JK
12/19/13
Agenda Item #8

AN ORDINANCE 2013-12-19-0896

ACCEPTING THE PROPOSAL FROM SAS INSTITUTE INC. TO PROVIDE THE SAN ANTONIO POLICE DEPARTMENT WITH A FUSION INTELLIGENCE SYSTEM FOR A COST OF $249,700.00, FROM THE 2011 STATE HOMELAND SECURITY PROGRAM GRANT AND THE 2012 URBAN AREA SECURITY INITIATIVE.

* * * * *

WHEREAS, San Antonio Police Department (SAPD) supports a Criminal Intelligence Unit and a Major Urban Area Fusion Center with the mission of engaging in intelligence led policing strategies to combat crime and other threats to our community; and

WHEREAS, SAPD requires a system that will provide SAPD the ability to track, record, and improve documented interactions with confidential informants; and

WHEREAS, SAS Institute, Inc., can provide a system which includes functional requirements to provide both the SAPD Intelligence Unit and the Southwest Texas Fusion Center with an electronic repository for information and intelligence in compliance with federal regulations; **NOW THEREFORE,**

BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF SAN ANTONIO:

SECTION 1. An agreement with the SAS Institute to provide the San Antonio Police Department with Fusion Intelligence System, for a cost of $249,700.00, is hereby approved. A copy of the agreement is attached hereto and is incorporated by reference as **Attachment 1**.

SECTION 2. Fund 2606520017 entitled "HOMELAND SECURITY GRANT - 2011" and Internal Order 120000000088 and fund 2606520021 entitled "2012 UASI" and Internal Order 120000000087 are hereby designated for use in the accounting for the fiscal transaction in authorization of this contract.

SECTION 3. The sum of $239,160.00 and $10,540.00 is hereby appropriated in the above designated funds and internal orders. Payment is authorized to SAS Institute, Inc. upon issuance of a Purchase Order.

SECTION 4. The financial allocations in this Ordinance are subject to approval by the Director of Finance, City of San Antonio. The Director of Finance, may, subject to concurrence by the City Manager or the City Manager's designee, correct allocations to specific SAP Fund Numbers, SAP Project Definitions, SAP WBS Elements, SAP Internal Orders, SAP Fund Centers, SAP Cost Centers, SAP Functional Areas, SAP Funds Reservation Document Numbers, and SAP GL Accounts as necessary to carry out the purpose of this Ordinance.

JK
12/19/13
Agenda Item #8

SECTION 5. This ordinance shall be effective immediately upon passage by eight affirmative votes; otherwise it shall be effective on the tenth day after passage hereof.

PASSED and APPROVED this 19th day of December 2013.

M A Y O R
Julián Castro

ATTEST:

Leticia M. Vacek, City Clerk

APPROVED AS TO FORM:

By:

Robert F. Greenblum, City Attorney

Agenda Item:	**8 (in consent vote: 6, 7, 8, 9, 10, 1010A, 1010B, 11, 13, 1313A, 1313B, 1313C, 14, 15, 16, 17, 18, 19, 20, 21, 23, 24, 25, 26, 27, 28, 29, 30, 32, 34, 36, 37)**
Date:	12/19/2013
Time:	10:01:40 AM
Vote Type:	Motion to Approve
Description:	An Ordinance accepting the proposal from SAS Institute Inc. to provide the San Antonio Police Department with a Fusion Intelligence system for a cost of $249,700.00, from the 2011 State Homeland Security Program grant and the 2012 Urban Area Security Initiative. [Ben Gorzell, Chief Financial Officer; Troy Elliott, Director, Finance]
Result:	Passed

Voter	Group	Not Present	Yea	Nay	Abstain	Motion	Second
Julián Castro	Mayor		x				
Diego Bernal	District 1		x				x
Ivy R. Taylor	District 2		x				
Rebecca Viagran	District 3	x					
Rey Saldaña	District 4		x			x	
Shirley Gonzales	District 5		x				
Ray Lopez	District 6		x				
Cris Medina	District 7		x				
Ron Nirenberg	District 8		x				
Joe Krier	District 9		x				
Carlton Soules	District 10		x				

INTEGRATION AGREEMENT FOR INTEGRATED INFORMATION AND INTELLIGENCE MANAGEMENT LAW ENFORCEMENT SOLUTION

REQUEST FOR COMPETITIVE SEALED PROPOSAL ("RFCSP")
NO.: 6100003495 (RFCSP-013-096)

BETWEEN THE CITY OF SAN ANTONIO, TEXAS **("CITY")**
AND
SAS INSTITUTE INC.

STATE OF TEXAS §
§
COUNTY OF BEXAR §

This Agreement is entered into by and between the City of San Antonio, Texas, a home-rule municipal corporation (City), and SAS Institute Inc., (SAS), both of which may be referred to herein collectively as the "Parties".

The Parties hereto severally and collectively agree, and by the execution hereof are bound, to the mutual obligations herein contained and to the performance and accomplishment of the tasks hereinafter described.

1.0 CONTRACT DOCUMENTS

1.1 The terms and conditions for performance and payment of compensation for this Agreement are set forth in the following contract documents, true and correct copies of which are attached hereto and fully incorporated herein for all purposes, and shall be interpreted in the order of priority as appears below:

a. This Integration Agreement, including;

b. SAS License Attachment (Exhibit D);

c. SAS Statement of Work (SOW) (Exhibit B);

d. City's Request for Competitive Sealed Proposal No.: 6100003495 (RFCSP-013-096) (Exhibit A), including all attachments, addendums and clarification statements thereto; and

e. SAS proposal submitted in response to City's RFCSP (Exhibit C).

2.0 ENTIRE AGREEMENT

This Agreement, together with its exhibits, if any, constitutes the final and entire agreement between the parties hereto and contains all of the terms and conditions agreed upon. No other agreements, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or to bind the parties hereto, unless the same are in writing, dated subsequent to the date hereto, and duly executed by the parties.

EXECUTED and AGREED to as of the dates indicated below. This Agreement may be executed in multiple copies, each of which shall constitute an original.

CITY OF SAN ANTONIO	SAS INSTITUTE INC.
_____	_____
Print Name: _____	Print Name: Victoria P. Clayton
Title: _____	Title: Senior Manager, Contracts Administration, SAS Institute Inc.
Date: _____	Date: November 25, 2013

Approved as to Form:

_____
Assistant City Attorney

LEGAL

License Attachment

This License Attachment ("LA") is between SAS Institute Inc. ("SAS") and the City of San Antonio ("Customer") in connection with (i) Customer's license of SAS® software listed on Attachment I to this LA ("Software") and (ii) the provision of certain services by SAS which are described on Attachment II to this LA ("Services"). This LA is made a part of the Integration Agreement ("Integration Agreement") executed by the parties in connection with Customer's Request for Competitive Sealed Proposal (RFCSP-013-096) ("RFP"). To the extent the terms contained in this LA conflict with the RFP, this LA shall control.

1. **License Grant; Authorized Use**. SAS grants Customer a nonexclusive, nontransferable and nonassignable license to use the Software with the designated operating systems specified on Attachment I to this LA. SAS also grants Customer a limited license to the Work Product (as defined in Attachment II) resulting from any Services provided hereunder, to the extent more fully set forth on Attachment II. Except as otherwise provided in the LA, the Software may be accessed only by Customer's employees and on site contractors ("Users") doing work in the Territory solely for Customer. The license is an annual license renewed at the mutual agreement of the parties. Renewal is accomplished by SAS sending an invoice for the applicable Software license renewal fees and Customer paying the invoice.

1.1 **Reserved.**

1.2 **Territory; Report Access.** Customer may install and use the Software (a) within the territory listed on Attachment I ("Territory"); (b) on a portable computer in countries outside the Territory for up to three (3) months of an annual license period; and (c) in a manner allowing any party in or outside the Territory limited access to Software applications to view reports showing results of Customer's analysis of Customer's data ("Reports"). Customer may allow this limited Report viewing via the internet, Customer's intranet or terminal emulation sessions.

1.3. **Other Uses of the Software.**

This LA describes standard rights of use. Attachment I also includes special use rights and limits related specifically to the Software. SAS grants no usage rights beyond those specifically listed in this LA. By way of example, the following uses are prohibited unless specifically set forth on Attachment I or a written amendment to this LA: (a) installation or use outside the Territory; (b) use for the benefit of a third party in exchange for compensation; (c) use in application or data service provision, outsourcing, time-sharing, data or information technology management, or other similar arrangements; (d) use to process third party data; or (e) allowing any party other than Users to use, edit, modify, or otherwise access underlying Software, or to perform free form programming with the Software.

2. **Authorized Hardware.** Customer shall install the Software only on hardware authorized under this LA ("Authorized Hardware"). If the Software is licensed for use on mainframe or server hardware, Authorized Hardware is hardware located on Customer's premises that Customer identifies to SAS by type and CPU number. If the Software is licensed for use on personal computers, Authorized Hardware is hardware owned or leased by Customer or its employees.

3. **Fees.** License fees for each Software product are based on the applicable pricing metric and the usage rights and limits set forth on Attachment I. First year fees, pricing metrics and any special usage rights or limits are listed on Attachment I. Renewal fees are listed on invoices and may vary each year. Prior to any license renewal period, SAS may propose pricing metric changes. Some pricing metrics are based on use of certain Software offerings as an integrated solution. Accordingly, the Software components in these offerings may be used only through the Software under which they are bundled and Customer may not use or deploy any individual component as a replacement for other SAS software.

4. **Product Authorization Code.** Customer may allow Users to access Software licensed to Customer for which Customer receives a Product Authorization Code. Customer shall not allow Users to install or attempt to use other products contained on media received from SAS. The "Product Authorization Code" is a component of the Software that enables the Software to operate for the applicable license period. At each new license period, or if required as a result of changes in Authorized Hardware or Software, Customer must apply a new Product Authorization Code to keep the Software operating. SAS is not required to provide the Product Authorization Code if Customer is in breach of this LA or has not paid any undisputed amounts due under this LA. SAS is not liable for damages caused by the resulting Software interruption. Customer may allow only Users to access the Product Authorization Code. Customer acknowledges and agrees that the Product Authorization Code is SAS' confidential and proprietary information. This section shall not be considered in conflict with the "Undisclosed Features" section of the RFP.

5. **Copying.** Customer may copy the Software only for (a) disaster recovery and back-up purposes, and (b) installation of personal computer Software authorized hereunder. All copies remain the property of SAS. Customer may deliver a copy of the Software to a disaster recovery contractor to perform temporary disaster recovery work for Customer. Customer shall give SAS the name and address of the disaster recovery contractor before delivery. The identical copyright notices and any other proprietary rights notices found on the original Software media must be reproduced on all copies authorized under this Section.

6. **Title; Source Code.** Title to the Software and its documentation remains with SAS and its licensors at all times. Copyright notices and other proprietary rights notices in the Software shall not be deleted or modified. Neither this LA, nor the Integration Agreement (and related attachments thereto) transfers any ownership rights to Customer. Source code from which the Software object code is derived ("Source Code") is not being provided and is a trade secret of SAS and SAS' licensors to which access is not authorized. Neither Customer nor any other User shall reverse engineer, reverse assemble or decompile the Software or in any way attempt to recreate the Source Code, except and only to the extent applicable laws specifically prohibit such restriction.

7. **Technical Support.** During the term of the Software license, SAS will use reasonable efforts, either by telephone or in writing, to help Customer solve specific problems with installation or use of the Software within the Territory. Customer may obtain on-site Software support from SAS by executing additional paperwork with SAS and paying applicable additional fees to SAS. It may not be possible for SAS to solve all problems or correct all errors in the Software. From time to time, SAS may make available, and Customer agrees to use reasonable efforts to install, new releases, updates and corrective code. During ongoing Software development, SAS may add, change or delete individual components or functionality in new releases. Such Software modifications shall be subject to the terms of this LA. If Customer chooses not to install the most current release of the Software, the level of technical support may diminish over time.

8. **Payment.**

EXHIBIT D

8.1 **Invoices.** SAS will invoice Customer (a) prior to each applicable license period, for any Software license fees due and (b) any Services fees due. Payment terms for all invoices are net thirty (30) days. License fees do not include taxes. SAS will use reasonable efforts to include all taxes applicable to Customer on the relevant invoice and Customer agrees to pay such taxes to SAS; however, Customer is responsible for taxes on its licensing of the Software. Customer is not responsible for taxes based on SAS' income. Except as otherwise allowed in this LA, refunds are not available after the Product Authorization Code has been provided.

8.2 **License Fee Calculations; Upgrades.** Customer agrees to (a) keep records of where the Software is being used and the extent of usage of the Software relative to the pricing metric and the applicable usage rights and limits, and (b) provide a copy of such records to SAS upon reasonable request. Customer may call or write SAS to change operating systems, Authorized Hardware or any factor affecting the applicable pricing metric or any applicable usage rights. These changes may result in additional license fees which are effective and will be invoiced as of the time of the change.

8.3 **Third Party Payments.** Customer may, by written notice to SAS, designate a third party to pay license fees on Customer's behalf. Customer shall be responsible for any related charges assessed by such third party. When a third party is designated by Customer to pay fees under this LA, SAS will send its standard notices regarding fees only to such third party, and all payments due under this LA will remain Customer's ultimate responsibility.

9. Limited Warranties and Representations.

9.1 **Warranties by SAS; Remedies.**

9.1.1 SAS warrants that it has the right to license the Software to Customer. The exclusive remedy for breach of this warranty is set forth in Section 11 (Indemnification).

9.1.2 SAS warrants that each production release of the Software shall substantially conform to its documentation including any updates thereto, and the Software and the media on which it is installed shall be free of software viruses when received by Customer. As the exclusive remedy for breach of these warranties, SAS, at its option, shall: (a) repair the Software; (b) replace the Software; or (c) terminate the Software license and refund the fees paid for the Software at issue during the then-current license period.

9.2 **Warranty Disclaimers. SAS AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ARISING AS A RESULT OF CUSTOM OR USAGE IN THE TRADE OR BY COURSE OF DEALING. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, SAS AND ITS LICENSORS DO NOT WARRANT OR REPRESENT THAT THE SOFTWARE WILL RESULT IN COMPLIANCE, FULFILLMENT OR CONFORMITY WITH THE LAWS, RULES, REGULATIONS, REQUIREMENTS OR GUIDELINES OF ANY GOVERNMENTAL AGENCY. SAS' LICENSORS PROVIDE THEIR SOFTWARE "AS IS." NOTHING IN THIS SUBSECTION NEGATES THE EXPRESS WARRANTIES SAS PROVIDES IN THIS LA.**

9.3 **Representations by Customer.** Customer represents it shall (a) implement procedures to verify accuracy of data input and output while using the Software, and (b) inform all parties authorized to use the Software of the relevant terms of this LA and any related user documentation, and be responsible for their adherence to such terms. Customer agrees that the Software and Services, in and of themselves, will not ensure compliance with laws.

10. Exclusions of Damages; Limitation of Liability.

10.1 **Exclusions of Damages. NEITHER CUSTOMER, SAS, NOR SAS' LICENSORS ARE LIABLE FOR SPECIAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, PUNITIVE, OR RELIANCE DAMAGES (ARISING IN TORT, CONTRACT OR OTHERWISE), EVEN IF THEY HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. NEITHER SAS NOR SAS' LICENSORS ARE LIABLE FOR ANY CLAIM AGAINST THE CUSTOMER BY A THIRD PARTY RELATING TO USE OF THE SOFTWARE, EXCEPT AS SET FORTH IN SECTION 11 (INDEMNIFICATION). SAS' LICENSORS ARE NOT LIABLE FOR DIRECT DAMAGES (ARISING IN TORT, CONTRACT OR OTHERWISE) AND DISCLAIM ANY LIABILITY CONNECTED WITH USE OF THE SOFTWARE. THE PARTIES MAKE THESE EXCLUSIONS IN CONSIDERATION OF THE FEES PAID AND LICENSES GRANTED IN CONNECTION WITH THIS LA.**

10.2 **Limitation of Liability. THE TOTAL AMOUNT CUSTOMER MAY RECOVER FOR ANY CLAIMS OR DAMAGES OF ANY KIND RELATING TO THIS LA OR THE INTEGRATION AGREEMENT (INCLUDING ALL ATTACHMENTS THERETO) IS LIMITED IN THE AGGREGATE TO THE FEES PAID FOR THE SOFTWARE AT ISSUE DURING THE RELEVANT LICENSE PERIOD OR FOR THE SERVICES AT ISSUE.**

10.3 **Applicability.** The limitations in this Section shall apply even if any of the warranties provided in Section 9 fail of their essential purpose. Some jurisdictions do not allow limitations of liability or exclusions for incidental or consequential damages, so certain provisions of this Section may not apply to Customer; however, they apply to the greatest extent permitted by applicable law.

11. Indemnification. As set forth on Exhibit A of the Integration Agreement.

12. Termination; Expiration. Customer may terminate an annual license for any Software at any time. SAS may terminate this LA immediately for any violation by Customer of SAS' intellectual property rights. For any other breaches, SAS may terminate the Software license for a breach of this LA if not cured within thirty (30) days of SAS' written notice. Obligations in this LA that by their nature are continuing will survive termination or expiration. Upon termination or expiration of each Software license hereunder, or when a User, Related Entity or disaster recovery contractor is no longer authorized to access the Software, Customer agrees to reclaim, delete, and destroy the Software at issue, along with any related user documentation.

13. Governing Law; Export and Import Restrictions. The laws of Texas, excluding choice of law provisions, govern this LA. SAS hereby notifies Customer that United States export laws and regulations apply to the Software. Both parties agree to comply with these and other applicable export and import laws and regulations. The parties expressly agree to exclude from this LA and the Integration Agreement the United Nations Convention on Contracts for the International Sale of Goods.

14. General.

14.1 **Severability.** If a court of competent jurisdiction finds any part unenforceable, that part is excluded, but the remainder of this LA stays in full force and effect.

14.2 **No Waiver.** Failure to require compliance with a part of the LA is not a waiver of that part. Nothing in this subsection waives any remedy SAS may have under the LA at law, in equity, or otherwise.

14.3 **Non-assignment.** Customer may not assign this LA or any of its rights or obligations hereunder without SAS' written permission, which permission will not be unreasonably withheld.

14.4 **Audit.** Upon fifteen (15) business days' notice to Customer, SAS will have the right to conduct an on-site audit during Customer's normal business hours to verify compliance with the terms and conditions of this LA. Customer shall cooperate with SAS by: (a) making applicable records available; (b) providing copies of the records requested; and (c) directing all agents to cooperate. If the audit reveals that Customer owes additional license fees, Customer shall pay the amounts owed and SAS' reasonable expenses in conducting the audit.

14.5 **Injunctive Relief.** Breach of SAS' or SAS' licensors' intellectual property rights will lead to damages not adequately remedied by an award of money; therefore, SAS may protect those intellectual property rights through temporary restraining orders or injunctions, without the obligation of posting bond.

15. Complete Agreement; Modifications. This LA, the Integration Agreement (and all attachments thereto), and invoices arising under it are the parties' complete and exclusive statement relating to their subject matter. Modifications must be in writing, signed by both parties, and specifically reference the LA. Additional or different terms on current or future Customer or third party purchasing documents are expressly objected to and rejected.

1. **License of Software**. This Attachment I shall provide additional terms which govern Customer's license of the Software specified on the preceding chart and any related user documentation provided by SAS. When licensed alone or as a subcomponent, SAS AppDev Studio software may be used for development purposes only.
2. **Pricing Metrics**. The pricing metrics described herein apply to the Software and any Software subcomponents listed on the preceding chart. For the avoidance of doubt, only those pricing metrics listed on preceding chart apply to the Software and Software subcomponents licensed hereunder.
   (a) **Total Users** - The Software license fee is based on the total number of Users (not concurrent) who access the Software during the applicable license period.
   (b) **Capacity Based -** The Software license fee is based on the total processing power of the Authorized Hardware on which the Software is installed. With respect to server hardware, processing power includes each processor core contained within the Authorized Hardware. With respect to mainframe hardware, processing power is based on Millions of Instructions Per Second ("MIPS").
   (c) **Limited Scope –**The Software may be used solely to support Customer's operation of its law enforcement operation located at the Southwest Texas Fusion Center, located in San Antonio, Texas. The Software will also include the following modules: Request for Service Module, Intelligence Management Module, Suspicious Activity Reporting Module ("SARS Module"), and Confidential Informant Management Module ("CIM Module"). Customer's use of the SARS Module shall be further limited to ten (10) named users and Customer's use of the CIM Module shall also be further limited to eight (8) named users.
3. **Subcomponent Installations**. Some Software consists of subcomponents which may be used only in connection with a single Software configuration. When the Software requires installation of subcomponents on more than one hardware tier, the server-tier subcomponents may be installed only on the Authorized Hardware listed on the preceding chart of this Attachment I. If authorized by SAS, however, some server-tier subcomponents also may be installed on separate hardware. Where the license fee is based on hardware capacity, then the separate hardware must have the same or lower classification as the Authorized Hardware. Software or subcomponents licensed to SAS by third parties may only be installed once.
4. **Committed Term**.
   4.1. **License Grant; Termination**. SAS hereby grants and Customer hereby accepts a license to use the Software for two (2) non-cancelable annual license periods commencing on the License Beginning Date ("Committed Term"). Notwithstanding the foregoing, either party may terminate the license in the event of a material breach of the terms of the LA by the other party provided such breach is not cured within thirty (30) days of the breaching party's receipt of written notice from the other party. This right to cure does not apply to breaches that threaten to cause or have caused damage to or loss of all or part of SAS' intellectual property rights.
   4.2. **License Fees During the Committed Term; Invoicing**. The license fees during the Committed Term shall be payable in two (2) annual installments as follows:

Annual License Period	**Annual License Fee Installment**
First Annual License Period	$103,590
Second Annual License Period	Included
Total License Fees During Committed Term	$103,590

The license fees set forth above do not include applicable taxes which will be added to SAS' invoices. If Customer desires to increase its usage of the Software beyond that agreed upon herein by, for example, increasing the capacity of the Authorized Hardware, increasing the number of Users authorized to access the Software, or increasing the value of a pricing metric, additional fees may apply.

