing training on the operation and use of the cameras and video management system. The Respondent should be prepared to offer ongoing training for their product as newer units are procured by the City. Training must consist of an appropriate blend of classroom instruction and hands-on practical training with the equipment to be used.

MAINTENANCE AND SUPPORT PLAN - Describe your plan for post-implementation maintenance and ongoing support of the cameras, back end software, and all equipment included as part of the solution. Provide a detailed service level agreement for post-implementation for the proposed solution.

REPLACEMENT PLAN - Explain how you will support the City's Replacement Plan requirements in Section 004.1, Paragraph D of this solicitation. Include an explanation of the planned useful life and lifecycle replacement of cameras and associated peripherals and equipment and your plan for introducing new devices into the City's environment.

RFCSP ATTACHMENT B

RESPONDENT QUESTIONNAIRE

1. **Respondent Information:** Provide the following information regarding the Respondent.
(NOTE: Co-Respondents are two or more entities proposing as a team or joint venture with each signing the contract, if awarded. Sub-contractors are not Co-Respondents and should not be identified here. If this proposal includes Co-Respondents, provide the required information in this Item #1 for each Co-Respondent by copying and inserting an additional block(s) before Item #2.)

Respondent Name: _____
(NOTE: Give exact legal name as it will appear on the contract, if awarded.)

Principal Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No:_____

Website address:_____

Year established: _____

Provide the number of years in business under present name: _____

Social Security Number or Federal Employer Identification Number: _____

Texas Comptroller's Taxpayer Number, if applicable: _____
(NOTE: This 11-digit number is sometimes referred to as the Comptroller's TIN or TID.)

DUNS NUMBER: _____

Business Structure: Check the box that indicates the business structure of the Respondent.

___Individual or Sole Proprietorship If checked, list Assumed Name, if any: _____
___ Partnership
___Corporation If checked, check one: ___For-Profit ___ Nonprofit
Also, check one: ___Domestic ___Foreign
___Other If checked, list business structure: _____

Printed Name of Contract Signatory: _____
Job Title: _____

(NOTE: This RFCSP solicits proposals to provide services under a contract which has been identified as "High Profile". Therefore, Respondent must provide the name of person that will sign the contract for the Respondent, if awarded.)

Provide any other names under which Respondent has operated within the last 10 years and length of time under for each:

_____
_____
_____

Provide address of office from which this project would be managed:
City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Annual Revenue: $_____

Total Number of Employees: _____

Total Number of Current Clients/Customers: _____

Briefly describe other lines of business that the company is directly or indirectly affiliated with:

_____
_____
_____

List Related Companies:

_____
_____
_____

2. **Contact Information:** List the one person who the City may contact concerning your proposal or setting dates for meetings.

Name: _____ Title: _____

Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Email: _____

3. Does Respondent anticipate any mergers, transfer of organization ownership, management reorganization, or departure of key personnel within the next twelve (12) months?

Yes ___ No ___

4. Is Respondent authorized and/or licensed to do business in Texas?

Yes ___ No ___ If "Yes", list authorizations/licenses.

_____

_____

5. Where is the Respondent's corporate headquarters located? _____

6. **Local/County Operation**: Does the Respondent have an office located in San Antonio, Texas?

Yes ___ No ___ If "Yes", respond to a and b below:

a. How long has the Respondent conducted business from its San Antonio office?

Years _____ Months_____

b. State the number of full-time employees at the San Antonio office.

If "No", indicate if Respondent has an office located within Bexar County, Texas:

Yes ___ No ___ If "Yes", respond to c and d below:

c. How long has the Respondent conducted business from its Bexar County office?

Years _____ Months_____

d. State the number of full-time employees at the Bexar County office. _____

7. **Debarment/Suspension Information**: Has the Respondent or any of its principals been debarred or suspended from contracting with any public entity?

   Yes ___ No ___ If "Yes", identify the public entity and the name and current phone number of a representative of the public entity familiar with the debarment or suspension, and state the reason for or circumstances surrounding the debarment or suspension, including but not limited to the period of time for such debarment or suspension.

   _____

   _____

8. **Surety Information**: Has the Respondent ever had a bond or surety canceled or forfeited?

   Yes ___ No ___ If "Yes", state the name of the bonding company, date, amount of bond and reason for such cancellation or forfeiture.