SAS will invoice the first Annual License Fee Installment as soon as both parties sign the Integration Agreement. SAS will invoice the Annual License Fee Installments for the remaining Annual License Periods of the Committed Term approximately thirty (30) days prior to each annual Anniversary Date. Customer will pay such invoices net thirty (30) days regardless of whether Customer discontinues its use of the Software prior to the expiration of the Committed Term. SAS will provide one (1) year Product Authorization Codes each year for the Software when SAS receives Customer's payment of the applicable Annual License Fee Installment.

   4.3. **Renewal following the Committed Term**. Following the expiration of the Committed Term, the parties may renew the Software license annually in accordance with this LA unless otherwise mutually agreed by written amendment to this LA. Such license renewals shall be accomplished by SAS sending an invoice for the applicable Software license renewal fees and taxes and Customer paying the invoice. The following renewal year pricing shall apply to the three optional one-year periods following the Commited Term:

Renewal Option Year	Renewal Fees
Year Three	$23,793
Year Four	$24,983
Year Five	$26,232

4.4. **Indemnification; Warranty; Limitation of Liability**. For the purposes of determining the amount of license fee refund in the Indemnification and Warranty Sections of the LA, and the amount of license fees subject to the Limitation of Liability Section of the LA, the applicable license fee amount shall be the Annual License Fee Installment paid for the Annual License Period when the claim arose, as specified above.

ATTACHMENT II

1. **RESERVED.**

2.1 **Services, Deliverables, Work Product and Fees.**

2.1 Work Product. In exchange for Customer paying the fees and any applicable taxes arising under this LA, SAS agrees to provide (a) the services described in Section 2.2 below ("Services") related to Customer's use of the Software and (b) a limited license as described in Section 3.1 below in relation to any documentation, computer code or other materials delivered by SAS in connection with the Services (collectively, "Work Product"). As used herein, the term "Time and Materials" means a consultative model where SAS provides Services at the hourly rates identified below. SAS' time and a limited license to any Work Product resulting from performance of the Services are the only deliverables to be provided to Customer hereunder.

2.2 Description of the Services: SAS shall provide Services directed toward the services described on Exhibit B to the Integration Agreement.

2.3 Hourly Rates; Customer Funds; Travel and Living Expenses; Invoicing.

2.3.1 Hourly Rates. The hourly rate(s) for the Services shall be as follows:

Resource	Hourly Rate
Senior Consultant	$190
Consultant	$150
Project Manager	$170

2.3.2 Customer Funds. Customer has made available funds in the amount of One Hundred Forty Six Thousand One Hundred Ten Dollars ($146,110) (U.S.) for Services ("Customer Funds"), which is based on the estimated budget for labor for the Services determined by SAS. Travel and living expenses and applicable taxes are additional and are not reflected in the Customer Funds. Neither party shall have any obligation with respect to the performance of, or payment for, Services beyond the depletion of the Customer Funds. Customer may make additional Customer Funds available for the performance of the Services by amendment to this LA.

2.3.3 Travel and Living Expenses. Travel and living expenses, and any applicable taxes, are additional and are not reflected in the rates above.

2.3.4 Invoicing. SAS will invoice Customer monthly for any Services fees due. Payment terms shall be net thirty (30) days.

3. TERMS AND CONDITIONS.

3.1 Ownership of Work Product. SAS grants Customer a nonexclusive, nontransferable, non-assignable, royalty-free license to use the Work Product only with the Software with which the Work Product operates and only for as long as Customer maintains a license for such Software. Nothing herein shall be construed as granting Customer a license to any SAS Software, which shall be licensed separately pursuant to a license agreement between SAS and Customer. SAS has no obligation to provide continued support or maintenance for any Work Product. Ownership of the Work Product, including any intellectual property embodied therein, and any techniques, skills, concepts or know-how that are utilized or developed while performing the Services remains with SAS. Prototype systems and sample programs furnished by SAS are designed to help Customer learn to use the Software and for demonstration purposes; they are not intended to be used for production purposes without appropriate Customer testing.

3.2 Confidential Information. SAS agrees to use reasonable efforts to prevent any Confidential Information from being revealed to third parties for a period of three (3) years from the date of disclosure. As used herein, the term "Confidential Information" shall mean only that information of Customer provided to SAS in connection with and related to the Services. This restriction does not apply to information which is: (1) generally available to the public; (2) released by Customer without restriction; (3) independently developed or acquired by SAS; or (4) known to SAS prior to receipt from Customer. In the event the Confidential Information must be disclosed pursuant to judicial order or requirement of law, SAS shall make reasonable efforts to notify Customer of such order or requirement. For the purposes of this Section, SAS' subsidiaries and subcontractors performing Services shall not be deemed "third parties." No proprietary source code or individually identifiable information will be disclosed under this LA.

3.3 Change Management. "Change Management" refers to a process for the parties to agree on a change or modification to the scope of Services, and "Change Order" refers to the document reflecting the change or modification. Requests by Customer or SAS for such changes will be made in writing to the other party. SAS will prepare the Change Order, which will contain the following information:

a. A description of any additional work to be performed and/or any changes to the performance required of either party.

b. A statement of the impact of the work or changes on the Services and the project schedule.

c. The estimated timetable to complete the work specified in the Change Order.

d. The estimated time and cost of any additional work associated with the Change Order.

SAS will provide the proposed Change Order to Customer's project manager for review, and if additional fees will be charged, SAS will provide the proposed amendment to this LA. Customer's project manager will respond in writing to the proposed Change Order within five (5) business days. Each party must agree in writing to the Change Order. Pending such written agreement (and if additional fees will be charged, execution of the associated amendment), SAS will continue to perform as if such Change Order had not been requested or recommended. If Customer provides its acceptance of the proposed Change Order in writing and, if applicable, executes the proposed amendment, SAS' project manager will update the project plan to reflect the change(s).

3.4 Warranties; Disclaimers; Limitation of Liability. SAS warrants that the Services will be performed by qualified personnel in a workmanlike manner and in accordance with the requirements set forth in this LA. The exclusive remedy for breach of this warranty is refund of fees paid for the Services at issue. SAS warrants that it has the right to license the Work Product to Customer. The exclusive remedy for breach of this warranty is provided in the section of the LA addressing SAS' indemnification obligations for intellectual property infringement claims. SAS' indemnification obligations and the disclaimers of warranty and exclusions of consequential damages and limitations of liability contained in the LA also apply to any Work Product and Services under this LA. For purposes of this LA, with respect to SAS' indemnification obligations and the limitations of liability contained in the LA, the term "Work Product" shall replace "Software," "IPPs," "Micro-IPPs" or any other defined term for the SAS software products licensed under the LA. The parties acknowledge and agree that Customer may use the Work Product in connection with its work for a third party on behalf of Customer ("Client"), or other third parties whom SAS has no contractual relationship. Accordingly, except for claims for which Customer is entitled to reimbursement pursuant to the LA, Customer shall defend, indemnify, and hold SAS harmless from and against any liability for claims by Client or any other third party arising from use of the Work Product.

3.5 Reserved.

3.6 Customer Responsibilities; Equipment; Personnel. Customer is responsible for furnishing facilities, equipment, information and access to Customer personnel required to perform the Services. SAS may subcontract all or portions of the Services. Customer agrees not to solicit for hire any individual who provides the Services to Customer within six (6) months after the Services are performed. Notwithstanding the foregoing, responses to general advertisements in the media or on the Internet or Customer's intranet shall not be deemed to be a solicitation for hire within the context of this Section 3.6.

ATTACHMENT I

Software and Subcomponents[1]		Applicable Pricing Metric, Number of Authorized Units[2], Limited Scope	Operating System[3]	Authorized Hardware (CPU/Server Manufacturer, Model type/Serial No.)[3]	Initial Fees[4] (in above Currency Type)	License Beginning Date	Anniversary Date
						FOR SAS USE ONLY	
SAS Fusion Center Solution for San Antonio Police Department							
Software:	Memex Platform	Total Users (14) Limited Scope	LINA - Linux for x64	To be defined by Customer in writing	See Section 4.2 of Attachment I	30NOV2013	30NOV
Software:	Memex eGuardian CONNECT	Capacity Based Limited Scope	LINA-Linux for x64	To be defined by Customer in writing	See Section 4.2 of Attachment I	30NOV2013	30NOV

1. Pricing metrics, operating systems and/or Authorized Hardware for subcomponents which differ from that of the Software with which they are associated are listed in the column that corresponds to the applicable subcomponent. Unless otherwise noted, subcomponents listed here are included in the Software license fee for the Software product with which they are licensed or provided.
2. The pricing metric is used to derive license fees; for example, but without limitation, Capacity Based, Total Users, PC Use, etc. as described on the next page of this Attachment I. Certain pricing metrics contain additional terms that pertain to Customer's use of the Software.
3. Customer must provide Operating System and Authorized Hardware information to SAS prior to shipment of Software.

SAS Fusion Center Solution

Professional Services Statement of Work.

For

San Antonio Police Department

October 17, 2013
Updated: November 21, 2013

Exhibit B

SAS INSTITUTE INC. WORLD HEADQUARTERS SAS CAMPUS DRIVE CARY, NC 27513
TEL: 919 677 8000 FAX: 919 677 4444 U.S. SALES: 800 727 0025 www.sas.com

PROFESSIONAL SERVICES

As part of this proposal, SAS is including professional services associated with deploying the Fusion Center Solution. The following is a description of the proposed tasks to be carried out by SAS professional services consultants.

DEPLOYMENT OF CORE MEMEX PLATFORM

TASK
Hardware and Network Analysis SAS consultants will work with SAPD IT personnel to ensure all hardware and any necessary network configuration necessary for a successful deployment of SAS Fusion Center Solution is in place.
Installation Media and License Generation The SAS Memex platform requires a license file unique to each server on which it is deployed. SAS consultants will work with SAPD IT personnel to obtain the necessary information from the target servers and to generate and deploy the resulting license files.
Server Commissioning and Prerequisite Software Installation SAS consultants will work with SAPD IT department to make sure the target servers have the correct Operating System version installed and that any necessary third-party libraries or applications are installed.
Core Memex Platform Installation SAS consultants will carry out the installation of the core Memex components. These are the baseline components used by all Memex modules.
Core System Testing SAS Consultants will carry out testing of the core Memex Platform to ensure its correct operation with SAPD's environment.
DELIVERABLE - Documentation of Server Environment (Site Guide) SAS consultants will create a site guide which will include server and configuration details related to the deployment within SAPD's environment. This document will act as reference for both SAS consultants and SAPD technical staff. Details will include: • Installation location of deployed components • Location of relevant system log files. • Access details necessary for the correct administration of the deployed components

- Component version numbers where appropriate.
- Details of deployed licenses files;
- SAS and SAPD system personnel contact details.

DEPLOYMENT OF MEMEX INTELLIGENCE MODULE

TASK
Install Intelligence Module in SAS Project Environment SAS consultants will deploy the standard Memex Intelligence Module to a project environment provided by SAS using SAS hardware. The SAS project environment will be used by SAS consultants to apply any configuration changes to the Intelligence Module identified as being necessary over the course of the project. Upon completion of all agreed configuration changes, SAS consultants will transfer the finished configuration to SAPD's servers. The hardware hosting the project environment will remain in the possession of SAS at all times. The environment will be used strictly for system configuration. No production data will be loaded on to the project environment.
Review Current Intelligence Procedures and Software SAS Consultants will carry out a review of SAPD's current intelligence practices and related software tools. The information gathered during this task will be used, where appropriate, to guide the configuration of the Memex Intelligence Module to best support SAPD policies and procedures.
Coordinate and Conduct Working Group SAS Consultants will conduct a two day working group with key members of SAPD project team to review the Memex Intelligence Module. The purpose of the working group is to introduce the module to SAPD key stakeholders and to identify and document areas where configuration changes may be necessary.
Review and Agree Upon Configuration Changes from Working Group Following completion of the working group, SAS consultants will review and assess the feasibility and level of effort required to implement each configuration change identified during the working group. SAS will then present this information to SAPD stakeholders. Should the estimated level of effort exceed the budgeted hours included for applying configuration changes, SAS consultants will work with SAPD to prioritize the configuration changes to meet the available hours.
Apply Configuration Modifications Agreed Upon During Working Group Based on the approved list of configuration changes, SAS consultants will make adjustments to the module in the project environment. These changes will be presented to SAPD stakeholders during a second, online working group.

Deploy to SAPD Test Environment

SAS consultants will deploy the final Intelligence Module configuration to the SAPD test environment. A pre-requisite for this and all subsequent tasks is the successful completion of all tasks listed under Deployment of the Core Memex Platform

SAS Testing

After deployment to the SAPD test environment, SAS consultants will perform functional testing of the deployed module to verify correct operation within SAPD's environment.

SAPD Testing

SAPD will be given the opportunity to carry out their own testing of the deployed module. To avoid potential project overruns it is essential that this testing is carried out in a timely manner. The SAS project management team will work with their counterparts at SAPD to determine an appropriate timeline for the carrying out of this testing. This activity will be coordinated with user training to ensure those people tasked with carrying out system testing have sufficient knowledge of the system to be able to test effectively.

Remedial Work from Testing

SAS consultants will work to resolve any issues identified and documented during either SAS or SAPD testing of the module.

Deployment of Final Configuration to SAPD's Production Environment

SAS consultants will deploy the final configuration of the Intelligence Module, including corrections to the system applied during remedial work, to SAPD's production environment.

DELIVERABLE

SAS consultants will update the site guide document to include details of the deployed configuration of the Memex Intelligence Module. Details will include:

- Installation location of deployed components
- Location of relevant system log files.
- Access details necessary for the correct administration of the deployed components
- Component version numbers where appropriate.

DEPLOYMENT OF MEMEX SARS MODULE

TASK
Install SARS Module in SAS Project Environment SAS consultants will deploy the standard Memex SARS Module to a project environment provided by SAS using SAS hardware. The SAS project environment will be used by SAS consultants to apply any configuration changes to the SARS Module identified as being necessary over the course of the project. Upon completion of all agreed configuration changes, SAS consultants will transfer the finished configuration to SAPD's servers. The hardware hosting the project environment will remain in the possession of SAS at all times. The environment will be used strictly for system configuration. No production data will be loaded on to the project environment.
One day working group to identify potential changes SAS Consultants will conduct a one day working group with key members of SAPD project team to review the baseline Memex SARS Module. The purpose of the working group will be to introduce the module to SAPD key stakeholders and to identify and document possible configuration changes.
Review and Agree Upon Configuration Changes from Working Group Following completion of the working group, SAS consultants will review and assess the feasibility and level of effort required to implement each configuration change identified during the working group. SAS will then present this information to SAPD stakeholders. Should the estimated level of effort exceed the budgeted hours included for applying configuration changes, SAS consultants will work with SAPD to prioritize the configuration changes to meet the available hours.
Apply Configuration Modifications Agreed Upon During Working Group Based on the approved list of configuration changes, SAS consultants will make adjustments to the module in the project environment. These changes will be presented to SAPD stakeholders during a second, online working group.
Conduct Webinar to Review Configuration Changes SAS Consultants will conduct an online meeting with key members of SAPD project team to review and confirm the applied changes from the working group. The purpose of the working group is to finalize the module for testing.

Deploy to SAPD Test Environment

SAS consultants will deploy the final SARS Module configuration to the SAPD test environment. A pre-requisite for this and all subsequent tasks is the successful completion of all tasks listed under Deployment of the Core Memex Platform.

Coordinate Between SAPD and FBI for Issuance of Digital Certificate

The eGuardian interface for the SARS Module requires a digital certificate be issued by the FBI before it will operate correctly. Each agency using the interface must have its own certificate. SAS consultants will facilitate a dialogue between the FBI and SAPD to allow this certificate to be issued.

SAS Testing

After deployment to the SAPD test environment, SAS consultants will perform functional testing of the deployed module to verify correct operation within SAPD's environment.

SAPD Testing

SAPD will be given the opportunity to carry out their own testing of the deployed module. To avoid potential project overruns it is essential that this testing is carried out in a timely manner. The SAS project management team will work with their counterparts at SAPD to determine an appropriate timeline for the carrying out of this testing. This activity will be coordinated with user training to ensure those people tasked with carrying out system testing have sufficient knowledge of the system to be able to test effectively.

Remedial Work from Testing

SAS consultants will work to resolve any issues identified and documented during either SAS or SAPD testing of the module.

Deployment of Final Configuration to SAPD's Production Environment

SAS consultants will deploy the final configuration of the SARS Module, including corrections to the system applied during remedial work, to SAPD's production environment.

DELIVERABLE

SAS consultants will update the site guide document to include details of the deployed configuration of the Memex SARS Module. Details will include:

- Installation location of deployed components
- Location of relevant system log files.
- Access details necessary for the correct administration of the deployed components

- Component version numbers where appropriate.

DEPLOYMENT OF MEMEX REQUEST FOR SERVICE MODULE

TASK
Install RFS Module in SAS Project Environment SAS consultants will deploy the standard Memex RFS Module to a project environment provided by SAS using SAS hardware. The SAS project environment will be used by SAS consultants to apply any configuration changes to the SARS Module identified as being necessary over the course of the project. Upon completion of all agreed configuration changes, SAS consultants will transfer the finished configuration to SAPD's servers. The hardware hosting the project environment will remain in the possession of SAS at all times. The environment will be used strictly for system configuration. No production data will be loaded on to the project environment.
Working group to identify potential changes SAS Consultants will conduct a working group with key members of SAPD project team to review the Memex RFS Module. The purpose of the working group will be to introduce the module to SAPD key stakeholders and to identify and document possible configuration changes.
Review and Agree Upon Configuration Changes from Working Group Following completion of the working group, SAS consultants will review and assess the feasibility and level of effort required to implement each configuration change identified during the working group. SAS will then present this information to SAPD stakeholders. Should the estimated level of effort exceed the budgeted hours included for applying configuration changes, SAS consultants will work with SAPD to prioritize the configuration changes to meet the available hours.
Apply Configuration Modifications Agreed Upon During Working Group Based on the approved list of configuration changes, SAS consultants will make adjustments to the module in the project environment. These changes will be presented to SAPD stakeholders during a second, online working group.
Conduct Webinar to Review Configuration Changes SAS Consultants will conduct an online meeting with key members of SAPD project team to review and confirm the applied changes from the working group. The purpose of the working group is to finalize the module for testing.

Deploy to SAPD Test Environment

SAS consultants will deploy the final RFS Module configuration to the SAPD test environment. A pre-requisite for this and all subsequent tasks is the successful completion of all tasks listed under Deployment of the Core Memex Platform.

SAS Testing

After deployment to the SAPD test environment, SAS consultants will perform functional testing of the deployed module to verify correct operation within SAPD's environment.

SAPD Testing

SAPD will be given the opportunity to carry out their own testing of the deployed module. To avoid potential project overruns it is essential that this testing is carried out in a timely manner. The SAS project management team will work with their counterparts at SAPD to determine an appropriate timeline for the carrying out of this testing. This activity will be coordinated with user training to ensure those people tasked with carrying out system testing have sufficient knowledge of the system to be able to test effectively.

Remedial Work from Testing

SAS consultants will work to resolve any issues identified and documented during either SAS or SAPD testing of the module.

Deployment of Final Configuration to SAPD's Production Environment

SAS consultants will deploy the final configuration of the RFS Module, including corrections to the system applied during remedial work, to SAPD's production environment.

DELIVERABLE

SAS consultants will update the site guide document to include details of the deployed configuration of the Memex RFS Module. Details will include:

- Installation location of deployed components
- Location of relevant system log files.
- Access details necessary for the correct administration of the deployed components
- Component version numbers where appropriate.

DEPLOYMENT OF MEMEX CONFIDENTIAL INFORMANTS MANAGEMENT (CIMS) MODULE

TASK
Install CIMS Module in SAS Project Environment SAS consultants will deploy the standard Memex CIMS Module to a project environment provided by SAS using SAS hardware. The SAS project environment will be used by SAS consultants to apply any configuration changes to the SARS Module identified as being necessary over the course of the project. Upon completion of all agreed configuration changes, SAS consultants will transfer the finished configuration to SAPD's servers. The hardware hosting the project environment will remain in the possession of SAS at all times. The environment will be used strictly for system configuration. No production data will be loaded on to the project environment.
Working group to identify potential changes SAS Consultants will conduct a working group with key members of SAPD project team to review the Memex CIMS Module. The purpose of the working group will be to introduce the module to SAPD key stakeholders and to identify and document possible configuration changes.
Review and Agree Upon Configuration Changes from Working Group Following completion of the working group, SAS consultants will review and assess the feasibility and level of effort required to implement each configuration change identified during the working group. SAS will then present this information to SAPD stakeholders. Should the estimated level of effort exceed the budgeted hours included for applying configuration changes, SAS consultants will work with SAPD to prioritize the configuration changes to meet the available hours.
Apply Configuration Modifications Agreed Upon During Working Group Based on the approved list of configuration changes, SAS consultants will make adjustments to the module in the project environment. These changes will be presented to SAPD stakeholders during a second, online working group.
Conduct Webinar to Review Configuration Changes SAS Consultants will conduct an online meeting with key members of SAPD project team to review and confirm the applied changes from the working group. The purpose of the working group is to finalize the module for testing.