   _____

   _____

9. **Bankruptcy Information**: Has the Respondent ever been declared bankrupt or filed for protection from creditors under state or federal proceedings?

   Yes ___ No ___ If "Yes", state the date, court, jurisdiction, cause number, amount of liabilities and amount of assets.

   _____

   _____

10. **Disciplinary Action:** Has the Respondent ever received any disciplinary action, or any pending disciplinary action, from any regulatory bodies or professional organizations? If "Yes", state the name of the regulatory body or professional organization, date and reason for disciplinary or impending disciplinary action.

    _____

    _____

11. **Previous Contracts:**

    a. Has the Respondent ever failed to complete any contract awarded?

       Yes ___ No ___ If "Yes", state the name of the organization contracted with, services contracted, date, contract amount and reason for failing to complete the contract.

       _____

       _____

    b. Has any officer or partner proposed for this assignment ever been an officer or partner of some other organization that failed to complete a contract?
       Yes ___ No ___ If "Yes", state the name of the individual, organization contracted with, services contracted, date, contract amount and reason for failing to complete the contract.

       _____

       _____

    c. Has any officer or partner proposed for this assignment ever failed to complete a contract handled in his or her own name?

Yes ___ No ___ If “Yes”, state the name of the individual, organization contracted with, services contracted, date, contract amount and reason for failing to complete the contract.

_____

_____

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

REFERENCES

Provide three (3) references, that Respondent has provided services to within the past three (3) years. The contact person named should be familiar with the day-to-day management of the contract and be willing to respond to questions regarding the type, level, and quality of service provided.

Reference No. 1:

Firm/Company Name _____

Contact Name: _____ Title: _____

Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Date and Type of Service(s) Provided: _____

_____

Contact Email Address: _____

Reference No. 2:

Firm/Company Name _____

Contact Name: _____ Title: _____

Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Date and Type of Service(s) Provided: _____

_____

Contact Email Address: _____

Reference No. 3:

Firm/Company Name _____

Contact Name: _____ Title: _____

Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Date and Type of Service(s) Provided: _____

_____

Contact Email Address: _____

EXPERIENCE, BACKGROUND, QUALIFICATIONS

Prepare and submit narrative responses to address the following items. If Respondent is proposing as a team or joint venture, provide the same information for each member of the team or joint venture.

1. Identify whether this response is On-Premise or Off-Premise solution. Respondents have an option to propose On-Premise, Off-Premise or both solutions.
    a. On-Premise Solution
    b. Off-Premise Solution
    c. Both On-Premise / Off-Premise Solutions
        i. Respondent must submit separate proposals if desire is to submit both options.

2. Identify if the respondent is a private or public entity. Including any organizational classification changes that occurred over the last three (3) years.

3. Indicate the number of years Respondent has been in the business of providing Body Worn Camera solutions. Indicate if this is the Respondent's primary line of business. If not, state the Respondent's primary line of business.

    a. Clarify if years of service have in any way been influenced by an acquisition, merger, and/or organizational consolidation/restructuring in any form.

4. List other lines of business respondent is engaged in, aside from police body worn camera solutions.

5. List and describe three (3) relevant projects of similar size and scope to this RFCSP, performed over the past four years. Identify associated results or impacts of the project/work performed.

6. List all Body Worn Camera solution projects that are in progress with Respondent as of the proposal due date. For each project listed, give the target date of completion, and the contact name, phone number, and email address for the project manager.

7. Describe Respondent's specific experience with public entities clients, especially large municipalities or authorities. If Respondent has provided services for the City in the past, identify the name of the project, city department and contact for which Respondent provided those services.

8. If Respondent is proposing as a team, multi-vendor partnership, joint venture or has included sub-contractors, describe the rationale for selecting the team and the extent to which the team, joint ventures and/or sub-contractors have worked together in the past.

9. Provide an organizational chart showing how the Respondent proposes to staff the project. For each position reflected on the organizational chart:

    a. Identify each individual's relationship with the respondents organization – employee, contractor, 3rd party service/software provider
    b. Identify the number and professional qualifications (to include licenses, certifications, associations)
    c. Identify relevant experience on projects of similar size and scope
    d. State the primary work assignment and the percentage of time to be devoted to the project.
    e. Identify the length of service individual has been employed by the respondent's organization
    f. Provide resumes as an appendix to submitted proposal

10. Describe the company's support organization and volume of support inquiries managed per month over the past 2 years.

11. List the number of customers currently using proposed solution. Include company name, type of business, city & state.
    a. List any previous projects that Respondent has completed that integrate with other solutions and indicate which solutions/systems.
    b. What systems will Body Worn Cameras integrate with?