Deploy to SAPD Test Environment

SAS consultants will deploy the final RFS Module configuration to the SAPD test environment. A pre-requisite for this and all subsequent tasks is the successful completion of all tasks listed under Deployment of the Core Memex Platform.

User Account Set-Up

An important part of the deployment of the CIMS module is the correct set up of user accounts to ensure all necessary data protection is applied correctly. SAS consultants will work with SAPD personnel to ensure all CIMS user accounts are correctly set up with the appropriate security permissions.

SAS Testing

After deployment to the SAPD test environment, SAS consultants will perform functional testing of the deployed module to verify correct operation within SAPD's environment.

SAPD Testing

SAPD will be given the opportunity to carry out their own testing of the deployed module. To avoid potential project overruns it is essential that this testing is carried out in a timely manner. The SAS project management team will work with their counterparts at SAPD to determine an appropriate timeline for the carrying out of this testing. This activity will be coordinated with user training to ensure those people tasked with carrying out system testing have sufficient knowledge of the system to be able to test effectively.

Remedial Work from Testing

SAS consultants will work to resolve any issues identified and documented during either SAS or SAPD testing of the module.

Deployment of Final Configuration to SAPD's Production Environment

SAS consultants will deploy the final configuration of the CIMS Module, including corrections to the system applied during remedial work, to SAPD's production environment.

DELIVERABLE

SAS consultants will update the site guide document to include details of the deployed configuration of the Memex CIMS Module. Details will include:

- Installation location of deployed components
- Location of relevant system log files.
- Access details necessary for the correct administration of the deployed components

- Component version numbers where appropriate.

SYSTEM TRAINING

Fusion Center Solution User Training

SAS Consultants will provide 2 user training classes, each lasting 2 days, covering the use of the SAS Fusion Center solution. Up to 10 people may attend each class. It is assumed staff attending the training will not have any prior experience of using the Memex system.

Memex Administrator Training

SAS Consultants will provide 1 system administrator training class, lasting 1 day, covering the administration of the SAS Memex system upon which the Fusion Center Solution is built. The course will cover managing system users and permissions as well as server 'housekeeping' activities. It is assumed attendees will have some experience of administering similar systems.

Fusion Center Solution Refresher User Training

SAS Consultants will provide 2 days of refresher training to users of the system some time (usually 2 weeks) after the system becomes operational. The purpose of this training is to cover items that have been forgotten or were not covered during initial training, but have subsequently come up during operational use of the system.

DELIVERABLE

As part of the training activities, SAS will provide SAPD with manuals covering the use of the delivered system in PDF format. Note that the manuals will cover all areas of system functionality, but are based on a generic configuration of the delivered system. Screenshots and examples within the documentation may vary in places from the final configured system deployed at SAPD.

PROJECT MANAGEMENT

- SAS will assign a Project Manager to the project. The project manager will be responsible for the following activities:

- Ensuring that adequate project planning takes place.
- Facilitating and managing cross-organizational activities.
- Monitoring progress of project.
- Ensure that team members have access to all required resources.
- Managing project risks.
- Coordinating with SAPD's project manager.
- Managing users' expectations.
- Maintaining the project timeline.
- Acting as liaison between the SAS team and SAPD users.
- Keeping both SAS management and SAPD project sponsors informed of project progress.
- Establishing software configuration management and change control practices for agreed module

modifications.
DELIVERABLE During the initial stages of the project, the SAS project manager will create and hand over to SAPD, a high level project plan covering the remained of the project.

ASSUMPTIONS, DEPENDENCIES, EXPECTATIONS AND RESPONSIBILITES

The success and timely delivery of these services is dependent upon the timely access to appropriate people, responsiveness of all parties and a shared understanding of the tasks. The SAS team will include various as-needed Consultants and a Project Manager. From time to time SAS personnel may require access to and assistance from IT and networking staff at SAPD.

The following is a list of specific assumptions and responsibilities necessary for the successful and timely delivery of the services:

- A SAS Services Supplement (contract) will be executed prior to commencement of any services.
- Both parties agree to adhere to the project plan and project definition document in all material respects.
- Any material changes to the project must be reflected by Change Control following the Change Management Process. Any change to the project will be assessed for its impact to the project and a revised effort estimate will be provided as part of the change control process.
- The SAPD project manager will arrange meetings with appropriate personnel as needed throughout the implementation. SAS will require access to SAPD system administrators, network administrators, business users and the project executive sponsor.
- SAPD will provide systems access, including login IDs as required, needed to accomplish the tasks described in this document.
- Upon contract award, SAS may require up to 30 days advance notice prior to work commencement.
- SAPD will provide SAS with notice of any required confidentiality, security procedures and/or paperwork requirements prior to work commencement.
- SAPD will grant suitably vetted SAS personnel remote access via VPN to all system hardware for the duration of the services. In the interest of minimizing travel costs, SAS personnel will conduct as much of the services as possible from SAS locations using the provided remote access.

CITY OF SAN ANTONIO

San Antonio Police Department

REQUEST FOR COMPETITIVE SEALED PROPOSAL
("RFCSP")

for

INTEGRATED INFORMATION AND INTELLIGENCE MANAGEMENT
LAW ENFORCEMENT SOLUTION

6100003495 (RFCSP-013-096)

Release Date: SEPTEMBER 11, 2013

Proposals Due: SEPTEMBER 27, 2013

EXHIBIT A

002 TABLE OF CONTENTS

002 TABLE OF CONTENTS 2
003 BACKGROUND 2
004 SCOPE OF SERVICE 2
005 ADDITIONAL REQUIREMENTS 5
006 TERM OF CONTRACT 7
007 PRE-SUBMITTAL CONFERENCE 7
008 PROPOSAL REQUIREMENTS 7
009 CHANGES TO RFCSP 8
010 SUBMISSION OF PROPOSALS 8
011 RESTRICTIONS ON COMMUNICATION 10
012 EVALUATION CRITERIA 10
013 AWARD OF CONTRACT AND RESERVATION OF RIGHTS 11
014 BONDS 13
015 SOFTWARE ESCROW REQUIREMENT 13
016 ACCEPTANCE CRITERIA 13
017 SCHEDULE OF EVENTS 13
018 RFCSP EXHIBITS 14
019 RFCSP ATTACHMENTS 25

003 BACKGROUND

The San Antonio Police Department (SAPD) has a requirement to provide an integrated information and intelligence management law enforcement solution (IMLES) for the Southwest Texas Fusion Center (SWTFC). The SWTFC serves a critical role in assisting SAPD units, particularly that of developing the Department's Intelligence Led-Policing (ILP) strategies and operations. The SWTFC also assists in tactical and strategic decision making across the region by facilitating the creation of intelligence products distributed and consumed by numerous other local, state and federal public safety entities.

The requested fusion center solution will act as a force multiplier, resulting in the production of more informed, efficient and effective crime prevention strategies. SWTFC personnel will be able to manage a broad range of operational and analytical resources and activities by accessing data in a manner previously unavailable due to technological constraints.

004 SCOPE OF SERVICE

The scope of the work to be performed will result in a contract for an operational, turnkey Fusion Intelligence consisting of different modules – Request for Service (RFS), Suspicious Activity Reporting (SAR), Criminal Intelligence Management (CIM), and a Confidential Informant (CI). The system operates in a client server environment where the contactor is to provide installation of the purchased equipment, system design specifications, production, development, and full system installation and integration for the systems design that it proposes. A number of other tasks essential to successful implementation and operation are expected. The Respondent shall include overall project management for the installation, documentation, training, testing and acceptance as well as ongoing maintenance and support services during the Respondent's proposed two years warranty period.

The following four modules must be provided:

RFS Module must:

1. Record, manage, and monitor service calls.
2. Include performance metrics at organizational and individual levels.
3. Record and monitor activity expended on service calls from units/organizations supported by the SWTFC.
4. Allocate requests based on subject matter expertise or workload.
5. Use of RFS statistics to quantify SWTFC service value.

SAR Module must:

1. Be compliant and integrate with the National SAR Initiative (NSI).
2. Have capability to interface with ESRI GIS platform.

3. Document tips and leads for SAPD and within the SAR cycle, from intake and work-up, through disposition.
4. Allow investigators and analysts to collaborate on the same SAR.
5. Have ability to interface with NSI Shared Space and or eGuardian.

CIM Module must:

1. Operate within the basic intelligence process and support compliance with federally mandated 28 CFR Part 23.
2. Have a single federated search capability.
3. Include real time electronic alerts and notifications.
4. Support customization of data entry and input.
5. Support multiple level review and approval process.
6. Capture, evaluate and refine raw data for use in actionable intelligence products.
7. Automate group-based data security assignment; reduce SAPD liability by implementing data and workflow controls to ensure safe management and dissemination of intelligence information.

CI Module must:

1. Support the vetting, approval, and handling of registered informants.
2. Single federated search with anonymous pointer.
3. Supports deconfliction process.
4. Provide informant interaction tracking and payment audit process.
5. Supports ESRI GIS tracking/mapping.

Services shall include:

- Professional Services
- Configure and install the software application
- System Configuration
- Testing
- Training
- Create three customized forms for agency use
- Support and Maintenance

A. MINIMUM REQUIREMENTS

The Respondent must present an integrated fusion center solution. The Respondent selection is based on the need for an end-to-end Integrated Information and Intelligence Management Law Enforcement Solution. The Respondent must have a minimum of 10 years experience working in a Major City Intelligence Unit or recognized Fusion Center.

B. BUSINESS REQUIREMENTS

The City of San Antonio (COSA) desires the implementation of an IMLES that will meet the following high-level requirements:

1. IMLES shall be a single platform that includes functionality for suspicious activity reporting, service request management, intelligence management and confidential informant management.
2. IMLES shall include a multi-level security user groups.
3. IMLES shall have security and audit capability.
4. IMLES shall have customizable data entry forms.
5. IMLES shall have document indexing and archiving.
6. IMLES shall have a single sign-on.
7. IMLES shall be deployable via thin client, i.e., web browser Supports duplication of data to MS SQL environment Interface to Microsoft Exchange and ESRI GIS.
8. IMLES must be Commercial-off-the-Shelf (COTS) software to support expedited deployment.
9. IMLES shall support tasks to improved customer service, efficiency, and accuracy.
10. IMLES shall leverage existing knowledge base by linking to other critical systems.
11. IMLES shall support legal and regulatory compliance.
12. IMLES shall integrate with the Nationwide SAR Initiative and eGuardian and allow investigators and analysts to collaborate on the same SAR.
13. IMLES shall capture, evaluate and refine raw data into actionable intelligence products.

14. IMLES shall provide consistent levels of checks and balances to mitigate risk through workflow standardization.
15. IMLES shall be designed in compliance with existing handling policies, consent decrees, court orders and other legislation

C. City Hosted Solution - City purchases the software and the solution runs on City 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 Attachment F.

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

D. Third Party Products / Options Software

The Respondent must explicitly state the name of any third-party products that Respondent will be providing as part of the proposed solution. Respondent must have, and must demonstrate upon request, that it has authorization to transfer any rights of use and warranties for third-party products to the City. 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.

E. Maintenance and Support

Respondent should specify the prime contractor and software vendor(s) who plan to carry out post-implementation and ongoing support, including:

1. Telephone support (include toll-free support, hours of operation). A hotline that provides at least 12 hours, 5 days per week availability Monday through Friday from 7:00 a.m. to 7 p.m.

2. Delivery method for future upgrades and product enhancements including frequency of upgrades.

3. Problem reporting and resolution procedures.

4. Delete.

5. Bug fixes and patches.

6. Performance tunings and incremental enhancement.

7. On-line support.

Maintenance and support will begin after the expiration of a two-year warranty period and last for the remainder of the initial term, and include the optional extension terms. Warranty period shall begin upon final written acceptance of system by City.

F. Training and Costs

Provide training options and details of training plans and costs. Provide training costs on a per trainee basis. Training options should include web-based and classroom-based training.

G. Travel

If the selected, Respondent is not located within the corporate limits of the City of San Antonio, the selected Respondent shall include the cost of travel to San Antonio or any other location for the performance of the services contemplated herein to be included. Meetings (with the exception of the exception of the presentation(s) may be conducted telephonically.

H. TECHNICAL REQUIREMENTS

The proposed system solution should be able to integrate with the current Information Technology Environment Description Standards. Refer to RFCSP Exhibit 5.

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.

If any 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.

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
Restrictions on Communication
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

The anticipated term of the proposed contract is from the effective date of City Council approval and expires two years after final acceptance of the system by the City.

007 PRE-SUBMITTAL CONFERENCE

A Pre-Submittal Conference will be held at Riverview Towers Building at 111 Soledad, Ste. 1100, San Antonio, TX 78205 (11Th Floor Hill Country Conference Room) at 9:00 a.m., Central Time, on September 17, 2013. Respondents are encouraged to prepare and submit their questions in writing 3 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 Riverview Towers Building located at 111 Soledad, Ste. 1100, San Antonio, TX 78205 (11Th Floor Hill Country Conference Room) is wheelchair accessible. The accessible entrance is located at at the front of the building. Accessible parking spaces are located at Rand parking garage near the building. 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.

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.

If submitting a hard copy proposal, submit one original, signed in ink, ten copies, and one copy of the proposal on compact disk (CD) containing an Adobe PDF version of the entire proposal. Each of the items listed below must be labeled with the heading indicated below as a separate file on the CD.

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.

FUNCTIONAL REQUIREMENTS. 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.

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

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.

FINANCIAL INFORMATION. Submit a recent copy of a Dun and Bradstreet financial report, or other credit report, on Respondent and its partners, affiliates and subtenants, if any.

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 may be submitted in hard copy format.

Submission of Hard Copy Proposals.

Respondent shall submit one original, signed in ink, ten copies, and one copy of the proposal on compact disk (CD) containing an Adobe PDF version of the entire proposal in a sealed package clearly marked with the project name, **"Integrated Information and Intelligence Management Law Enforcement Solution"** on the front of the package.

Proposals must be received in the Office of the City Clerk's no later than 2:00 p.m., Central Time, on September, 27, 2013 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:
Office of the City Clerk's
Attn: Finance Department, Purchasing Division
"Integrated Information and Intelligence Management Law Enforcement Solution"
P.O. Box 839966
San Antonio, Texas 78283-3966

Physical Address:
Office of the City Clerk's
Attn: Finance Department, Purchasing Division
"Integrated Information and Intelligence Management Law Enforcement Solution"
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 A – Respondent Questionnaire form may not exceed insert maximum of 150 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. Failure to meet the above conditions may result in disqualification of the proposal or may negatively affect scoring.

Modified Proposals. Proposals may be modified provided such modifications are received prior to the due date for submission of proposals and submitted in the same manner as original proposal. For hard copy proposals, provide a cover letter with the proposal, indicating it is a modified proposal and that the Original proposal is being withdrawn.

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 Director of San Antonio Police Department 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 ninety (90) days following the deadline date for submissions or, if a proposal is accepted, throughout the entire term of the contract.

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.

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.,** Local Time, on **September 20, 2013**. Questions received after the stated deadline will not be answered. All questions shall be sent by e-mail to:

Lisa Mendoza, Procurement Specialist II
City of San Antonio, Finance Department
Lisa.Mendoza@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 International and 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(s), if any. The point of contact is Catherine Olukotun. Ms. Olukotun may be reached by telephone at (210) 207-8088 or by e-mail at catherine.olukotun@sanantonio.gov. Contacting the Small Business Office regarding this RFCSP after the proposal due date is not permitted.

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

The City will conduct a comprehensive, fair and impartial evaluation of all Proposals received in response to this RFCSP. The City may appoint a selection committee to perform the evaluation. Each Proposal will be analyzed to determine overall responsiveness and qualifications under the RFCSP. Criteria to be evaluated may include the items listed below. The selection committee may select all, some or none of the Respondents for interviews. If the City elects to conduct interviews, Respondents may be interviewed and re-scored based upon the same criteria. The City may also request additional information from Respondents at any time prior to final approval of a selected Respondent. The City reserves the right to select one, or more, or none of the Respondents to provide services. City's decision will be made based on compliance with the evaluation criteria. Final approval of a selected Respondent is subject to the action of the City of San Antonio City Council.

Evaluation criteria:

Proposal (35 points)

Experience, Background, Qualifications (25 points)

Pricing (20 points)

SBEDA (20 points possible) SBE, ESBE Prime Contract Points

SBE Prime Contract Program – 10 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 ten (10) evaluation criteria percentage points, and

ESBE Prime Contract Program – 10 pts

Certified ESBE (Emerging Small Business Enterprise) 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% ESBE participation (prime and/or subcontractor) will receive ten (10) evaluation criteria percentage points.

No evaluation criteria percentage Points will be awarded to non-ESBE or non-SBE Prime Contractors through subcontracting to certified ESBE or SBE 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. If subsequent negotiations are conducted, they shall not constitute a rejection or alternate RFCSP on the part of City. 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. 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 negotiate and execute a contract within the time specified, City reserves the right to terminate negotiations with the selected Respondent and commence negotiations 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.

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

This section is intentionally left blank.

016 ACCEPTANCE CRITERIA

This section is intentionally left blank.

017 SCHEDULE OF EVENTS

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

RFCSP Release Date	September 11, 2013
Pre-Submittal Conference	September 17, 2013 at 9:00 a.m.
Final Questions Accepted	September 20, 2013 at 2:00 p.m.
Proposal Due	September 27, 2013 at 2:00 p.m.

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

Prior to the commencement of any work under this Agreement, Respondent shall furnish copies of all required endorsements and an original completed Certificate(s) of Insurance to the City's Finance Department, Purchasing Division which shall be clearly labeled "Integrated Information and Intelligence Management Law Enforcement 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. 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 City. City shall have no duty to pay or perform under this Agreement until such certificate and endorsements have been received and approved by City's Finance Department, Purchasing Division. No officer or employee, other than City's Risk Manager, shall have authority to waive this requirement.

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 whereupon City may incur increased risk.

A Respondent's financial integrity is of interest to City; therefore, subject to Respondent's right to maintain reasonable deductibles in such amounts as are approved by 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, 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:

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(Technology E&O, claims-made basis) To be maintained and in effect for no less than two years subsequent to the completion of the professional service.	$1,000,000 per claim, to pay on behalf of the insured all sums which the insured shall become legally obligated to pay as damages by reason of any act, malpractice, error, or omission in professional services.

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 Respondent and City as additional insureds. Respondent shall provide 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.

As they apply to the limits required by City, 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
Attn: Finance Department, Purchasing Division
P.O. Box 839966
San Antonio, Texas 78283-3966

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 insured 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 polices;

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

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

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.

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 Agreement. Failure to provide and to maintain the required insurance shall constitute a material breach of this Agreement.

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.

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.

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.

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 City shall be limited to insurance coverage provided.

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

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.

Defense Counsel - CITY shall have the right to select or to approve defense counsel to be retained by RESPONDENT in fulfilling its obligation hereunder to defend and indemnify CITY, unless such right is expressly waived by CITY in writing. RESPONDENT shall retain CITY approved defense counsel within seven (7) business days of CITY'S written notice that CITY is invoking its right to indemnification under this Contract. If RESPONDENT fails to retain Counsel within such time period, CITY shall have the right to retain defense counsel on its own behalf, and RESPONDENT shall be liable for all costs incurred by CITY. CITY shall also have the right, at its option, to be represented by advisory counsel of its own selection and at its own expense, without waiving the foregoing.

Employee Litigation - In any and all claims against any party indemnified hereunder by any employee of RESPONDENT, any subcontractor, anyone directly or indirectly employed by any of them or anyone for whose acts any of them may be liable, the indemnification obligation herein provided shall not be limited in any way by any limitation on the amount or type of damages, compensation or benefits payable by or for RESPONDENT or any subcontractor under worker's compensation or other employee benefit acts.

RFCSP EXHIBIT 3

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 Respondent'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. Respondent 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 Respondent 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 Respondent by the Entity.

Respondent authorizes City's use of Respondent's name, trademarks and Respondent 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.

RFCSP EXHIBIT 4

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.

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.**

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.)

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.

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.

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 not 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.

Emerging SBE (ESBE) – a certified SBE 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, that is no more than five years old at the time of its original certification as an ESBE or whose annual revenues and number of employees are no greater than 25% of the small business size standards for its Industry as established by the U.S. Small Business Administration and meets the Significant Business Presence requirements as defined herein.

Emerging M/WBE – a certified M/WBE firm that is no more than five years old at the time of its original certification as an Emerging M/WBE, that is actively enrolled in the M/WBE or SBE Mentor-Protégé Program for its Industry (once established by the City), whose annual revenues and number of employees are no greater than 25% of the small business size standards for its Industry as established by the U.S. Small Business Administration, and meets the Significant Business Presence requirements as defined herein.