RFCSP ATTACHMENT C

CONTRACTS DISCLOSURE FORM

Contracts Disclosure Form may be downloaded at https://www.sanantonio.gov/eforms/atty/ContractsDisclosureForm.pdf .

Instructions for completing the Contracts Disclosure form are listed below:

1. Download form and complete all fields. Note: All fields must be completed prior to submitting the form.
2. Click on the “Print” button and place the copy in proposal response as indicated in the Proposal Checklist.

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

RFCSP ATTACHMENT D

LITIGATION DISCLOSURE FORM

Respond to each of the questions below by checking the appropriate box. Failure to fully and truthfully disclose the information required by this Litigation Disclosure form may result in the disqualification of your proposal from consideration or termination of the contract, once awarded.

Have you or any member of your Firm or Team to be assigned to this engagement ever been indicted or convicted of a felony or misdemeanor greater than a Class C in the last five (5) years?

Yes ___ No ___

Have you or any member of your Firm or Team to be assigned to this engagement been terminated (for cause or otherwise) from any work being performed for the City of San Antonio or any other Federal, State or Local Government, or Private Entity?

Yes ___ No ___

Have you or any member of your Firm or Team to be assigned to this engagement been involved in any claim or litigation with the City of San Antonio or any other Federal, State or Local Government, or Private Entity during the last ten (10) years?

Yes ___ No ___

If you have answered "Yes" to any of the above questions, please indicate the name(s) of the person(s), the nature, and the status and/or outcome of the information, indictment, conviction, termination, claim or litigation, as applicable. Any such information should be provided on a separate page, attached to this form and submitted with your proposal.

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

RFCSP ATTACHMENT E

SBEDA FORM(S)

FOLLOW ON DOCUMENT ATTACHED AS SEPARATE DOCUMENT

RFCSP ATTACHMENT F

PRICING SCHEDULE

This offer will remain in effect for a period of 180 calendar days from the bid opening date and is irrevocable unless it is in the City's best interest to do so.

The City will evaluate both On-Premise and Off-Premise solutions. Vendor will submit proposals for On-Premise, Off-Premise or both solutions. Each will be evaluated on its own merits. The City reserves the right to award based on a determination of what solution best meets the City's business need.

1. ALL OR NONE PROPOSAL PRICE SCHEDULE: OFFSITE SOLUTION

Note: Prices offered shall not include applicable federal, state and local taxes.

Item No.	Description	Manufacturer & Product No.	Quantity	Unit Price Excluding Tax	Total Price Excluding Tax
1.	Body Worn Video Cameras		251 each	$	$
2.	Evidence Transfer Equipment for 251 cameras		251 each	$	$
3.	Licenses		251 each	$	$
4.	Annual Offsite Data Download Storage, Access, and Maintenance Costs		Year 1	$	$
5.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 1	$	$
				Grand Total of Lines 1 - 5 All or None	$

2. ADDITIONAL PURCHASES

Item No.	Description	Manufacturer & Product No.	Quantity	Unit Price Excluding Tax
1.	Body Worn Video Camera		1 each	$
2.	Evidence Transfer Equipment		1 each	$
3.	License		1 each	$
4.	Annual Offsite Data Download Storage, Access, and Maintenance Costs		Year 2	$
5.	Annual Offsite Data Download Storage, Access, and Maintenance Costs		Year 3	$
6.	Annual Offsite Data Download Storage, Access, and Maintenance Costs		Year 4	$
7.	Annual Offsite Data Download Storage, Access, and Maintenance Costs		Year 5	$

8.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 2	$
9.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 3	$
10.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 4	$
11.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 5	$
12.	Battery		1 each	$
13.	On-Device Storage		1 each	$
14.	SD Card		1 each	$
15.	Cable		1 each	$

3. EMERGENCY TWENTY-FOUR HOUR SERVICE CONTACT

Name _____

Telephone Number _____

Alternate Contact _____

Telephone Number _____

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

4. **ALL OR NONE PROPOSAL PRICE SCHEDULE: ONSITE SOLUTION**

Note: Prices offered shall not include applicable federal, state and local taxes.