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 1/16th 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. SBEDA Program Compliance – General Provisions

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 Initiative 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. 7. (a), 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.

ESBE Prime Contract Program. In accordance with the SBEDA Ordinance, Section III. D. 7. (b), this contract is being awarded pursuant to the Emerging SBE (ESBE) Prime Contract Program, and as such, CONTRACTOR affirms that if it is presently certified as an ESBE, CONTRACTOR agrees not to subcontract more than 49% of the contract value to a non-ESBE 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).

RFCSP EXHIBIT 5

CITY OF SAN ANTONIO
INFORMATION TECHNOLOGY ENVIRONMENT DESCRIPTION

Posted as separate documents.

RFCSP EXHIBIT 6

SEBDA PROGRAM PRESENTATION

Posted as separate documents.

019 RFCSP ATTACHMENTS

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: _____

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.

_____

_____

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._____ Email: _____

Date and Type of Service(s) Provided: _____

_____

Reference No. 2:

Firm/Company Name _____

Contact Name: _____ Title: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone No._____ Email: _____

Date and Type of Service(s) Provided: _____

_____

Reference No. 3:

Firm/Company Name _____

Contact Name: _____ Title: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone No._____ Email: _____

Date and Type of Service(s) Provided: _____

_____

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. Describe Respondent's experience relevant to the Scope of Services requested by this RFCSP. List and describe three relevant projects of similar size and scope performed over the past four years. Identify associated results or impacts of the project/work performed.

2. Indicate the number of years Respondent has been in the business of working in a Major City Intelligence Unit or recognized Fusion Center, respectively. Indicate if Integrated Information and Intelligence Management Law Enforcement Solutions is the Respondent's primary line of business. If not, state the Respondent's primary line of business.

3. List all Integrated Information and Intelligence Management Law Enforcement Solution projects that the Respondent has completed in the last four years.

4. List all Integrated Information and Intelligence Management Law Enforcement Solution projects that Respondent has in progress 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.

5. 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 and the department for which Respondent provided those services.

6. If Respondent is proposing as a team or 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.

7. 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

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

9. List the number of customers currently using the proposed solution. Include company name, type of business, city & state.

10. List a least three (3) references for customers which Respondent has recently been engaged with on similar projects. Include company name, type of business, city & state. Describe high level business function delivered as part of the project.

11. What percentage of existing customers are in the annual support phase of the contract?

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.

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.

RFCSP ATTACHMENT E

SBEDA FORM(S)

CITY OF SAN ANTONIO SUBCONTRACTOR/SUPPLIER UTILIZATION PLAN

Posted as separate documents.

RFCSP ATTACHMENT F

PRICING SCHEDULE

Posted as separate documents.

RFCSP ATTACHMENT G

FUNCTIONAL REQUIREMENTS

Posted as separate documents.

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: www.sanantonio.gov/purchasing/saeps.aspx

By submitting a proposal by paper, 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 will be able and willing to comply with the insurance and indemnification requirements set out in RFCSP Exhibits 1 & 2.

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.

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: _____

(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: _____

RFCSP ATTACHMENT I

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	
*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	
Functional Requirements RFCSP Attachment G	
*Signature Page RFCSP Attachment H	
Proposal Checklist RFCSP Attachment I	
Proof of Insurability (See RFCSP Exhibit 1) Insurance Provider's Letter Copy of Current Certificate of Insurance	
Financial Information	
One (1) Original, ten copies, and one (1) CD of entire proposal in PDF format if submitting in hard copy.	

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

PROPOSAL

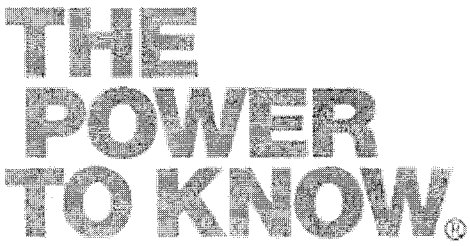
Exhibit C

SAS Fusion Center Solution for Integrated Information and Intelligence Management Law Enforcement

SAS Response to Solicitation Number 6100003495, RFCSP-013-096

San Antonio Police Department

September 27, 2013



Contact Info

Andrew Coulter
Account Representative
(919) 531-5791
Andrew.Coulter@sas.com

Table of Contents

EXECUTIVE SUMMARY **1**
PROPOSAL: ATTACHMENT A **4**
004 SCOPE OF SERVICE 4
RFS Module *4*
SAR Module *5*
CIM Module *6*
CI Module *7*
A. MINIMUM REQUIREMENTS 12
B. BUSINESS REQUIREMENTS 13
C. CITY HOSTED SOLUTION 24
Server Specifications *24*
Virtualized Server Architecture *24*
Presentation Server *25*
Production Server *25*
Training Server *25*
Client Environment *26*
D. THIRD PARTY PRODUCTS/OPTIONS SOFTWARE 27
E. MAINTENANCE AND SUPPORT 27
F. TRAINING AND COSTS 30
G. TRAVEL 32
H. TECHNICAL REQUIREMENTS 33
005 ADDITIONAL REQUIREMENTS 34
RESPONDENT QUESTIONNAIRE: ATTACHMENT B **35**
REFERENCES 36
EXPERIENCE, BACKGROUND, QUALIFICATIONS 37
CONTRACTS DISCLOSURE FORM: ATTACHMENT C **55**
LITIGATION DISCLOSURE: ATTACHMENT D **56**
SBEDA FORM: ATTACHMENT E **57**
PRICING SCHEDULE: ATTACHMENT F **58**
FUNCTIONAL REQUIREMENTS: ATTACHMENT G **59**
SIGNATURE PAGE: ATTACHMENT H **60**
PROPOSAL CHECKLIST: ATTACHMENT I **61**
PROOF OF INSURABILITY **62**
FINANCIAL INFORMATION **63**
APPENDIX A: RESUMES **64**
STEVE SERRAO, ADVISORY INDUSTRY CONSULTANT 64
DALE PEET, SENIOR INDUSTRY CONSULTANT 65
GRAEME ROBINSON, DIRECTOR OF PROFESSIONAL SERVICES 66
KYLE EVERS, SENIOR TECHNICAL CONSULTANT 67

LIBBY STENGEL, SENIOR IMPLEMENTATION PROJECT MANAGER / CONSULTANT 68
RANGA GOPAL, PRINCIPAL TECHNICAL ARCHITECT 69
COLIN PATERSON, PRINCIPAL TECHNICAL ARCHITECT 70

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. Copyright © 2013, SAS Institute Inc. All rights reserved.

Executive Summary

The San Antonio Police Department (SAPD) and the Southwest Texas Fusion Center's (SWTFC) overall missions are to provide timely information and analysis necessary to prevent and protect against all threats while enhancing SAPD's Intelligence Led-Policing strategy and operations. SAS understands SAPD needs a dynamic technical solution to drive operational insight and facilitate the strategic and tactical deployment of available resources while reducing risk to the agency and improving the overall capabilities to deter criminal activity and investigate those that have occurred. In support of these missions, the solution will need to:

- Capture criminal intelligence within a large-scale, multi-jurisdictional, 28 Code of Federal Regulations (CFR) Part 23 compliant environment allowing users to manage and develop the data used to support the targeting of threats from individual or organized criminal entities.
- Provide a powerful data search tool for research and identification of trends/patterns that operates on a single platform that is secure from improper access.
- Provide analysts with search results in a user friendly, proficient and expedient manner.
- Provide for the collection of Suspicious Activity Reports (SARS) from different sources and then pass terrorism related SARS to NSI, e-Guardian or both.
- Provide a request for service module that tracks request for information/service and monitors activity of the fusion center while collecting the appropriate data for reporting purposes.
- Provide a Confidential Informant Management Module (CIMS) with a detailed workflow that reduces risk and provides improved officer safety, deconfliction of CIs across units while providing more detailed information for those commanders making decisions concerning the use of a particular person as an informant and tracks CI contacts and payments.
- Provide integration capability with ESRI.
- Provide federated search capacities to external systems
- Provide a configurable and expandable architecture that can stay abreast of new business and data integration requirements.

The SAS Fusion Center Solution

The SAS Fusion Center Solution meets SAPD's needs. SAS understands more than just business intelligence is required to protect our citizens and our Law Enforcement personnel. The SAS solution can help surface insights into criminal activity through the use of the SAS Fusion Center Solution. The proposed solution allows SWTFC and SAPD personnel—from analysts to detectives to command staff—to use the insight that will be available to better protect the public and inform key decision makers. SAS aims to maximize the value of the SWTFC, through the implementation of a single platform that has been designed to bring a multitude of capabilities together as one operational system. The solution will break down silos of information and provide for the future growth of department, enabling SWTFC to respond quickly to changes in trends and overall department objectives.

Our proposed approach will build a strong intelligence collection capability that supports the entire intelligence cycle and is compliant with 28 CFR Part 23. The included Suspicious Activity Reporting module supports the intelligence cycle and ensures that terrorism related SARs are vetted and submitted to the NSI and or e-guardian, supporting the national effort to ensure the safety of Texans and other Americans from internal and external threats. Investigative efforts will be supported while reducing the overall risk to the department through a very robust CIMS with a streamlined workflow that keeps all supervisory levels informed yet protects the security of the informants' identity to only those that have a need and right to know. The included Request for Service module provides an efficient method to collect and report out to internal and external customers the activities of the SWTFC while providing case deconfliction—ultimately saving time for investigators and analyst and while assisting in putting agencies and units together that are focused on the same target or trend.

Why SAS?

SAS can provide SAPD and the SWTFC with a flexible solution to help address the dynamic and changing landscape of gang activity, criminal enterprises and terrorism within the Southwest Texas region. The SAS solution and approach are unique in that we offer a fully integrated system that can be configured to meet your specific needs. It is not another suite of cobbled together and acquired technologies that dazzle but do not provide the desired outcomes. Only a handful of global companies have the full depth and breadth of technologies to support SWTFC's vision. SAS is on that short list. SAS software is recognized by customers and within the industry—by industry experts and analysts—as best-of-breed and SAS can help ensure the information driving operations is timely, accurate, and reliable so SWTFC can prevent crime, enforce laws, and support public safety.

Solution Overview

The SAS Fusion Center Solution is comprised of a number of proven, innovative technologies to help SAPD and the SWTFC combat rising threats and meet its mission including:

- Single platform that includes functionality for suspicious activity reporting, service request management, intelligence management and confidential informant management
  - Multi-level security user groups
  - Security and audit capability
  - Customizable data entry forms
  - Document indexing and archiving
  - Single sign-on
  - Supports active directory authentication
  - Deployable via thin client (i.e., web browser)
  - Supports duplication of data to MS SQL environment
- Suspicious Activity Reporting (SAR) Functionality
  - Compliant and able to integrate with the National SAR Initiative (NSI)
  - Interface with NSI Shared Space and/or eGuardian
  - Interface with ESRI GIS platform
- Service Request Functionality
  - Records, manages, and monitors service calls
  - Provides performance metrics at organizational and individual levels

- Intelligence Management Functionality
  - Supports 28 CFR Part 23 compliance
  - Single federated search capability
  - Real time electronic alerts and notifications
  - Supports customization of data entry and input
  - Supports multiple level review and approval process
- Confidential Informant Management Function
  - Supports the vetting, approval, and handling of registered informants
  - Single federated search with anonymous pointer
  - Supports deconfliction process
  - Informant interaction tracking and payment audit process
  - Supports ESRI GIS tracking/mapping

SAS is excited and very pleased to have this opportunity to provide a response and solution in support of the SAPD and SWTFC's ongoing mission to protect all of us.

Proposal: Attachment A

004 SCOPE OF SERVICE

The scope of the work to be performed will result in a contract for an operational, turnkey Fusion Intelligence consisting of different modules – Request for Service (RFS), Suspicious Activity Reporting (SAR), Criminal Intelligence Management (CIM), and a Confidential Informant (CI). The system operates in a client server environment where the contactor is to provide installation of the purchased equipment, system design specifications, production, development, and full system installation and integration for the systems design that it proposes. A number of other tasks essential to successful implementation and operation are expected. The Respondent shall include overall project management for the installation, documentation, training, testing and acceptance as well as ongoing maintenance and support services during the Respondent's proposed two year warranty period.

The following four modules must be provided: RFS Module must:
1. Record, manage, and monitor service calls.
2. Include performance metrics at organizational and individual levels.
3. Record and monitor activity expended on service calls from units/organizations supported by the SWTFC.
4. Allocate requests based on subject matter expertise or workload.
5. Use of RFS statistics to quantify SWTFC service value.

RFS Module

The RFS module of the SAS Fusion Center Solution was specifically designed for the Fusion Center environment and has now been deployed to many sites across the US. RFS fulfills a significant need in the recording and monitoring of activity expended on service calls from organizations supported by the center.

As a Fusion Center fulfills its diverse service commitments, it has become increasingly important to record and report on the services provided, identify success factors and measure performance at organizational and individual levels. This provides insight into a number of key areas by the generation of Fusion Center metrics such as:

- Number of service calls received per time period
- Type of service calls received
- Number of calls per agency/organization
- Average analyst RFS workload per time period
- Average RFS turnaround time
- Average RFS turnaround time per analyst
- Number of RFS products produced per time period

At a Glance
- *Improves operation monitoring*
- *Provides request and case deconfliction*
- *Prevents duplication of work*
- *Request are not lost or misplaced*
- *Assist in balancing work loads*
- *Supports reporting as required by DHS*

The recording and monitoring of RFS activity in a format provided by the SAS Fusion Center Solution has provided agencies with important data from which performance baselines can be established and measured against. These numbers have become increasingly important as Fusion Centers strive to identify success criteria, monitor throughput capabilities and evaluate performance, particularly when resourcing levels are being reviewed and economic conditions dictate staffing levels.

SAR Module must:
1. Be compliant and integrate with the National SAR Initiative (NSI).
2. Have capability to interface with ESRI GIS platform.
3. Document tips and leads for SAPD and within the SAR cycle, from intake and work-up, through disposition.
4. Allow investigators and analysts to collaborate on the same SAR.
5. Have ability to interface with NSI Shared Space and or eGuardian.

SAR Module

SAS developed its first SAR module at the end of 2001 as part of a statewide counter-terrorist initiative. It was developed and deployed as an extension to an existing multi-jurisdictional intelligence program and quickly became the primary collection point and triage mechanism for all terrorist related information in the state. Our SAR module became an instant success and was attributed to significant results obtained by the participating agencies through the combination of three simple factors:

- Multiple roles and agencies collaborating on the same integrated platform
- Integration of multiple data sources
- An easy to use system-wide search capability

At a Glance
- *NIEM compliant and integrates with NSI SAR and e-Guardian*
- *Improves collaboration*
- *Supports multi-jurisdictional intelligence programs*
- *Detailed workflow*
- *Tracks vetting activities*

Since that time, this module has gone through significant technical and workflow related improvements as the SAR environment at a national level has matured and become an initiation point for criminal investigations or intelligence projects for all types of criminal activity. It is the most used of the SAS Fusion Center components due to its ease of use, close integration with the Intelligence and Case Management modules and its data exchange links with the two national SAR sharing initiatives.

As Law Enforcement agencies rely more on data analysis to support command-level decision making, outputs are produced to provide management with statistics on operational status and data trends.

CIM Module must:
1. Operate within the basic intelligence process and support compliance with federally mandated 28 CFR Part 23.
2. Have a single federated search capability.
3. Include real time electronic alerts and notifications.
4. Support customization of data entry and input.
5. Support multiple level review and approval process.
6. Capture, evaluate and refine raw data for use in actionable intelligence products.
7. Automate group-based data security assignment; reduce SAPD liability by implementing data and workflow controls to ensure safe management and dissemination of intelligence information.

CIM Module

The underlying precepts on which the SAS Fusion Center Solution's Intelligence module is built have been tested and proven in the field for over 10 years. The result is an off-the-shelf product that meets both the operational and compliance needs associated with a modern intelligence environment. The module provides an organization with a proven process that is deployed with the technology. Together they provide an environment that enforces the classic intelligence lifecycle process and captures, evaluates and refines raw data into valuable intelligence products. These products will then go on to influence the tactical and strategic decision making process, identify prominent criminal networks with their members and hierarchy and finally, underpin both officer and public safety initiatives.

At a Glance
- *Classic intelligence cycle support*
- *Supports 28 CFR Part 23 compliance*
- *Automated, group based data security assignment*
- *Comprehensive audit mechanism*
- *Electronic alerts and notifications*
- *Visual linking module*
- *Multi-level review process*
- *Multi-jurisdictional support*
- *Target profile dissemination packages*

Included with the module are the data and workflow controls that ensure the safe management and dissemination of intelligence information. These include multi-level, group based security, automated generation of intelligence review dates, data flagging and notifications sent to your organizational email accounts and an unparalleled audit mechanism that tracks the usage of all system users. All of these combine to ensure that an organization can operate an intelligence initiative with the knowledge that controls are in place to ensure compliance with Federal guidelines and that information can be shared between different law enforcement disciplines or agencies without compromising security or privacy regulations.

As with all SAS Fusion Center modules the CIM module inherits the enterprise search capability of the SAS Memex Platform allowing databases, whether internal or external to the solution to be searched by a single query using the Federated Search feature.

CI Module must:
1. Support the vetting, approval, and handling of registered informants.
2. Single federated search with anonymous pointer.
3. Supports deconfliction process.
4. Provide informant interaction tracking and payment audit process.
5. Supports ESRI GIS tracking/mapping.

CI Module

The Confidential Informant Management Module (CIMS) is the latest addition to the SAS integrated suite of Law Enforcement modules. It is the culmination of best practices and cutting edge technology, delivering a structured informant management system that aggressively enforces the vetting, approval and handling processes for registered sources within a multi-jurisdictional law enforcement environment. The demands and sensitivity of this subject matter have been thoroughly researched to create a solution that delivers a consistent level of checks and balances that when deployed will mitigate the risks associated with this environment through the implementation of standardized, role-specific workflow for each phase of the informant handling process.

At a Glance
- *Adheres to Law Enforcement best practices*
- *Reduces Risk and Improves Officer Safety*
- *Tracks CI Contacts and Payments*
- *Powerful Deconfliction capability*
- *Detailed workflow supports vetting and approval process*
- *Robust Security protecting the CI's Identity*

Considerable effort was expended in the research and design of this module using subject matter expertise and the most advanced SAS Memex technology. A variety of official resources formed the basis of the design including existing informant management handling policies, consent decrees, court orders and legislation, including "Rachel's Law."

The features included in CIMS are broad and cover operational, administrative and technical areas however; it is system and data security that forms the absolute priority throughout each of these. The inclusion of role-based user profiles supports the allocation of specific system permissions to differing groups. This allows different functionality, responsibilities and notifications to be delivered to CI oriented groups such as Handlers, Unit Supervisors and Approval authorities.

A number of key objectives are met by the adoption of the new CI Management module:
- Aggressively enforce minimum standards of CI Management
- Risk reduction in the follow areas
  - Officer safety
  - Organizational liability
  - Informant safety
  - Use of undesirable CI candidates
  - Deconfliction of existing CIs
  - Measure quality and ROI of CIs

- Improved CI evaluation process by leveraging all of the data held within the SAS Fusion Center system
- Recognition of emerging CI handling standards

Services shall include:

• Professional Services

As part of this proposal, SAS is including professional services associated with deploying the Fusion Center Solution. SAS will assign a Project Manager to the project, who will be responsible for the following activities:

- Ensuring that adequate project planning takes place
- Facilitating and managing cross-organizational activities
- Monitoring progress of project
- Ensure that team members have access to all required resources
- Managing project risks
- Coordinating with SAPD's project manager
- Managing users' expectations
- Maintaining the project timeline
- Acting as liaison between the SAS team and SAPD users
- Keeping both SAS management and SAPD project sponsors informed of project progress
- Establishing software configuration management and change control practices for agreed module modifications

In addition, the following is a description of the proposed tasks to be carried out by SAS professional consultants.

• Configure and install the software application

For deployment of the core SAS Fusion Center Solution, SAS professional services consultants will perform the following:

- **Hardware and Network Analysis:** SAS consultants will work with SAPD IT personnel to ensure all hardware and any necessary network configuration necessary for a successful deployment of SAS Fusion Center Solution is in place.
- **Installation Media and License Generation:** The SAS Fusion Center Solution requires a license file unique to each server on which it is deployed. SAS consultants will work with SAPD IT personnel to obtain the necessary information from the target servers and to generate and deploy the resulting license files.
- **Server Commissioning and Prerequisite Software Installation:** SAS consultants will work with SAPD IT department to make sure the target servers have the correct operating system version installed and that any necessary third-party libraries or applications are installed.
- **Core Memex Platform Installation:** SAS consultants will carry out the installation of the core solution components. These are the baseline components used by all the SAS Fusion Center solution modules.

• System Configuration

For the deployment and configuration of the SAS Fusion Center Modules, SAS Industry Advisors and professional service consultants will perform the following tasks:

- **Working Group Events.** SAS Consultants will conduct working groups with key members of SAPD project team to review the SAS Fusion Center Solution modules. The purpose of the working group is to introduce the module to SAPD key stakeholders and to identify and document areas where configuration changes may be necessary.
- **SAPD Configuration Request Review**. Review and agree upon configuration changes from working group
- **SAS Configuration Request Review.** Following completion of the working group, SAS consultants will review and assess the feasibility and level of effort required to implement each configuration change identified during the working group. SAS will then present this information to SAPD stakeholders. Should the estimated level of effort exceed the budgeted hours included for applying configuration changes, SAS consultants will work with SAPD to prioritize the configuration changes to meet the available hours.
- **Implemented Changes.** Apply configuration changes agreed upon during the working group. Based on the approved list of configuration changes, SAS consultants will make adjustments to the module in the project environment. These changes will be presented to SAPD stakeholders during a second, online working group.

• *Testing*

- **Deploy to SAPD Test Environment.** SAS consultants will deploy the final Fusion Center Solution configuration to the SAPD test environment.
- **SAS Testing.** After deployment to the SAPD test environment, SAS consultants will perform functional testing of the deployed module to verify correct operation within SAPD's environment.
- **SAPD Testing.** SAPD will be given the opportunity to carry out their own testing of the deployed module. To avoid potential project overruns it is essential that this testing is carried out in a timely manner. The SAS project management team will work with their counterparts at SAPD to determine an appropriate timeline for the carrying out of this testing. This activity will be coordinated with user training to ensure those people tasked with carrying out system testing have sufficient knowledge of the system to be able to test effectively.
- **Remedial Work from Testing.** SAS consultants will work to resolve any issues identified and documented during either SAS or SAPD testing of the module.

• *Training*

- **Fusion Center Solution User Training:** SAS Consultants will provide 3 onsite user training classes, each lasting 3 days, covering the use of the SAS Fusion Center solution that will include RFS, SAR and Intelligence Module Training. Up to 12 people may attend each class. It is assumed staff attending the training will not have any prior experience of using the Memex system.
- **Confidential Informant Management Module Training:** SAS Consultants will provide up to 3 x 1 day onsite training classes for up to 12 users per class who are involved in the confidential informant management process. (Note. It is currently unknown what the total number of Confidential Information Management module users will be. This proposal assumes up to 35 users may need to be trained on this module.) CIMS students must have completed Fusion Center Solution User Training.

- **Memex Administrator Training:** SAS Consultants will provide 1 system administrator training class, lasting 1 day, covering the administration of the SAS Memex system upon which the Fusion Center Solution is built. The course will cover managing system users and permissions as well as server 'housekeeping' activities. It is assumed attendees will have some experience of administering similar systems.
- **Fusion Center Solution Refresher User Training:** SAS Consultants will provide 2 days of refresher training to users of the system at a mutually agreed time after the system becomes operational. The purpose of this training is to optimize knowledge transfer and retention. This training can be provided in a consolidated format onsite in a classroom environment or remotely via the web as part of a series of the short (60 – 90 minute) tactical training classes totaling 16 hours that will focus on specific components or modules. These webinar training sessions will be recorded and will be available for download by the customer for future use as part of a library of training videos.

• ***Create three customized forms for agency use***

In addition to the off-the-shelf law enforcement modules required by this RFP the proposed solution provides a fully customizable interface and workflow environment allowing the forms and solution behavior to be tailored to meet any requirements that are specific to the SWTFC. The forms provided for SAR, Request for Service, Intelligence Management and Person/Gang member forms are all customizable. The graphic below details the Form Designer application that is used by trained administrators to modify the design and behavior of the interface.

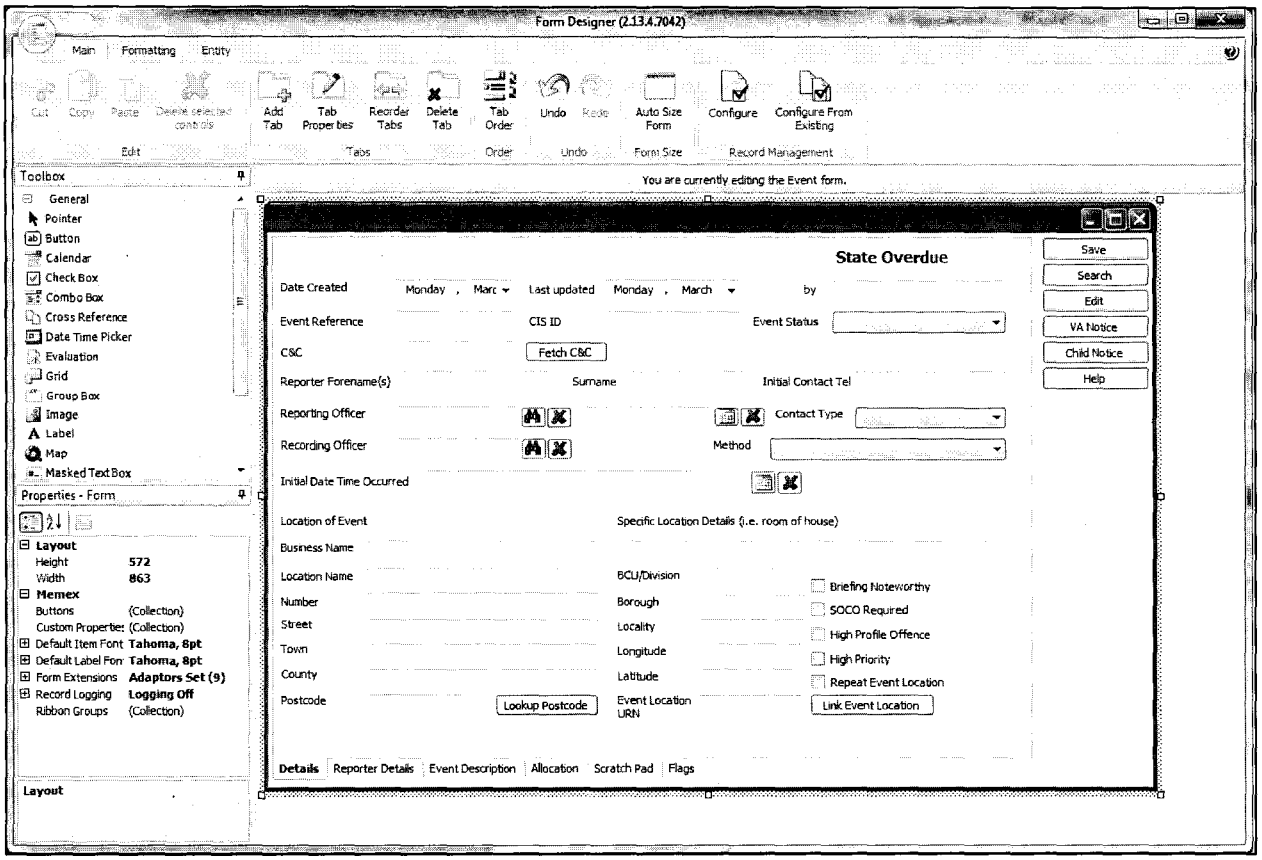


Figure 1: Form Designer

- ***Support and Maintenance***
  - **Documentation of Server Environment:** SAS consultants will create a site guide which will include server and configuration details related to the deployment within SAPD's environment. This document will act as reference for both SAS consultants and SAPD technical staff.
  - The SAS license and maintenance agreement provides technical maintenance and support at no additional charge.

A. MINIMUM REQUIREMENTS

The Respondent must present an integrated fusion center solution. The Respondent selection is based on the need for an end-to-end Integrated Information and Intelligence Management Law Enforcement Solution. The Respondent must have a minimum of 10 years experience working in a Major City Intelligence Unit or recognized Fusion Center.

SAS has had experience of implementing software for major city intelligence initiatives since 1995 with an agency wide deployment of a Criminal Intelligence Management system for the London Metropolitan Police Service (MPS). Today 40, 000 police and civilian members of MPS now operate what is the 4th generation of that original intelligence product.

Today through continual focus on this specialized Law Enforcement discipline and the constant reinvestment in its development of ILP and Fusion Center Support solutions the SAS Fusion Center Solution has become a valuable tool in assisting organizations in the tactical and strategic decision making process by facilitating the creation of products that will be distributed and consumed by a wide range of Law Enforcement and other trusted parties. This is made possible through SAS Memex Platform —a commercially available software framework that provides a unique end-to-end, enterprise solution for Fusion Centers.

At a Glance
- *Integrate data on this flexible integration platform and eliminate your data silos*
- *Allow your teams to collaborate on a single platform*
- *Stay compliant with information handling policies*
- *Optionally available connection to national level data sharing programs such as NSI, eGuardian and RISS*

Within a service-based environment such as the SWTFC which is responsible for managing a wide range of operational and analytical resources and activities, the SAS Memex Platform (SMP) acts as a force multiplier by:
- Consolidating access to multiple data sources.
- Providing access to data that was previously unavailable due to technological constraints.
- Hosting a variety of integrated operational modules that co-exist on the same platform and deployed to manage and report on the diverse activities of a Fusion Center—including RFS, Suspicious Activity Reporting, and Criminal Intelligence Management.

Access to this broad range of integrated data and management tools through a single interface significantly enhances the investigation and analytical process. It allows the variety of public safety and critical infrastructure protection disciplines to operate together within an environment that supports collaboration and deconfliction by default. For Fusion Center management personnel, the consolidation of data and modules that support different operational and analytical teams on a single platform allows greater visibility into the Center's operations.

SAS is proposing our Fusion Center solution for the SAPD, to include the following:
- The core Memex Platform
- The Memex Intelligence Module

- The Memex SARS Module, including the eGuardian interface
- The Memex Request for Service Module
- The Memex Confidential Informants Module

This proposal covers both the licensing cost of the software and the professional services required to deploy the software at the SAPD.

B. BUSINESS REQUIREMENTS

The City of San Antonio (COSA) desires the implementation of an IMLES that will meet the following high-level requirements:

1. IMLES shall be a single platform that includes functionality for suspicious activity reporting, service request management, intelligence management and confidential informant management.

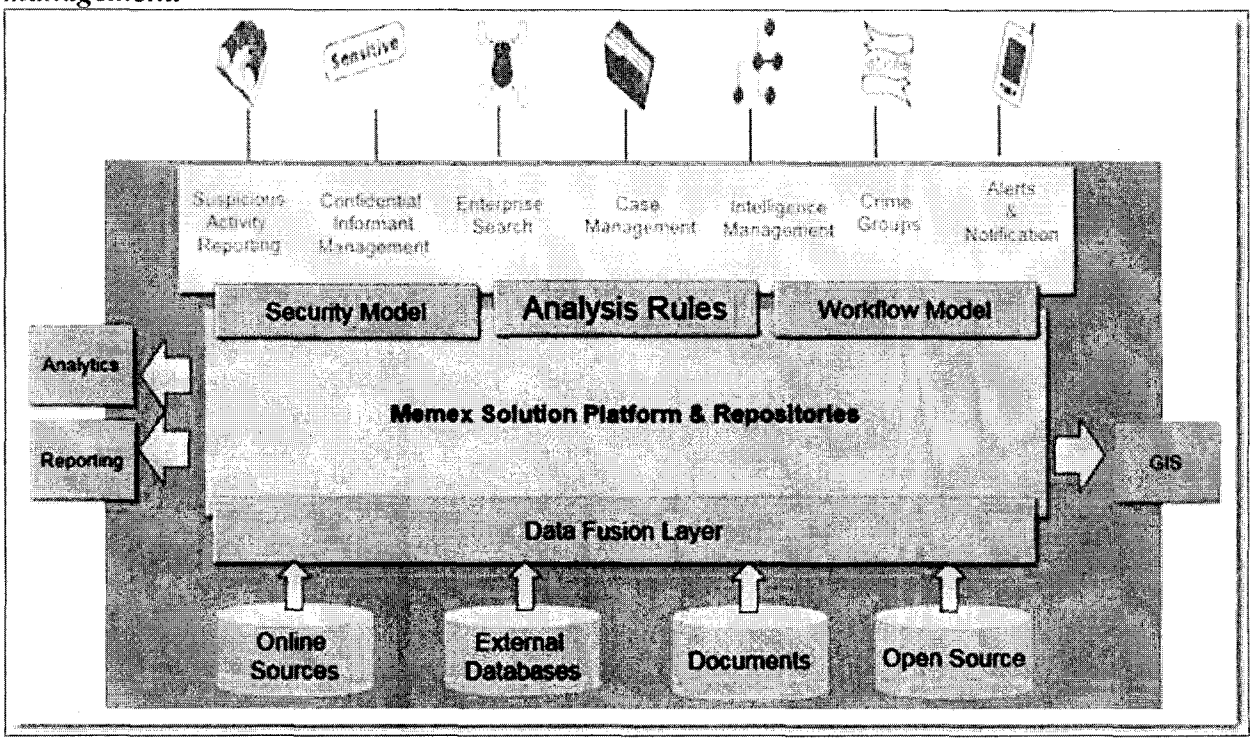


Figure 2: The SAS Memex Platform Architecture

The SAS Fusion Center Solution is supported at its core by the SAS Memex Platform (SMP) shown in Figure 2. The SMP is the foundation and core of our proposed solution for IMLES and is made up of many different components that are brought together as needed to provide a single platform that can meet the needs of the SWTFC and the SAPD today and well into the future.

The SMP is a foundation upon which a fusion center or intelligence unit can build a successful and powerful intelligence capability leading to the identification of criminal elements that may not have been previously known. It improves the ability to prevent or disrupt criminal activity to include terrorism from being carried out. All of this is made possible because of the scalability of the SMP and the power of the underlying technology that supports every aspect of this solution.

The SMP consist of different layers. The first layer is the Data Fusion Layer which supports the integration of disparate databases either through a direct integration or via a federated search capability. The Data Fusion Layer allows investigators and analysts to access this information using a powerful enterprise search capability putting every piece of data at their fingertips with a single query that provides results in a simple to understand view.

The SMP contains a very robust and granular multi-level security model. Access to information is based on a user's role, security group, and authorized access down to the record level. It is widely recognized that the security mechanism that is automatically inherited in the SMP provides a greater level of security and access control than traditional RMS solutions. The SMP also incorporates an unparalleled audit mechanism that tracks the usage of all system users. The secure solution contains controls to prevent unauthorized access and facilitates compliance with state and federal guidelines such as 28 CFR Part 23, allowing information to be shared among different law enforcement disciplines and agencies without compromising security or privacy regulations.

Solution workflow can be easily configured to make the submission and approval processes align with existing processes and practices. The extensible workflow capabilities of the solution are BPM compliant and administered through an easy to use designer. Existing workflows can be easily altered whenever workflow processes change.

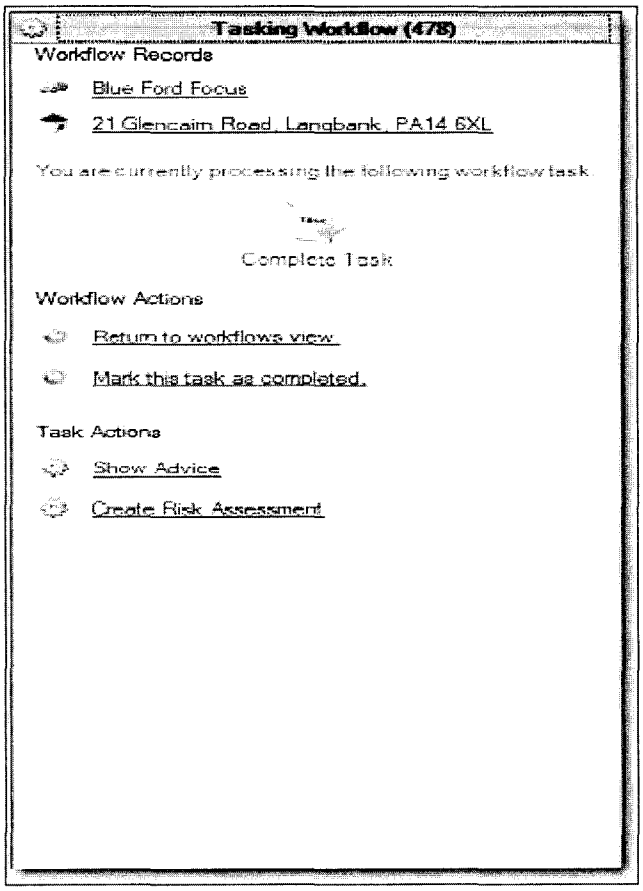


Figure 3: User friendly task panel

The workflow engine supports reminders and escalations as well as automatic forwarding. From a user's perspective, the workflow is presented as a user friendly task panel (as shown in Figure 3), which guides them through the available actions that apply to their current role in the workflow.

The SMP supports the use of analytical techniques and rules to assist the investigator and analyst in making decisions based on sound analytical practices and rules. These rules help maintain compliance with organizational policies, state and federal regulations as well as powering the Memex Advice Engine. The advice engine assist in retaining institutional knowledge and can provide guidance to a user at critical steps in any process or workflow. This capability improves effectiveness while reducing risk to the organization.

The SMP supports multiple options for integration with other systems including APIs for a number of programming languages including Java and C#, as well as web services based interfaces and XML load and extract facilities. These facilities provide a wealth of options for exposing system functionality to third-party systems such as dashboards and reporting tools. This same integration capability exists with ESRI and most other mapping software and GEO Spatial analysis tools.

The final layer of the framework is the operational layer which contains the operational modules desired by a unit or organization. In the case of IMLES this layer will contain the following modules:

- The core SAS Memex Platform
- The Memex Intelligence Module
- The Memex SARS Module, including the eGuardian interface
- The Memex Request for Service Module
- The Memex Confidential Informants Module

2. IMLES shall include a multi-level security user groups.

The SMP features both a role based access control (RBAC) system for all features in the system, and a multi-level security model. This functionality allows record access and security to be applied to 'logical' servers, individual data entities within those logical servers, or at the individual record level. Thus, when one user conducts an ad-hoc query, his/her specific RBAC privileges are enforced as are any security settings placed on records that would return in the results set. If the query is shared with another distinct user, when that user executes the query, his/her specific RBAC privileges are enforced as are any security settings placed on record. Therefore the results set for the same query could possibly result in different results sets if the two user's RBAC and security profiles were different.

The SMP supports a role-based model for the security of data and access to system functions and operations as shown in the following figure. Each user on the system is a member of one or more groups which enables his/her to log onto the system with the rights and privileges afforded to him/her from the aggregate of all the groups from which s/he is a member. Each group is allocated a number of permissions which are available at a level of granularity that allows maximum flexibility without unnecessary administrative overhead (see Figure 4). This allows

user accounts to operate using a least privileged security model where a user has only the rights and privileges s/he requires to perform his/her role.

The ability to access the data on a server depends on two factors:

- Permissions: the settings that determine which modules, menu options and buttons are available to individual users and to the members of different groups
- Record security: the access restrictions applied to individual records

Permissions and security can be assigned and applied either on an individual user basis, or on a group basis, or using a combination of users and groups. Large organizations, find it particularly useful to be able to assign permissions and apply security on a group basis. This makes it easy to ensure that all users at a certain level, or working in a particular area, have identical rights to access data or perform particular actions. Every user is a member of at least one role group and one security group:

- Role groups are sets of system permissions and database access rights. Users are assigned to role groups. Whenever a user is added to a role group, they gain all the permissions assigned to that group. A user's permissions are therefore the sum of the permissions of all the role groups to which they belong, plus any permissions that have been assigned as an individual.
- Security groups are classifications that control access to records. When a user secures a record they specify which security groups have covert or protected access to the record, and which groups are denied access. Whenever a user is added to a security group, they inherit all the access rights of that group. If the group has been specifically denied access to a record, they will no longer be able to access that record.