Item No.	Description	Manufacturer & Product No.	Quantity	Unit Price Excluding Tax	Total Price Excluding Tax
1.	Body Worn Video Cameras		251 each	$	$
2.	Evidence Transfer Equipment for 251 cameras		251 each	$	$
3.	Licenses		251 each	$	$
4.	Server Licenses (if applicable)				
5.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 1	$	$
				Grand Total of Lines 1 - 5 All or None	$

5. **ADDITIONAL PURCHASES**

Item No.	Description	Manufacturer & Product No.	Quantity	Unit Price Excluding Tax
1.	Body Worn Video Camera		1 each	$
2.	Evidence Transfer Equipment		1 each	$
3.	License		1 each	$
4.	Server License Renewal (if applicable)		Year 2	
5.	Server License Renewal (if applicable)		Year 3	
6.	Server License Renewal (if applicable)		Year 4	
7.	Server License Renewal (if applicable)		Year 5	
8.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 2	$
9.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 3	$
10.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 4	$
11.	Annual Warranty with all Patches, Hardware, and Software including Upgrades		Year 5	$

12.	Battery		1 each	$
13.	On-Device Storage		1 each	$
14.	SD Card		1 each	$
15.	Cable		1 each	$

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

RFCSP ATTACHMENT G

BUSINESS REQUIREMENTS

BUSINESS REQUIREMENTS			
CAMERA			
MODEL NAME: _____ **Height _____ Width _____** **Weight _____** **MODEL NUMBER:_____** **Thickness ____**			
RFCSP NUMBER	**SPECIFICATION**	**REQUIREMENT: MINIMUM (M) OR PREFERED (P)**	**YES NO**
1.	Meet Military specifications (MIL-STD-810G) or equivalent	**M**	
1a.	Storage Temperature Range	**M**	
1b.	Vibration	**M**	
1c.	Thermal Shock	**M**	
1d.	Dust	**M**	
1e.	Solar Radiation	**M**	
2.	Provide operating temperature range specifications.	**M**	
3.	Drop Test rating of 6 ft	**M**	
4.	Be water-resistant to IPX Rating 4	**M**	
5.	Have flexible mounting options on the officer's uniform with a forward facing field of view:	**M**	
5a.	Chest	**M**	
5b.	Lapel	**M**	
5c.	Point of view/head	**P**	
5d..	Windshield Mount	**P**	
6.	Have Video Recording Definition of 640x480 (30FPS)	**M**	
7.	Have Date and Time Stamp on video file	**M**	
7a.	Be capable of recording the devices geolocation via GPS locator	**P**	
8.	Be able to record at least 4 hours uninterrupted of continuous recording.	**M**	
9.	Be able to store a total of 8 hours of video	**M**	

9a.	Have 64GB preferred of internal memory.	**P**	
10.	Have a battery life of at least 12 hours.	**M**	
11.	Be able to synchronize time to an external time service.	**P**	
12.	Have industry standard security in place equal or greater than CJIS standards version 5.3 or later and policy standard dated 8/4/14 for minimum camera design.	**M**	
13.	Have color video.	**M**	
14.	Have a minimum field of view of 68 degrees.	**M**	
15.	Be compatible with Windows 7. .	**M**	
16.	Have USB cable computer connectivity.	**M**	
17.	Have a noise canceling internal microphone.	**M**	
18.	Have a one touch recording activation button.	**M**	
18a.	Have Mute Functionality	**M**	
18b.	Have Play Functionality .	**M**	
18c.	Have Resume Functionality	**M**	
19.	Have audio or visual or vibrating alert to confirm when it is turned off and on.	**M**	
20.	Have safeguards to prevent accidentally turning it on or off.	**M**	
21.	Have enhanced image quality and low-light capability to mirror the human eye.	**M**	
22.	Have the ability to be activated automatically via Department defined cue (overhead lights, vehicle door opening, etc.).	**M**	
23.	Allow for video categorization in the field.	**M**	
24.	Each Body Worn Camera Unit must have its own unique ID that can be registered to a specific Officer (i.e. by badge number, etc.)	**M**	