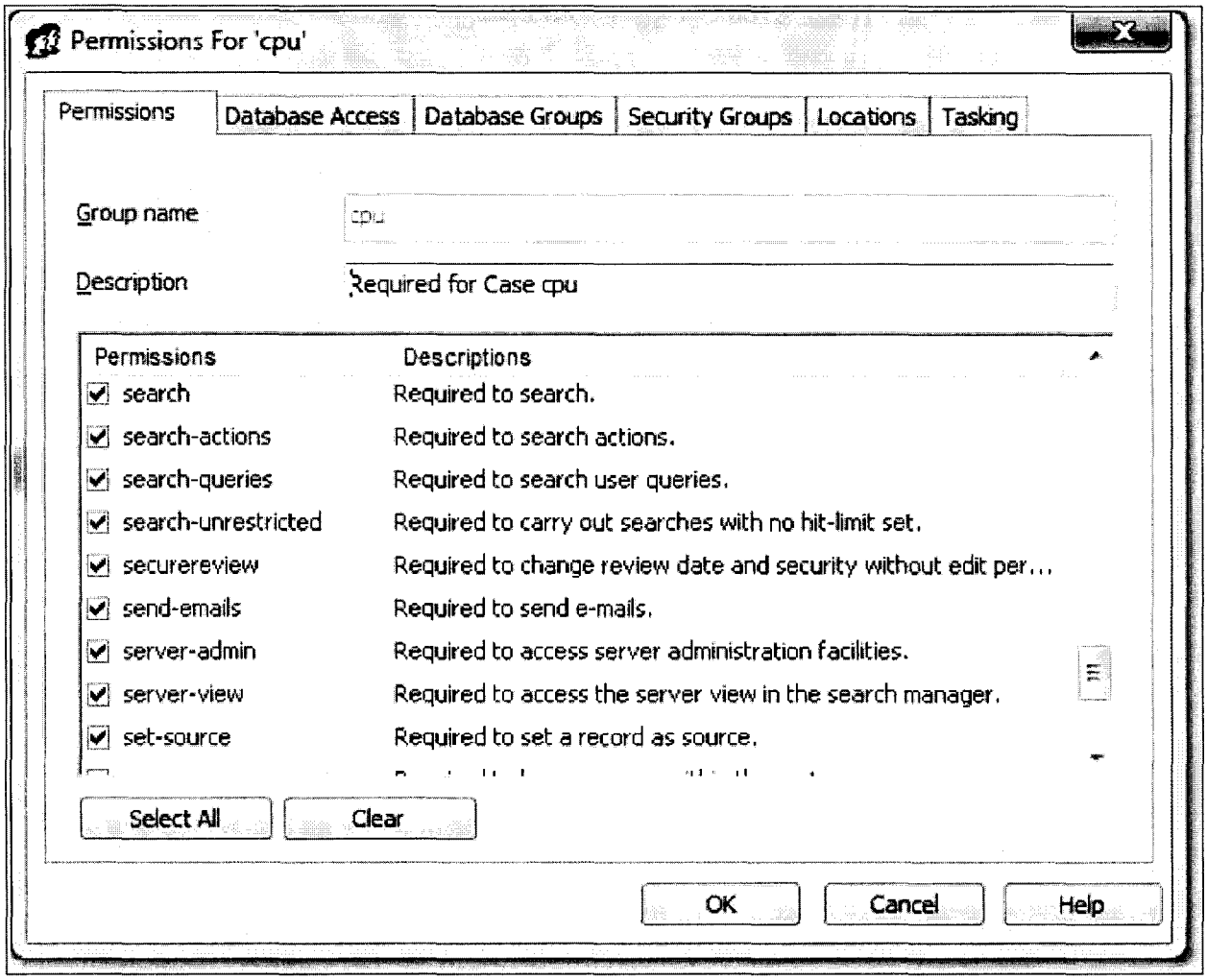


Figure 4: Specific permissions can be set by user or group

3. IMLES shall have security and audit capability.

As a system designed specifically for sensitive law enforcement applications, this solution maintains a complete and comprehensive audit trail of all user activity from the moment a user logs on to the moment they log out, including any failed log in attempts. Full details of searches, views of data, export or printing of data, record creation, modification or deletion, user and system administrative tasks are recorded. This includes the name of the user carrying out the action, date and time information, and workstation from which the activity took place. For searches, the query executed and the data sources against which it was searched are recorded. Any results returned in a hit list are also recorded. If any record is subsequently opened, that too is recorded. Audit data is stored in a repository which allows the full range of search functions to be applied including fielded and free-text searches. Access to the audit trail is generally restricted to administrative and senior supervisory users and the audit trail search functionality does not allow data to be deleted.

The solution's audit manager provides the capability to track user information on changes to reports, viewing of reports, etc. via a view into the centralized auditing mechanism that records all transactions performed on this system from point of log-in to log-out. All transactions can be

searched based on individual users, transaction types, specific records and/or date ranges. All data is searchable in the audit log. Designated users with audit manager permissions can perform searches of the audit system to retrieve and display on a wide range of transaction types, for example, details of activity by a specific user over a specific period of time.

4. IMLES shall have customizable data entry forms.
A wide range of user interface and workflow configuration options exist within the proposed solution that can be implemented without the need to change the existing code base. A complete set of administrative tools are included and the extensive training is provided to appointed SAPD staff. Using this capability, entry screens can be customized using different form views for different user's/group's workflow processes. A powerful Form Designer application is included as a standard module that allows administrative users to design and modify forms and system behavior without the need to modify code or acquire additional services from SAS.

5. IMLES shall have document indexing and archiving.
The SAS Fusion Center Solution includes an automated document indexing feature and a repository that will allow the SWTFC to define multiple locations for storing volumes of documents, files and images with the solution. When the files are added to these repositories, any textual content associated with the file such as author, title, subject, keywords and most importantly, the contents of the files are extracted and made searchable to all users on the system with the correct permission.

In addition to archiving textual content the image upload process also stores the GPS coordinates (if present) of where the image was taken alongside the image itself, adding a geographical context to the image and allows geo-tagged information to be searched and displayed using a map.

Not only does the document repository allow for new documents and images to be uploaded and shared within the agency but, due to the speed at which the files can be uploaded, the system can be used to upload existing documents which may be sitting on disparate PC's to open up the content of those documents quickly and securely to all investigative and analytical staff.

6. IMLES shall have a single sign-on.
SAS will provide access to the solution through the ITSD network. This is accomplished using different technologies. The proposed solution has the option of handling all authentication for access natively, or deferring authentication to a third party application using plug-in adaptors within a single sign-on environment. Support for Microsoft Active Directory is provided out of the box with other authentication providers supported via the creation of suitable adaptors for most networks. The solution includes a high encryption capability across the communication layer using SSL up to 256 bit AES.

7. IMLES shall be deployable via thin client, i.e., web browser Supports duplication of data to MS SQL environment Interface to Microsoft Exchange and ESRI GIS.
The SAS Fusion Center Solution supports both a thin client installed interface as well as a web-based interface. Each of these interfaces is functionally equivalent and users easily transition

from one interface to the other. An analyst can work through the desktop client while in the office but access the solution through the web-based interface when in the field.

To facilitate additional integration functions with reporting or other data exchange requirements the SAS Fusion Center Solution includes the inherent capability to duplicate data to external RDBMS environment including but not limited to MSSQL Server.

To support the user and administrative notification process the SAS Memex Platform includes a default capability to connect to any email environment that support SMTP

An embedded integration capability that interfaces with an existing ESRI implementation is included.

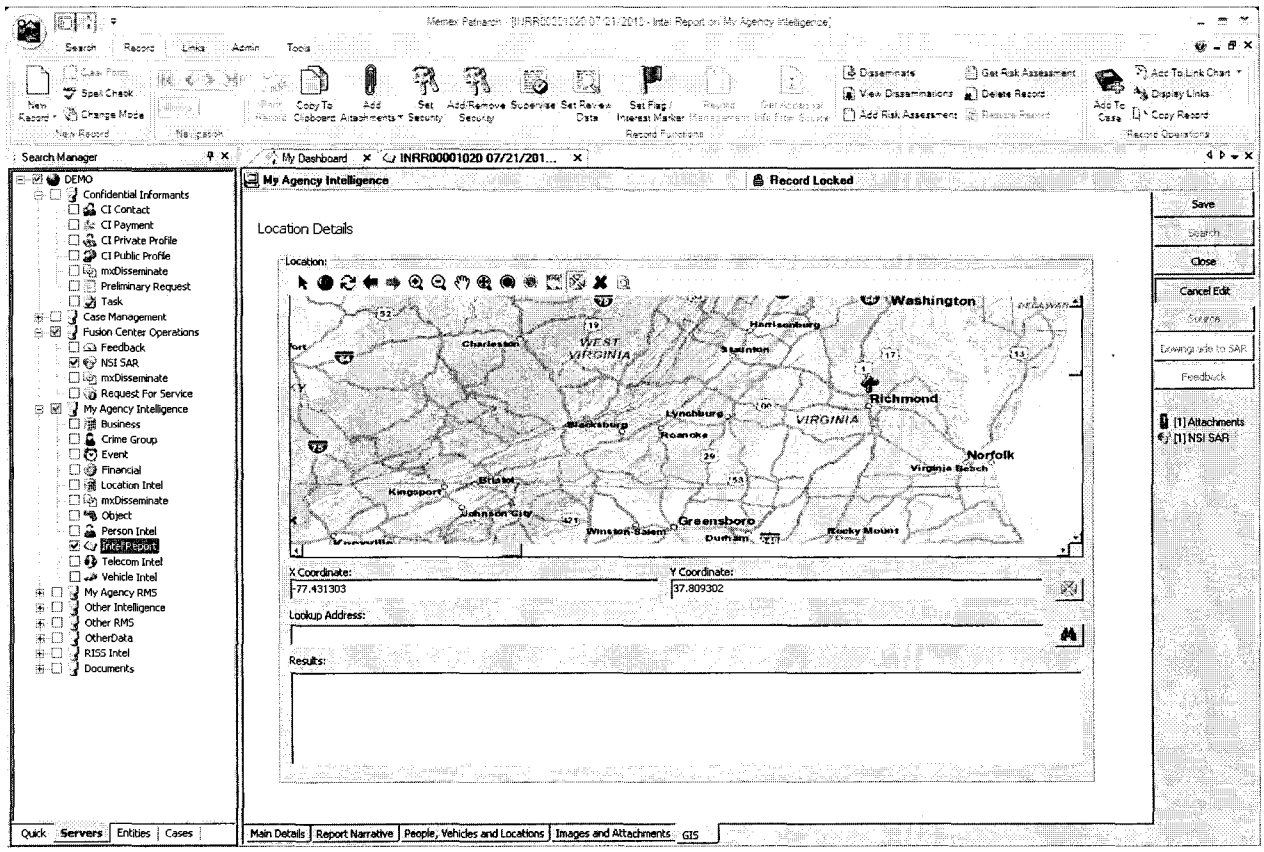


Figure 5: ESRI Integration

8. IMLES must be Commercial-off-the-Shelf (COTS) software to support expedited deployment.

The proposed SAS Fusion Center Solution is COTS product.

9. IMLES shall support tasks to improved customer service, efficiency, and accuracy.

The solution includes integrated tasking module has been developed to provide an enhanced level of support for task creation and allocation, notification and escalation. It uses a centralized module for the collection and processing of actions assigned to individuals or groups and its

functionality is controlled by the inherent role based access mechanism that allows the task to follow the organizational hierarchy and escalation process.

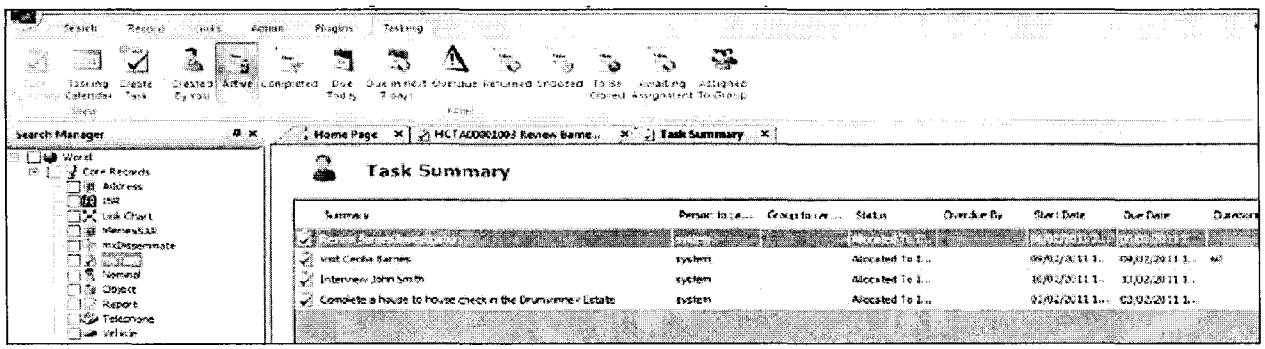


Figure 6: Task summary within the tasking module.

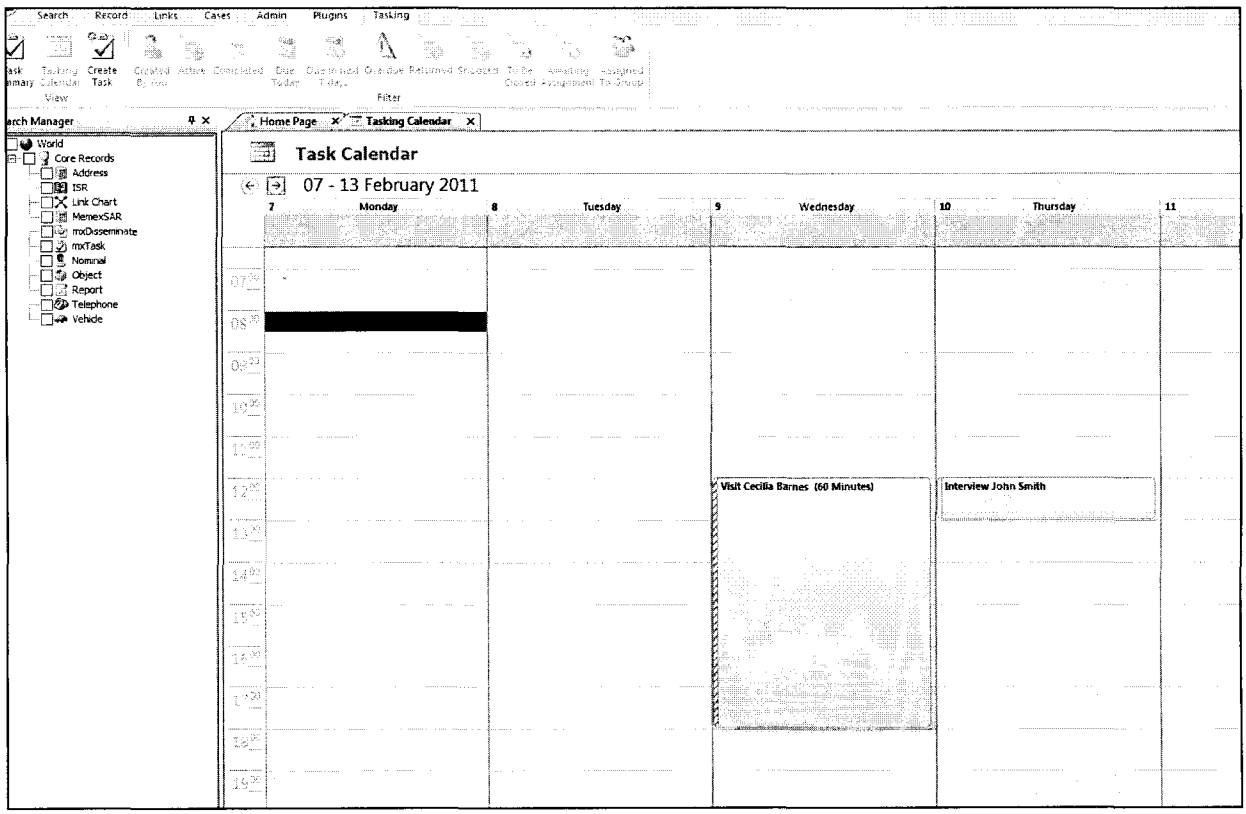


Figure 7: Tasking capability calendar view.

10. IMLES shall leverage existing knowledge base by linking to other critical systems.
SAS provides a flexible data integration platform that supports an unparalleled variety of data integration options. It is not possible that an organization's entire data integration requirement can be met with a single integration technique.

The SAS solution has the capability to import or export from or to any data source for which a suitable interface is available. Suitable interfaces include SQL based querying, programmatic

APIs, and database dump facilities. This includes all of the major database systems, including Oracle, Microsoft SQL Server, Access, DB2, etc. SAS has integrated many different types of system data into the solution—through integration, as well as through federated searches. This includes custom solutions as well as third-party vendor solutions—with data ranging from sex offender registries, ticketing systems, N-DEx, RMS, CAD, mugshot, jail management and many other data sources.

11. IMLES shall support legal and regulatory compliance.
The SAS solution complies with all requirements of 28 CFR Part 23 and is fully configurable. The retention periods, retention review periods, and deletion rules are fully configurable using a rule based engine that will generate reminder notifications to those performing the retention reviews. This review is based on the handling code assigned to the Intelligence Report by default, but this is also fully configurable.

By the very nature of the solution and its workflow capabilities, the SAS Memex solution can be configured to fit most policies as it pertains to state statutes, standards and regulations as well as fusion center privacy policies. SAS is currently used in 12 US fusion centers to maintain adherence to rules and regulations.

12. IMLES shall integrate with the Nationwide SAR Initiative and eGuardian and allow investigators and analysts to collaborate on the same SAR.
The SAS Fusion Center Solution's SAR module is NIEM / ISE-SAR compliant and includes an interface to both eGuardian and NSI programs.

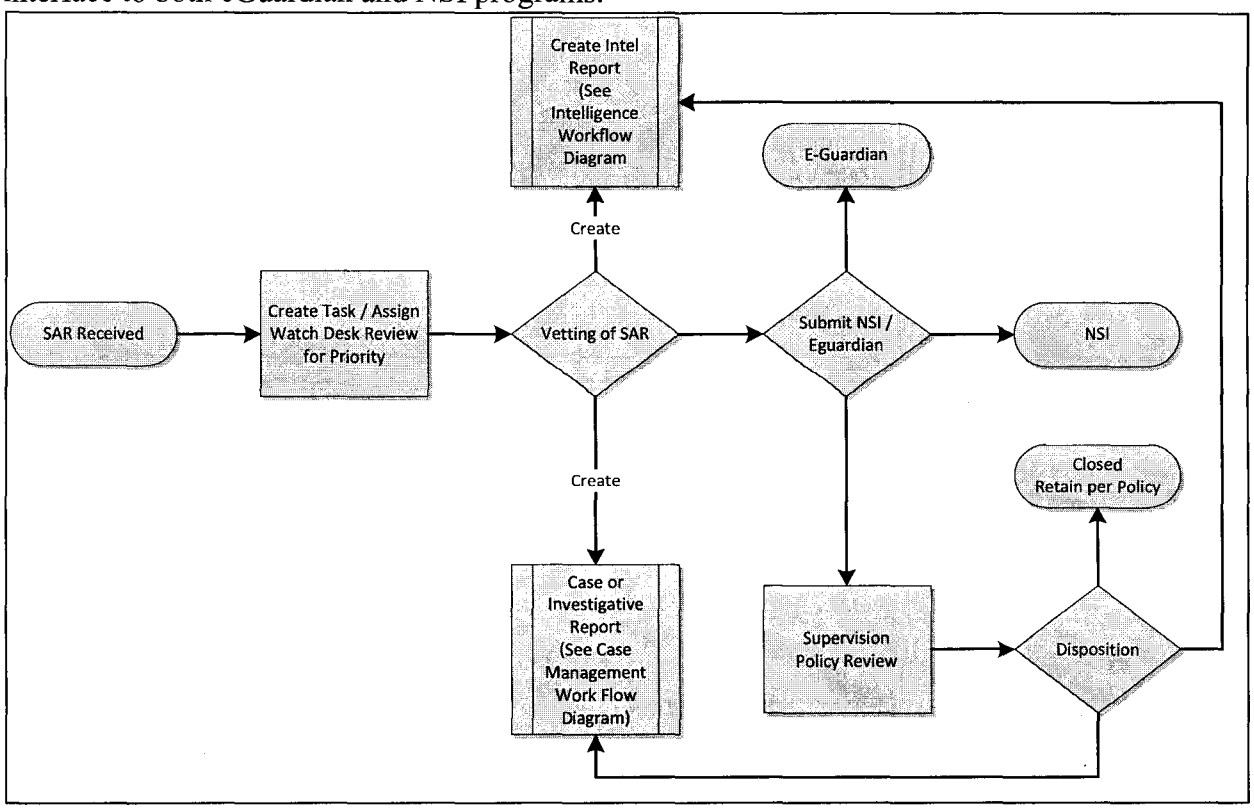


Figure 8: SAR workflow

13. IMLES shall capture, evaluate and refine raw data into actionable intelligence products.
The integrated nature of the proposed solution allows data, captured by a variety of different means and channels, to be managed in a structured manner to produce consistent levels of well substantiate intelligence products

The underlying precepts upon which the SAS intelligence module is built have been tested and proven in the field for almost two decades. The result is an off-the-shelf product that meets both the operational and compliance needs associated with a modern intelligence environment. The module provides a proven process that is deployed within the technology. Together they provide an environment that enforces the classic intelligence lifecycle process and captures, evaluates and refines raw data into actionable intelligence products. Included with the module are the data and workflow controls that offer the safe management and dissemination of intelligence information and products.

All of these combine to facilitate an intelligence initiative that contains controls to facilitate compliance with state and federal guidelines and allows information to be shared among different law enforcement disciplines and agencies without compromising security or privacy regulations.

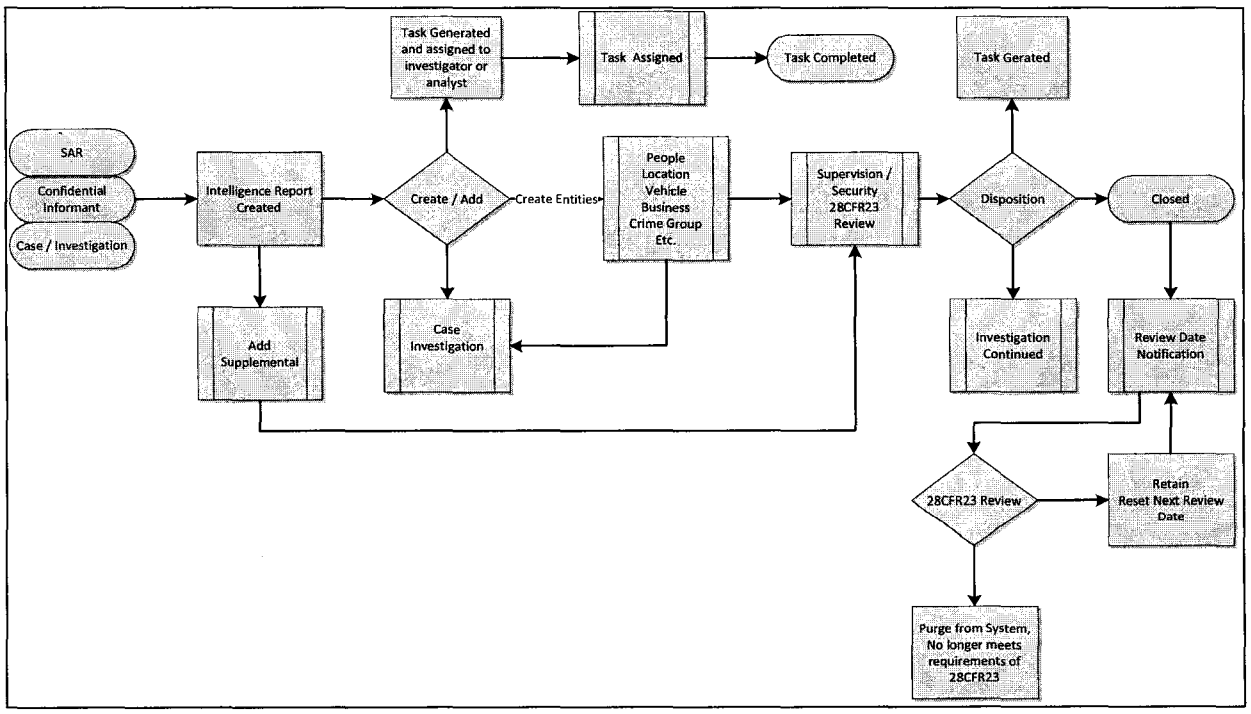


Figure 9: Intelligence report workflow.

14. IMLES shall provide consistent levels of checks and balances to mitigate risk through workflow standardization.
The SAS Fusion Center Solution provides a powerful workflow capability that can be easily configured to make the submission and approval processes align with an organization's processes and practices. This is nowhere more evident than in the Confidential Informant Management Module (CIMS). CIMS is designed to reduce risk, improve officer safety and

provide de-confliction between different units that utilize confidential informants. The extensible workflow capabilities of the solution are BPM compliant and administered through an easy to use designer. Existing workflows can be altered whenever an organization's workflow processes change as required by changes in policy, statute or the need to improve efficiency in a specific process.

The workflow engine supports reminders and escalations as well as automatic forwarding to ensure proper checks and balances are supported and enforced to ensure positive results. From a user's perspective the workflow is presented as a user friendly task panel (as shown in the following figure), which guides them through the available actions that apply to their current role in the workflow.

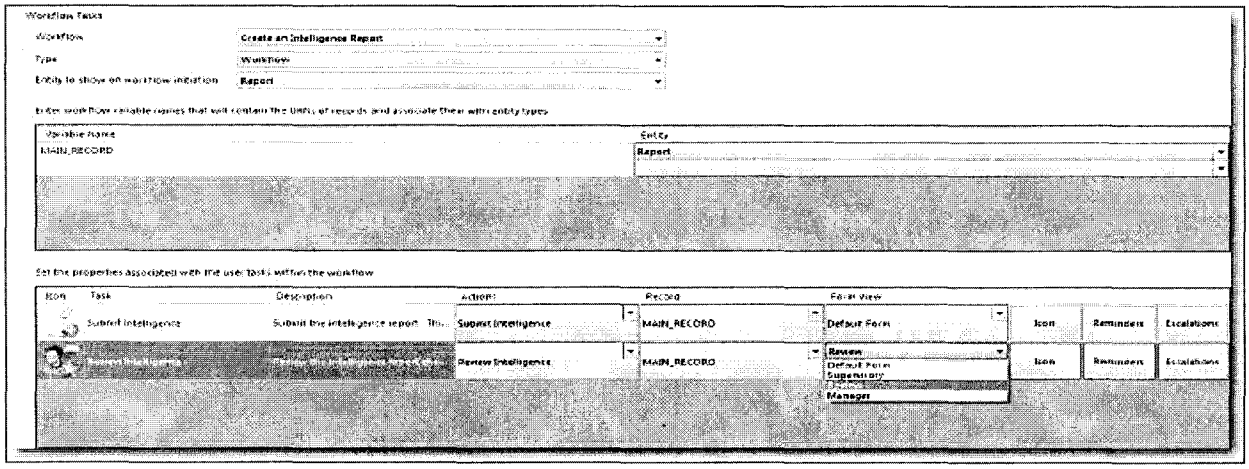


Figure 10: Workflow task example.

15. IMLES shall be designed in compliance with existing handling policies, consent decrees, court orders and other legislation

Controls have been implemented through-out the proposed solution that addressed specific mandates for the variety of policies and procedures that are associated with the capture and management of SAR, Intelligence Management and Confidential Informant data. These include:

- Mandatory field controls
- 5x5x5 intelligence evaluation controls
- Confirmation of compliance with threshold standard for the collection of intelligence information
- Automated security applied to classified content
- Notifications of specific events (Example – CI Payment)

Included with the solution workflow controls that provides the check and balances requirement for the safe management and dissemination of intelligence information. These include multi-level, group based security, automated generation of intelligence review dates, data flagging and notifications, and an unparalleled audit mechanism that tracks the usage of all system users. All of these combine to facilitate an intelligence initiative that contains controls to facilitate compliance with state and federal guidelines and allows information to be shared among different law enforcement disciplines and agencies without compromising security or privacy regulations.

C. City Hosted Solution

City purchases the software and the solution runs on City 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 Attachment F.

Server Specifications

This following outlines the technical specifications and prerequisite requirements for the SAS Fusion Center solution as proposed at San Antonio Police Department.

Virtualized Server Architecture

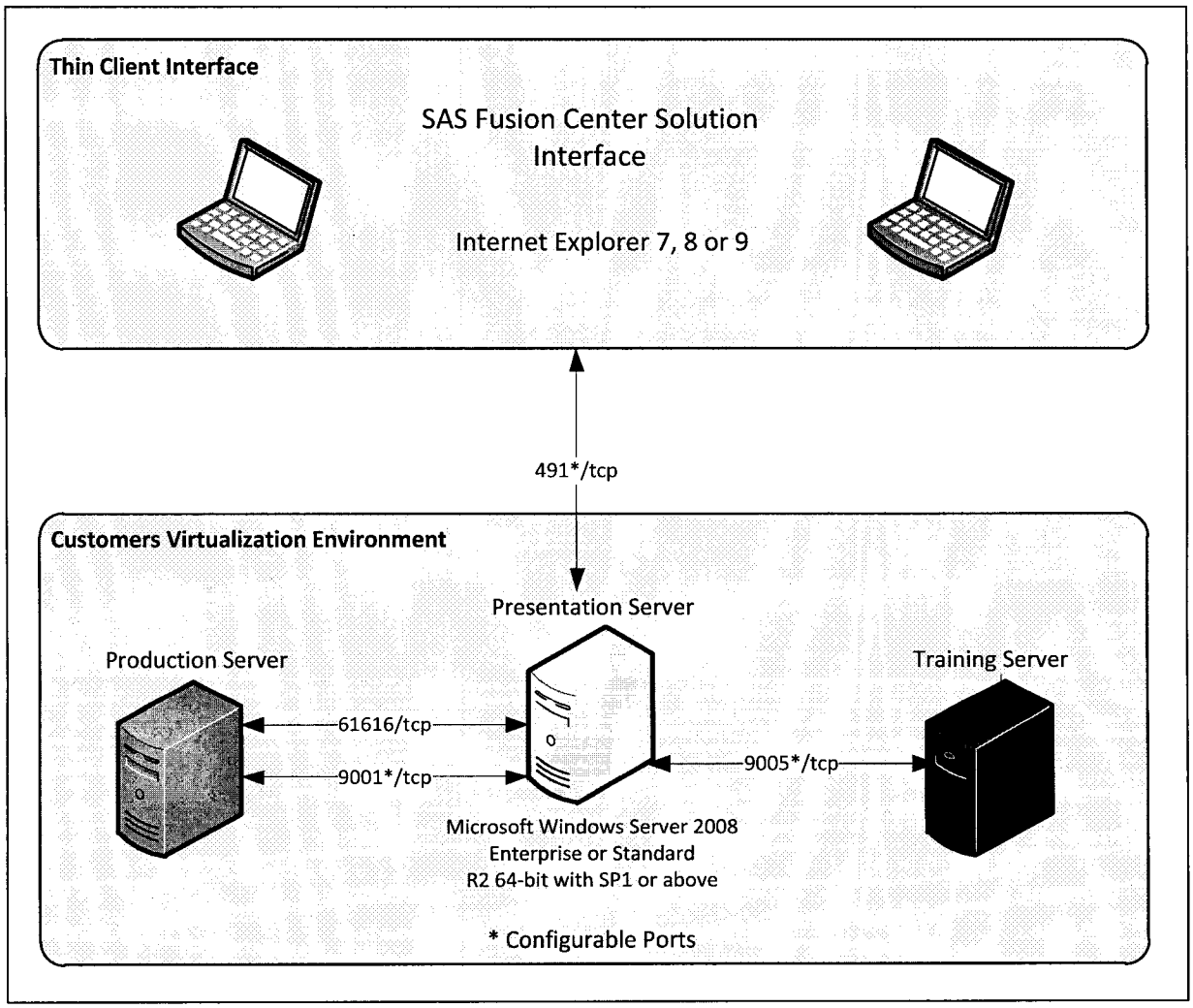


Figure 11: Production and Training Hardware Environment

Presentation Server

The presentation server will host the third party application "GoGlobal", a web enabling solution that allows client applications to be accessed via your corporate internet browser.

The following specifications are recommended.

Memory Requirements	2GB RAM
CPU Requirements	1 CPU Core

Production Server

For the proposed solution the production server is a self-sufficient environment containing all software components required to deploy and operate the solution. The software components installed and configured on the Production server are:

- Memex Intelligence Engine which includes:
  - The data repositories for the SAS Fusion Center Solution
  - The indexing engine for the management and search of structured and unstructured data
  - Authentication process
  - Security process
  - Auditing process
  - Batch services for email notifications
- SAS Fusion Center Solution meta data configuration for the following modules
  - Intelligence Management
  - Suspicious Activity Reporting
  - Request For Service
  - Confidential Informant Management
  - User Group database

Memory Requirements	8GB RAM
CPU Requirements (Assuming 2 GHz CPU speed)	2 CPU Cores
Estimated Disk Space Requirements	200 GB

Training Server

This server contains the exact configuration as the production server but will be used for training activities. Any optional components added to the production server will also be added to the Training Server. Typically the training server does not need the same level of hardware resources as the production server. As this machine is virtualized it can be turned off when not in use. Port 9005 is typically the default port used by the SAS Memex Server although this can be configured to another port if required.

Memory Requirements	1GB RAM
CPU Requirements (Assuming 2 GHz CPU speed)	1 CPU Core

Estimated Disk Space Requirements	100 GB

Client Environment

For SAS Software Release	2.13
Operating Systems	Microsoft Windows XP with Service Pack 3 Microsoft Windows 7 32-bit and 64-bit
Supported GIS Map Viewers	ESRI ArcGIS 9.3, 10.0 and 10.1
Deployment Mechanism	Full Client Installation / Web Browser Deploymeny
Client Prerequisites	
Microsoft Office	Microsoft Office 2003, 2007 or 2010
Microsoft .NET Framework	.NET 3.5 SP1
Adobe Flash	Server-based WebHelp requires Adobe Flash Player to be installed on the client computer
Document iFilters	To make the text of a document attached to a Memex record searchable, the appropriate iFilter for the file type must be installed on the computer on which SAS Memex is installed.

More technical information is available upon request.

Licenses products: SAS Fusion Center Solution
This includes the following modules:

- Request for Service (RFS) Module
- Intelligence Management Module
- Suspicious Activity Reporting (SARS) Module
- Confidential Informant Management Module

Please see next the response to the next question for information on license rights.

The City prefers broad license rights for all software and other technology, including perpetual, fully-paid and royalty free use rights for commercial off the shelf software. The City also strongly prefers ownership of all custom software and interfaces. The City will require a source code escrow agreement where applicable. The City will make a business decision for selecting a Vendor-Hosted Solution or a City Hosted Solution.

SAS' standard licensing model for the software described in this response is based on an annual, rather than perpetual model. SAS and the City have previously licensed software on such an annual basis and SAS is confident such a model will meet the requirements set forth by the City in the RFP. All right, title, interest, and ownership in the software and any resulting work product from the services described in this response will remain with SAS Institute Inc. at all times. Any mutually agreed upon license agreements for such software and services will set forth appropriate license terms for the City.

Consistent with Section 015 of the RFP, SAS does not intend to enter into a source code escrow agreement with the City for the solution described in this response.

D. Third Party Products/Options Software

The Respondent must explicitly state the name of any third-party products that Respondent will be providing as part of the proposed solution. Respondent must have, and must demonstrate upon request, that it has authorization to transfer any rights of use and warranties for third-party products to the City. 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.

License Type	Product	Comments
Commercial	Go Global	Web Enabling
Open Source	Activiti	BPMN Workflow
Open Source	Postgresql	Workflow datastore
Open Source	Jetty Web Server	Internal Web Services

E. Maintenance and Support

Respondent should specify the prime contractor and software vendor(s) who plan to carry out post-implementation and ongoing support, including:

1. Telephone support (include toll-free support, hours of operation). A hotline that provides at least 12 hours, 5 days per week availability Monday through Friday from 7:00 a.m. to 7 p.m.
Technical support is available to SAS customers five days a week from 8 a.m. to 6 p.m. Eastern time. Outside of these hours, SAS has customer support staff on call to handle any issues that arises. SAS' customer support team can be contacted via telephone, e-mail or the web. The SAS license and maintenance agreement provides technical maintenance and support at no additional charge that includes the following:

- Updates to software and documentation
- Software patches and bug fixes
- Help with system configuration problems, end-user problems, and with other aspects of using the proposed software system

2. Delivery method for future upgrades and product enhancements including frequency of upgrades.
Future upgrades and product enhancements can be downloaded from the SAS website and are free of additional charge; they are part of the standard service covered by the renewal fee. SAS uses three kinds of software releases:

- Major Releases: These releases contain significant design and functionality enhancements. These releases are available every 2 or 3 years.

- Minor Releases: These releases contain additions to existing functionality and minor enhancements and updates. On average these releases are available once a year.
- Maintenance Releases: These releases contain small additions of functionality and bug fixes. These releases are usually available twice every year.

3. Problem reporting and resolution procedures.
SAS technical support can be contacted via telephone, e-mail or the web. All problems reported are initially handled by a consultant who works with the customer to identify and (in many cases) solve the problem. If the consultant cannot resolve the problem on primary contact, he/she assigns it a tracking number and does additional research on the problem or passes it to a specialist. Goals for initial follow-up after a problem in production software is first reported are based on the nature and severity of the problem; and the consultant will make every attempt to contact the customer within these response time goals. If the normal support process does not produce the desired results, or if the problem has changed in priority, the problem can be escalated as follows:

- The customer should first contact the consultant working on the problem and request that the priority of the problem be escalated
- If additional escalation is required, the customer may request to speak with a Technical Support manager
- If continued escalation is required, the problem may be referred to the head of Technical Support

SAS has won numerous awards from software publications for the quality and responsiveness of its technical support. A recent survey found that over 83% of SAS users rated SAS' technical support as "better" or "much better" than other software support. On average, more than 58 percent of the questions for technical support in the U.S. are resolved on the first phone call; 77 percent are resolved within one day; and 87 percent are resolved within five days.

4. Delete.
Per Addendum III this requirement was deleted.

5. Bug fixes and patches.
Software maintenance for the SAS system is normally provided through replacement executable modules, or hot fixes. Availability of hot fixes is announced on SAS' technical support web site. SAPD can be notified of the availability of hot fixes via e-mail by subscribing to an automated mailing list.

6. Performance tunings and incremental enhancement.
Through SAS' Customer Care Program, SAPD may procure a block of hours for additional ad hoc consulting support on an ongoing basis to assist with performance tunings, incremental enhancement, and miscellaneous system support issues above and beyond normal technical support. All services are procured on a time and materials basis in accordance with a corresponding services agreement. The hourly rates for this are consistent with those quoted for the initial development resources of the project. Travel is generally billed at cost, but can also be built into the hourly rate if required.

7. On-line support.
SAS has an Online SAS Knowledge Base that provides a convenient way to locate information, answer questions, and ensure task completion. SAS knows that not all problems require technical support; therefore, this area provides self-help and assistance resources to our customers.

Maintenance and support will begin after the expiration of a two-year warranty period and last for the remainder of the initial term, and include the optional extension terms. Warranty period shall begin upon final written acceptance of system by City.
SAS standard licensing model issues software licenses to customers on an annual basis, subject to renewal by mutual agreement of the parties. SAS' prices offered to the City with respect to the software described in this response assumes a coterminous twelve (12) month period of support and maintenance and twelve (12) month warranty period, beginning on the date a contract with the City is executed. SAS acknowledges the City's desire for a twenty-four (24) month software license period. Accordingly, any resulting license for the software will be for a two year license period, which includes a (i) twenty-four (24) month warranty period, and (ii) twenty-four (24) month period of maintenance and support. The warranty, maintenance, and support for such software will begin on the date any contract with the City is executed. Any renewals to the software following such initial two year period will be upon mutual agreement of the parties.

F. Training and Costs

Provide training options and details of training plans and costs. Provide training costs on a per trainee basis. Training options should include web-based and classroom-based training.

Training Plan

- **Fusion Center Solution User Training:** SAS Consultants will provide 3 onsite user training classes, each lasting 3 days, covering the use of the SAS Fusion Center solution that will include RFS, SAR and Intelligence Module Training. Up to 12 people may attend each class. It is assumed staff attending the training will not have any prior experience of using the Memex system.
- **Confidential Informant Management System (CIMS) Module Training:** SAS Consultants will provide up to 3 x 1 day onsite training classes for up to 12 users per class who are involved in the confidential informant management process. (Note. It is currently unknown what the total number of CIMS users will be. This proposal assumes up to 35 users may need to be trained on this module) CIMS students must have completed Fusion Center Solution User Training.
- **Memex Administrator Training:** SAS Consultants will provide 1 system administrator training class, lasting 2 days, covering the administration of the SAS Memex system upon which the Fusion Center Solution is built. The course will cover managing system users and permissions as well as server 'housekeeping' activities. It is assumed attendees will have some experience of administering similar systems.
- **Fusion Center Solution Refresher User Training:** SAS Consultants will provide 2 days of refresher training to users of the system at a mutually agreed time after the system becomes operational. The purpose of this training is to optimize knowledge transfer and retention. This training can be provided in a consolidated format onsite in a classroom environment or remotely via the web as part of a series of the short (60 – 90 minute) tactical training classes totaling 16 hours that will focus on specific components or modules. These webinar training sessions will be recorded and will be available for download by the customer for future use as part of a library of training videos.

The costs below are based on the following assumptions:

- Thirty five (35) users will need to be trained on User and CIMS applications
- Five (5) users will be need to be trained on the Administrator functions
- A limit of 12 students per User and CIMS session
- A limit of 5 students per Administrator session
- Time includes training preparations and setup effort.
- Individual trainee pricing has been provided below however these training costs are based on training group classes with a maximum of 12 attendees.

User Type	SAS Prep Hrs	Train Hrs	Total Hrs	Cost per Hr	Training Session Cost	Cost per Student	Sessions needed	Total Cost
User	12	24	36	$190	$6,840	$570.00	3	$20,520
CIMS	8	8	16	$190	$3,040	$253.33	3	$9,120
Administrator	8	16	24	$190	$4,560	$912.00	1	$4,560

Refresher	N/A	16	16	$190	$3,040	$253.33	1	$3,040
								$37,240

Training Plans – User, CIMS and Administrator
SAS Memex classroom training uses near real-life scenarios to keep the instruction engaging and effective. Using law enforcement and homeland defense training examples culminates in increased user retention and adoption of SAS Memex.

The User Training Plan will cover the following topics:

- Configuration Overview
- Getting Started
- Getting to Know the Main Window
- Viewing your User Profile
- Finding Information
- Building Search Queries
- Entering Information - SAR
- Entering Information - Intel Report
- Entering Information - RFS
- Setting a Flag or Interest Marker
- Working with Notifications and Messages
- Linking Information
- Printing Records
- Deleting Records
- Working with Tasks
- Organizing Security
- Working with Bulletins
- Working with GIS
- Importing information from CSV files
- Using Memex Query Language

The CIMS Training Plan will cover the following topics:

- Introduction
- CIM Process Overview
- CIM User Setup
- Create and submit a Preliminary Request
- De-Confliction Checks by Level 3 Supervisors
- Approve, Deny or PFI - Preliminary Requests
- Create Private Profile
- Complete and Submit Private Profile
- Submitting a Private Profile
- Approve, Deny, PFI or Undesirable - Private Profile
- Create Public Profile
- Record CI Contact
- Adding Contact without Payment
- Adding Contact with Payment
- Approval of Contact

- Create an Intelligence Report from a CI Contact
- View Payments made to a CI – 2 ways
- Viewing all CI Contacts
- Deactivation of CI
- Request Deactivation
- Deactivation Request Response
- Reactivation of CI
- Request Reactivation
- Reactivation Request Response
- Changing Handler on Private Profile form
- Transition of CIs to new Handler or Supervisor

The Administrator Training Module will cover the following topics:

- Configuration Overview
- Getting Started
- Getting to Know the Main Window
- Finding Information
- Organizing Security
- Working with Bulletins
- Working with GIS
- Importing information from CSV files
- Using Memex Query Language
- Memex Patriarch Help
- Related documentation
- Configuring Memex Patriarch
- Managing users and user groups
- Creating and maintaining picklists
- Auditing user activity
- Restoring and archiving information
- Application logging
- Shutting down and restarting servers
- Importing information from CSV files
- Using Memex Query Language

G. Travel

If the selected, Respondent is not located within the corporate limits of the City of San Antonio, the selected Respondent shall include the cost of travel to San Antonio or any other location for the performance of the services contemplated herein to be included. Meetings (with the exception of the exception of the presentation(s) may be conducted telephonically.