SYSTEM			
RFCSP NUMBER	**SPECIFICATION**	**REQUIREMENT: MINIMUM (M) OR DESIRED (D)**	**YES NO**
1.	Capable of handling over 2000 user/Officer accounts	**M**	
2.	Must be able to create individual user accounts with varying degrees of access	**M**	
2a.	Administrator accounts	**M**	
2b.	Basic user accounts	**M**	
3.	Record at a minimum HE-AAC (High-Efficiency Advance Audio Coding) Audio Format or MP3.	**M**	
4.	Allow officer to initiate video file transfer.	**M**	
5.	Allow officer to upload through docked video transfer via auto-upload to secured evidence database.	**M**	
5a.	Allow officer to upload through wireless video transfer via auto-upload to secured evidence database.	**D**	
6.	Be able to integrate with Active Directory.	**M**	
7.	Be capable of categorizing a call for service or field activity categories.	**M**	
8.	Be customizable to allow for the minimum number of days that a recording shall be retained in the system.	**M**	
9.	Have capability of at least 15 seconds of Pre-Event video buffering.	**M**	
10.	Self-contained memory that cannot be modified or altered upon view.	**M**	
10a.	Have solid-state memory Enhancement	**D**	
11.	Have access control that requires security permission for viewing and copying a video file. .	**M**	
12.	Provide safeguards to ensure that the	**M**	

	camera cannot record over or delete video files.		
13.	Be able to burn expired videos or copies being requested to DVD and/or other means of export.	**M**	
14.	Be a secure and tamper-proof device.	**M**	
15.	Have standard software allowing for an officer to enter additional information to an existing video recording.	**M**	
16.	Have industry standard security in place equal or greater than CJIS standards version 5.3 or later and policy standard dated 8/4/14 for minimum camera design.	**M**	
17.	Ensure an unalterable chain-of-custody that records all access and activity of the system and video.	**M**	
18.	Be customizable to allow for Department retention schedules.	**M**	
19.	Have import, export, share, and record etc. functions for supervisory users to manage and share digital evidence.	**M**	
20	Include video editing software that will:	**D**	
20a.	Redact digital media.	**D**	
20b.	Render segments of digital media.	**D**	
20c.	Create event timelines and flags in digital media.	**D**	
20d.	Redact documents (similar to PDF Professional editor).	**D**	
21.	Provide a minimum of 2x or double redundancy for all stored digital media and associated entries.	**M**	
BACKEND SYSTEM			
RFCSP NUMBER	**SPECIFICATION**	**REQUIREMENT: MINIMUM (M) OR DESIRED (D)**	**YES NO**
1.	Automatic Video transfers from Body Worn Camera Unit into Local On-Site Storage Solution and/or Vendor Hosted Cloud Storage Solution.	**M**	
2.	Automatic Video transfers must be	**M**	

	performed via multi-charging/docking stations and/or USB cable via individual desktop computer.		
2a.	Ethernet connection.	**M**	
2b.	USB/Multi-docking station software must have throttle control capability when connected to network so as to not overload network pipe and allow for seamless upload and charging of captured media and battery	**M**	
2c.	Minimum 256bit AES Encryption in storage and transport.	**M**	
3.	Video Playback Backend System.	**M**	
3a.	Fast Forward and Rewind.	**M**	
3b.	Fast Forward and Rewind Slow.	**M**	
3c.	Advance forward and backward frame by frame.	**M**	
3d.	Must have Video Screen Capture capability.	**M**	
3e.	Must have Desktop Player compatibility with Windows Media Player, Quick Time, and VLC media player.	**M**	
3f.	Must have the ability to digitally enhance a captured image/video without altering the original.	**M**	
4.	For On-Site Backend System should have a recommended Disaster Recovery or Failover strategy that allows for periodic testing and validation.	**M**	
5.	Source code and encryption information to be held in escrow	**M**	
LIST SYSTEM ENHANCEMENTS			

RFCSP ATTACHMENT H

SIGNATURE PAGE

Respondent, and co-respondent, if any, must complete City's Certified Vendor Registration (CVR) Form prior to the due date for submission of proposals. The CVR Form may be accessed at: http://www.sanantonio.gov/purchasing/ or the direct link at: http://www.sanantonio.gov/purchasing/saeps.aspx

By submitting a proposal, by paper (hardcopy), Respondent represents that:

If Respondent is a corporation, Respondent will be required to provide a certified copy of the resolution evidencing authority to enter into the contract, if other than an officer will be signing the contract.

IF AWARDED A CONTRACT IN RESPONSE TO THIS RFCSP, RESPONDENT CERTIFIES THAT IT IS ABLE AND WILLING TO COMPLY WITH THE VENUE, THE INSURANCE AND INDEMNIFICATION REQUIREMENTS SET OUT IN RFCSP EXHIBITS 1 & 2. A FAILURE TO COMPLY WITH THE VENUE, JURISDICTION AND ARBITRATION, INTELLECTUAL PROPERTY, UNDISCLOSED FEATURES, OWNERSHIP AND LICENSES, CERTIFICATIONS, ACCEPTANCE CRITERIA, INSURANCE AND INDEMNIFICATION REQUIREMENTS OF THIS RFCSP WILL RESULT IN REJECTION OF THE PROPOSAL. RESPONDENT UNDERSTANDS AND AGREES THAT THE TERMS CONTAINED IN THIS RFCSP ARE PART OF THE FINAL CONTRACT AND PREVAIL OVER ANY CONFLICTING TERMS IN ANY DOCUMENT FURNISHED BY RESPONDENT, EVEN IF NOT EXPRESSLY PROVIDED IN THE BODY OF THE CONTRACT.

If awarded a contract in response to this RFCSP, Respondent will be able and willing to comply with all representations made by Respondent in Respondent's proposal and during Proposal process.

Respondent has fully and truthfully submitted a Litigation Disclosure form with the understanding that failure to disclose the required information may result in disqualification of proposal from consideration.

Respondent agrees to fully and truthfully submit the Respondent Questionnaire form and understands that failure to fully disclose requested information may result in disqualification of proposal from consideration or termination of contract, once awarded.

To comply with the City's Ethics Code, particularly Section 2-61 that prohibits a person or entity seeking a City contract - or any other person acting on behalf of such a person or entity - from contacting City officials or their staff prior to the time such contract is posted as a City Council agenda item.

(S)he is authorized to submit this proposal on behalf of the entity.

Acknowledgement of Prohibition regarding Campaign and Officeholder Contributions

I acknowledge that this contract has been designated a "high-profile" contract. I have read and understand the provisions regarding high profile contracts that appear on the cover page of this RFCSP.

If submitting your proposal by paper, complete the following and sign on the signature line below. Failure to sign and submit this Signature Page will result in rejection of your proposal.

_____
Respondent Entity Name

Signature: _____

Printed Name: _____

Title: _____

Email Address:_____

(NOTE: If proposal is submitted by Co-Respondents, an authorized signature from a representative of each Co-Respondent is required. Add additional signature blocks as required.)

_____
Co-Respondent Entity Name

Signature: _____

Printed Name: _____

Title: _____

Email Address:_____

THE REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY

RFCSP ATTACHMENT I

VOSBPP TRACKING FORM

Veteran-Owned Small Business Preference Program (VOSBPP) Ordinance Pursuant to Ordinance No. 2013-12-05-0864, effective for solicitations issued after January 15, 2014, all solicitations issued by the City are subject to tracking of Veteran Owned Small Business (VOSB) participation.

For more information on the program, refer to the Veteran-Owned Small Business Program Tracking Form attached to this solicitation.

Respondent must complete and return the attached Veteran-Owned Small Business Program Tracking Form.

FOLLOW ON DOCUMENT ATTACHED AS SEPARATE DOCUMENT

City of San Antonio

Veteran-Owned Small Business Program Tracking Form

Authority. The City of San Antonio Veteran-Owned Small Business Preference Program Ordinance 2013-12-05-0864 adopted a veteran-owned small business preference program for specific contracting categories for solicitations issued after January 15, 2014.

Tracking. This solicitation is not eligible for a preference based on status as a veteran-owned small business (VOSB). Nevertheless, in order to determine whether the program can be expanded at a later date, the City tracks VOSB participation at both prime contract and subcontract levels.

Certification. The City relies on inclusion in the database of veteran-owned small businesses (VOSB) maintained by the U.S. Small Business Administration to verify VOSB status; however, veteran status may also be confirmed by certification by another public or private entity that uses similar certification procedures.

Definitions. The program uses the federal definitions of veteran and veteran-owned small business found in 38 CFR Part 74.

- The term “veteran” means a person who served on active duty with the U.S. Army, Air Force, Navy, Marine Corps, Coast Guard, for any length of time and at any place and who was discharged or released under conditions other than dishonorable. Reservists or members of the National Guard called to federal active duty or disabled from a disease or injury incurred or aggravated in line of duty or while in training status.

- A veteran-owned small business is a business that is not less than 51 percent owned by one or more veterans, or in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; the management and daily business operations of which are controlled by one or more veterans and qualifies as “small” for Federal business size stand purposes.

The program does not distinguish between a veteran and a service-disabled veteran-owned business and is not limited geographically.

COMPLETE THE FOLLOWING FORM AND SUBMIT IT WITH YOUR BID/PROPOSAL.

City of San Antonio

Veteran-Owned Small Business Program Tracking Form

SOLICITATION NAME/NUMBER: _____

Name of Respondent:		
Physical Address:		
City, State, Zip Code:		
Phone Number:		
Email Address:		
Is Respondent certified as a VOSB with the U.S. Small Business Administration? (circle one)	Yes	No
If yes, provide the SBA Certification #		
If not certified by the SBA, is Respondent certified as a VOSB by another public or private entity that uses similar certification procedures? (circle one)	Yes	No
If yes, provide the name of the entity who has certified Respondent as a VOSB. Include any identifying certification numbers.		
Participation Dollar Amount		

Is Respondent subcontracting with a business that is certified as a VOSB? (circle one)	Yes	No
Name of **SUBCONTRACTOR** Veteran-Owned Small Business:		
Physical Address:		
City, State, Zip Code:		
Phone Number:		
Email Address:		
Is **SUBCONTRACTOR** certified as a VOSB with the U.S. Small Business Administration? (circle one)	Yes	No
If yes, provide the SBA Certification #		
If not certified by the SBA, is **SUBCONTRACTOR** certified as a VOSB by another public or private entity that uses similar certification procedures? (circle one)	Yes	No
If yes, provide the name of the entity who has certified **SUBCONTRACTOR** as a VOSB. Include any identifying certification numbers.		
Participation Dollar Amount		

ACKNOWLEDGEMENT

THE STATE OF TEXAS

I certify that my responses and the information provided on Veteran-Owned Small Business Program Tracking Form are true and correct to the best of my personal knowledge and belief and that I have made no willful misrepresentations on this form, nor have I withheld any relevant information in my statements and answers to questions. I am aware that any information given by me on this Veteran-Owned Small Business Program Tracking Form may be investigated and I hereby give my full permission for any such investigation. I fully acknowledge that any misrepresentations or omissions in my responses and information may cause my offer to be rejected.

BIDDER/RESPONDENT'S FULL NAME:

_____

(Print Name) Authorized Representative of Bidder/Respondent

_____

(Signature) Authorized Representative of Bidder/Respondent

_____

Title

_____

Date

This Veteran-Owned Small Business Program Tracking Form must be submitted with the Bidder/Respondent's bid/proposal.

RFCSP ATTACHMENT J

PROPOSAL CHECKLIST

Use this checklist to ensure that all required documents have been included in the proposal and appear in the correct order.

Document	Initial to Indicate Document is Attached to Proposal
Table of Contents	
Proposal RFCSP Attachment A	
Respondent Questionnaire RFCSP Attachment B	
Discretionary Contracts Disclosure form RFCSP Attachment C	
Litigation Disclosure RFCSP Attachment D	
*SBEDA Form RFCSP Attachment E; and Associated Certificates, if applicable	
Pricing Schedule RFCSP Attachment F	
Business Requirements RFCSP Attachment G	
*Signature Page RFCSP Attachment H	
*VOSBPP Tracking Form RFCSP Attachment I	
Proposal Checklist RFCSP Attachment J	
Proof of Insurability (See RFCSP Exhibit 1) Insurance Provider's Letter Copy of Current Certificate of Insurance	
Financial Information	
One (1) Original, Twelve (12) Copies and one (1) CD, one (1) Flash Drive of entire proposal in PDF format.	

*Documents marked with an asterisk on this checklist require a signature. Be sure they are signed prior to submittal of proposal.