Assumptions:

- Remote access to all networks and servers involved with project will be provided.
- Meetings and training will be conducted at or near downtown San Antonio
- Due to the short time line for implementation and travel expected around the holiday season, travel expenses will be higher than average.

- SAS is estimating 12 employee trips to San Antonio for this project. Each trip may have 1-3 individuals travelling.

Estimated Travel Cost:

Flights	Hotel (per night)	Food (per day)	Transport (per day)
$300-600	$150-$200	$75-100	$80-120

Example:

5 day, 4 night stay for 2 SAS employees	
Traveler 1:	Denver to San Antonio
Flight	$368
Hotel	$650
Food	$300
Transport	$400
Traveler 2:	Detroit to San Antonio
Flight	$550
Hotel	$650
Food	$300
Transport	NA
Total:	**$3,218**

H. TECHNICAL REQUIREMENTS

The proposed system solution should be able to integrate with the current Information Technology Environment Description Standards. Refer to RFCSP Exhibit 5.

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.

If any 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.
RFCSP Exhibit 5 has been reviewed and the proposed solution will integrate and operate within the documented environment.

As of the submission of this proposal no information technology equipment is required to be deployed outside of the City's managed datacenter environment.

005 ADDITIONAL REQUIREMENTS

SAS looks forward to putting in place a mutually agreeable contract for the software and services described herein. SAS agrees in principle with the provisions referenced in Section 005 of the RFP; provided, however, that SAS' response to the RFP does not constitute a contract with the City of San Antonio and is contingent upon the parties' agreement to separately negotiated, mutually acceptable contract terms and conditions should SAS be selected as the vendor. Such terms and conditions include, but are not limited to (i) the inclusion of license terms governing the City's use of the software and work product resulting from the delivery of any services, (ii) a statement that title to intellectual property is not transferred by any resulting contract and that the ownership of SAS' proprietary software and work product remains with SAS at all times, and (iii) the inclusion of a mutually agreed upon limitation of liability. Nothing in the RFP or SAS' response thereto shall be deemed to constitute an agreement between SAS and the City of San Antonio.

Notwithstanding anything else contained in the RFP to the contrary, all of SAS' ideas, products, services, solutions, and other information remain with SAS at all times.

Respondent Questionnaire: Attachment B

The Respondent Questionnaire: Attachment B is provided on the following pages in hard copy and as a separate PDF file on the CD.

019 RFCSP ATTACHMENTS

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: SAS Institute Inc.
(NOTE: Give exact legal name as it will appear on the contract, if awarded.)

Principal Address: 100 SAS Campus Drive

City: Cary State: North Carolina Zip Code: 27513-2414

Telephone No. (919) 677-8000 Fax No: (919) 677-4444

Website address: www.sas.com

Year established: 1976

Provide the number of years in business under present name: 37

Social Security Number or Federal Employer Identification Number: 56-1133017

Texas Comptroller's Taxpayer Number, if applicable: 15611330174
(NOTE: This 11-digit number is sometimes referred to as the Comptroller's TIN or TID.)

DUNS NUMBER: 040046724

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
_X_Corporation If checked, check one: _X_For-Profit ___ Nonprofit
Also, check one: ___Domestic ___Foreign
___Other If checked, list business structure: _____

Printed Name of Contract Signatory: Victoria P. Clayton
Job Title: Senior Contracts Manager

Provide any other names under which Respondent has operated within the last 10 years and length of time under for each:
Not Applicable

Provide address of office from which this project would be managed:
City: Cary State: NC Zip Code: 27513-2414

Telephone No. (919) 677-8000 Fax No: (919) 677-4444

Annual Revenue: $ 2.87 billion (2012)

Total Number of Employees: 13,732 worldwide

Total Number of Current Clients/Customers: SAS has customers in 135 countries and more than 65,000 business, government and university sites. SAS Customers represent 90 of the top 10 companies on the 2012 FORTUNE Global 500® list.

Briefly describe other lines of business that the company is directly or indirectly affiliated with:
Not Applicable

List Related Companies:
Not Applicable

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

Name: Andrew Coulter Title: Associate Inside Sales Account Rep

Address: SAS Institute Inc., 100 SAS Campus Drive

City: Cary State: North Carolina Zip Code: 27513-2414

Telephone No. (919) 531-5791 Fax No: (919) 677-4444

Email: Andrew.Coulter@sas.com

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 X

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

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

SAS' has a Certificate of Authority to do business in Texas as a foreign corporation under Charter Number 0006484906.

5. Where is the Respondent's corporate headquarters located? Cary, North Carolina

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

Yes ___ No X 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 X 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 X 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 X 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 X 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.

Not to SAS' knowledge after commercially reasonable investigation

11. **Previous Contracts:**

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

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

Not to SAS' knowledge after commercially reasonable investigation

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 X If "Yes", state the name of the individual, organization contracted with, services contracted, date, contract amount and reason for failing to complete the contract.
Not to SAS' knowledge after commercially reasonable investigation; SAS also provides that personnel actually assigned to the project, upon award of any contract with the city, will be dependent upon availability.

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 X If "Yes", state the name of the individual, organization contracted with, services contracted, date, contract amount and reason for failing to complete the contract.

Not to SAS' knowledge after commercially reasonable investigation; SAS also provides that personnel actually assigned to the project, upon award of any contract with the city, will be dependent upon availability.

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.

To ensure the most effective use of the State's and our customers' time, SAS would be happy to arrange a mutually convenient time for representatives of your organization to speak with a reference customer. Please contact our Customer Reference Manager, Donna Daniels, at (919) 531-6174 or Donna.Daniels@sas.com to coordinate customer reference calls.

The completed reference form is provided on the following pages in hard copy and as a separate PDF file on the CD.

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 Pennsylvania State Police

Contact Name: Lt. Colonel George Bivens Title: Lt. Colonel

Address: 1800 Elmerton Avenue
City: Harrisburg State: PA Zip: 17110
Telephone No. 717.783.5512 Email: gbivens@state.pa.us

Date and Type of Service(s) Provided: Initial Project Start: 1999, Initial Project Completion: 2000 Multiple enhancements: Through 2011. Services provided include: COTS intelligence management solution supporting the agency's intelligence-led policing philosophy Development of custom database interfaces; Expansion of solution to incorporate a tips and leads module; Expansion of solution to include the MDT/Officer safety interface; Integration with RISSNET; Move to 24/7 intelligence center

Reference No. 2:

Firm/Company Name Michigan State Police/Michigan Intelligence Operations Center (MIOC)

Contact Name: 1) D/Sgt. Gene Aldrich Title: MIOC Privacy Officer / MCIS Administrator
2) D/Lt. Paul Pummill Title: MIOC Assistant Commander

Address: 333 South Grand Ave.
City: Lansing State: MI Zip Code: 48909-0634

Telephone No.1) 517-335-0181 2) 517-335-4296 Email: 1) AldrichE@michigan.gov 2) PummillP@michigan.gov

Date and Type of Service(s) Provided: Initial Project Start: End of 2008, Initial Project Completion: 2010, Multiple enhancements: Through 2013. Services provided include: COTS state-wide intelligence management solution supporting the agency's intelligence-led policing philosophy; Fusion Center Support modules (SAR, RFS. Public SAR Web site); Data Integrations; Expansion of solution to interface with the Nationwide SAR Initiative (NSI); Integration with RISSNET

Reference No. 3:

Firm/Company Name: State of Nebraska/Nebraska Information and Analysis Center (NIAC)

Contact Name: Captain Kevin Knorr Title: Captain

Address: 3800 NW 12th Street
City: Lincoln State: NE Zip Code: 68521

Telephone No.402-479-4930 Email: Kevin.Knorr@nebraska.gov

Date and Type of Service(s) Provided: Initial Project Start: End of 2009; Initial Project Completion: 2013; Multiple enhancements: Through 2013. Services provided include: COTS state-wide intelligence management solution supporting the agency's intelligence-led policing philosophy; Fusion Center Support modules (SAR, RFS); 17 Data Integrations; Expansion of solution to interface with the Nationwide SAR Initiative (NSI); Integration with RISSNET; Expansion of solution to include Gang intelligence functionality

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. Describe Respondent's experience relevant to the Scope of Services requested by this RFCSP. List and describe three relevant projects of similar size and scope performed over the past four years. Identify associated results or impacts of the project/work performed.
The following references from Michigan State Police/Michigan Intelligence Operations Center (MIOC), State of Nebraska/Nebraska Information and Analysis Center (NIAC) and Pennsylvania State Police/Pennsylvania Criminal Intelligence Center (PaCIC)

Pennsylvania State Police

Pennsylvania State Police (PSP) initiated a search for an Automated Intelligence System (AIS) to replace their aging mainframe system (MOSAIC) in the mid 1990's and selected the SAS solution over a number of vendors to supply an enterprise wide intelligence and analysis system to Intel Officers throughout the Commonwealth. SAS' Memex Solutions Team was engaged to provide a set of integrated technologies that addressed specific intelligence gathering, management and analysis requirements and align them with the Commonwealth's adoption and deployment of the Intelligence Led Policing (ILP) model. In the capacity of prime contractor, SAS provided off-the-shelf intelligence software to address the PSP requirements in addition to custom-designed external interfaces. These custom features permitted authorized end users to search other proprietary Commonwealth databases including the Commonwealth Law Enforcement Assistance Network, Pennsylvania Department of Transportation, and the Pennsylvania Justice Network. Data migration programs were also developed to convert existing data held in a variety of database formats and systems into the SAS environment to allow comprehensive searches to be performed across multiple data sources.

The SAS team was embedded into the PSP environment and worked closely with operational intelligence personnel and the Bureau of Information Technology to design, manage, test and deploy the system across the state. Finally, SAS prepared the Commonwealth for success by providing end user and technical training prior to full deployment to 50 users, supporting many missions including: Major Crimes,

Summary

- *State Police Initiative*
- *Intensive selection process for replacement intelligence system*
- *COTS intelligence management solution supporting agencies Intelligence Led Policing philosophy*
- *Development of custom database interfaces*
- *Solution expanded to incorporate Tips and Leads module, soon to migrate to SARs*
- *RISSNet expansion*
- *Officer Safety Expansion*
- *Move to 24/7 Intelligence Center*
- *Ten year customer continuing to expand the functionality of the SAS solution*

Counter-Terrorism, Counter- Narcotics, Outlaw Motorcycle Gangs, Street Gangs, Organized Crime, Homeland Security, Screening / Watch-list, and First Responder Coordination. Today, there are more than 300 officers statewide that access the SAS solution via the web.

With the introduction of public tips and leads submissions, PSP engaged SAS to address the need to effectively capture and process incoming information for future assignment and analysis. The inherent flexibility of the SAS solution allowed the system to be expanded at no cost and, within weeks, an automated tip and lead capture mechanism was being used to stream incoming email submissions from the public into the existing SAS platform. The team is now working with the PSP, BJA and IJIS to schedule the replacement of the Tips and Leads module with the SARs module for integration with the NSI and the automated export of SARs data to the shared space.

In 2004, as part of the Commonwealth's Integrated Information Management System (IIMS) primed by Lockheed Martin, SAS used the new web services interface to open the PSP Automated Intelligence System to third party systems and allow access to subsets of data from mobile data units. The driving principle was Officer Safety, and by permitting automated search access to filtered intelligence information, SAS was able to provide relevant data or Officer Safety warnings to the patrol units anywhere in the Commonwealth.

In 2010, PSP became a Type 1 RISSNet Node and deployed SAS' RISSConnect software to push their data onto the RISS Network.

Relevance
The PSP solution addresses the following goals:

- *Intelligence-Led Policing model*
- *Centralized intelligence management platform*
- *Supports a broad range of users' roles and responsibilities, including browser-based usage*
- *Integration of legacy data*
- *Integration with third party systems*
- *Integration with law enforcement initiatives and networks, such as RISSIntel*
- *Advanced structured and unstructured search capability*

Most recently, PSP has contracted with SAS to deploy our SARs solution and to establish a pointer index system between the PSP Fusion Center Solution and the Lehigh Valley Data Sharing Initiative.

State of Nebraska/Nebraska Information and Analysis Center (NIAC)

The Nebraska Information and Analysis Center (NIAC) selected SAS via a competitive procurement to provide a turnkey, commercial off-the-shelf (COTS) software solution for use in the information and intelligence fusion process that can be used at remote sites, connect multiple databases and other sources of data, and provide for intelligence/intelligence case management and analytical capabilities including crime analysis. The NIAC's stakeholders include the Nebraska State Patrol, Lincoln Police Department and the Omaha Police Department.

SAS provides a platform for intelligence management, information exchange, case management, and analytical capabilities to NIAC. Some 200 law enforcement officials throughout Nebraska

will use the SAS Memex platform (the foundation for the SAS Fusion Center Solution) connecting 17 different law enforcement data sources through an indexed search of selected data and federated search model. Among those data repositories are Records Management Systems (RMS), Computer-Aided Dispatch (CAD), Mug Shot Integration, Penlink (subscription and toll records), RISS and Automated Fingerprint Identification System (AFIS). The NIAC is also using SAS to export SARs in conformance with the NSI. As a result of its compliance with the FBI's National Data Exchange (NDEX) system, SAS can also make it possible for NIAC and its sister agencies to easily export and share RMS data that is migrated into the solution. The solution is automating the collection, collation and processing of intelligence and criminal data in an all-hazards environment. The solution is automating the dissemination of intelligence information to law enforcement personnel internally and externally to the NIAC and its stakeholders. Additionally, SAS provided the hardware specifications for the solution, which the state subsequently procured.

Relevance
The NIAC solution addresses the following goals:

- *Centralized data sharing and intelligence management platform*
- *Supports a broad range of users roles and responsibility, including browser-based usage*
- *Integration of legacy data*
- *Integration with third party systems*
- *Multi-jurisdictional deployment*
- *Hardware recommendations and architecture deployed*
- *Advanced structured and unstructured search capability*
- *Integration with RISS, Penlink, RMS Systems and SARs export*

The State has secured an enterprise license for the software, which will permit every jurisdiction in the state to use the solution to access the 17 data sources being made available. The RMS and CAD data from the Nebraska State Patrol, Lincoln PD and Omaha PD are all being brought into the solution, and many of the remaining data sources will be accessed via federated queries. SAS is also providing its Comp Stat module to support standard reporting.

The state is also in the process of deploying the Gangs module as well as the Confidential Informants (CI) module, providing a single-source portal for the state's SARs, Intelligence, and Criminal Information needs.

Michigan State Police/Michigan Intelligence Operations Center (MIOC)

Implemented in November, 2010, the Michigan Criminal Intelligence System (MCIS) serves as the primary criminal intelligence processing system in the State of Michigan. It will potentially provide access to more than 600 law enforcement agencies, 21,300 certified police officers and numerous state and federal departments. The MIOC selected SAS Memex Platform (the foundation for the SAS Fusion Center Solution) as the foundation for MCIS to gather, collate, track, analyze and disseminate terrorism intelligence information. Additionally, the MCIS will

be used to counteract conventional criminal activity, including street gangs, organized crime and high-volume crimes.

SAS replaced the existing legacy Statewide Intelligence System and migrated the data to the SAS Fusion Center Solutions Intelligence module. In addition to criminal intelligence data, SAS is also laying the foundation for the sharing of CAD and RMS data in the MCIS.

The MCIS also includes a "Tip Tool" to store and process suspicious activity information received through various reporting methods, including a public-facing web page we developed. Most recently, SAS has expanded this capability by providing a web service interface to the FBI's eGuardian solution permitting the automated export of this data to the FBI. SAS has also provided a bi-directional interface with the Regional Information Sharing System (RISS) that permits intelligence data from Michigan to be shared with the RISS, and to read information contained on the RISS network.

Finally, the solution has also been integrated within the Michigan Criminal Justice Information Network (MiCJIN) portal for user authentication. The MiCJIN portal is compatible with eDirectory and Active Directory LDAP directory structures, utilizing industry standard SAML 2.0.

2. Indicate the number of years Respondent has been in the business of working in a Major City Intelligence Unit or recognized Fusion Center, respectively. Indicate if Integrated Information and Intelligence Management Law Enforcement Solutions is the Respondent's primary line of business. If not, state the Respondent's primary line of business.

SAS has been delivering solutions to the Criminal Intelligence marketplace in the US since 1998 giving the proposed team 15 years of software development and implementation experience in this vertical. Prior to the events of 9/11/2001 and the inception of the Fusion Center concept in 2002 the Justice and Public safety arm of SAS had already implemented their criminal intelligence platform to State Police departments in Pennsylvania and New Jersey and a nationwide intelligence management solution for the National Insurance Crime Bureau. These initiatives leveraged previous Law Enforcement successes in the United Kingdom where since 1995 the solution was being deployed to support large national, major city and major county Intelligence Led Policing initiatives including the London Metropolitan Police where today 40,000 registered users operate on the platform that is being proposed for the SWTFC. Customers continue to use the next generation of intelligence products and solutions produced by SAS and as of this response's submission date 12 Fusion Center and Terrorist Early Warning Group environments have been recipients and still operate the proposed solution.

SAS is the global leader in business analytics software and services, and the largest independent vendor in the business intelligence market. SAS services 10 major market verticals providing industry specific business solutions that are built on the SAS Analytics Framework. The system proposed is a business solution that has been specifically designed to meet the needs of a Fusion Center environment and is the spearhead application for ILP based customers who are serviced by the SAS State and Local Government business unit.

3. List all Integrated Information and Intelligence Management Law Enforcement Solution projects that the Respondent has completed in the last four years.

New law enforcement projects include:

Primary Customer	Customer Entity	Project Title	Description
State of Michigan	State Police / Michigan Intelligence Operation Center	Michigan Criminal Information System (MCIS)	➢ Fusion Center based solution including ➢ Request For Service ➢ NSI-SAR ➢ ISE-SAR Integration ➢ Multi-Agency Intelligence Management
State of Nebraska	State Police / Nebraska Information and Analysis Center	Nebraska Fusion Information Network	➢ Fusion Center based solution including ➢ Integration if 17 multi-jurisdictional data sources including RMS & CAD ➢ Request for Service ➢ NSI-SAR ➢ Multi-Agency Intelligence Management ➢ Confidential Informant Management ➢ Gang Intelligence ➢ RISS Integration
City of Phoenix	Homeland Defense Bureau - Arizona Counter Terrorism Information Center (Phoenix Police Dept.)	NA	➢ Intelligence Management ➢ Confidential Informant Management ➢ Case Management
City of Philadelphia	Philadelphia Police Depart. Integrity Control Office.		➢ Confidential Informant Management ➢ RISS Integration
Ohio Dept. of Public Safety	Strategic Analysis and Information Center		

Law enforcement project extensions with existing customers active within the last four years include:

Primary Customer	Customer Entity	Project Title	Description
State of Michigan	State Police / Michigan Intelligence Operation Center	Michigan Criminal Information System (MCIS)	➢ Sex Motivation Crime Reporting ➢ School Violence Reporting System
State of Delaware	Delaware Information and Analysis Center		➢ Dept. of Corrections – Security Threat Group Data Exchange ➢ Statewide RMS Integration
Maryland State	Maryland Coordination & Analysis Center		➢ LPR Data Integration Project ➢ RISS Integration
Commonwealth of Pennsylvania	Pennsylvania Criminal Intelligence Center		➢ Bi-Directional External Agency Search Interface
City of Roanoke	Roanoke Area Criminal Justice Information Network	RACJIN	➢ Jail System Data Integrations ➢ N-DEx Search Interface ➢ Intelligence Management
Kansas City MO. Police Dept.	Kansas City Terrorist Early Warning Group		➢ ISE-SAR Integration ➢ External Agency RMS &CAD Integration
Central California Intelligence Center	CCIC		➢ eGuardian Integration ➢ Public Facing SAR Web Site Integration
Tennessee Bureau of Investigation	Tennessee Fusion Center		➢ ISE-SAR

4. List all Integrated Information and Intelligence Management Law Enforcement Solution projects that Respondent has in progress 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.

Customer	Project	Estimated Completion Date	PM Contact Name	Phone Email
Philadelphia Police Department	RISS – Federated search	10/31/2013	Brooke McGinn	(215) 439-2518 Brooke.McGinn@phila.gov
Delaware State Police	Confidential Informant Management	10/31/2013	Lt William Crotty	(302) 741-2760 William.Crotty@state.de.us
Michigan State Police	School Violence Reporting	10/15/2013	Rose Muckenthaler	(517) 335-1351 MuckenthalerR@michigan.gov
Maryland Coordinatio n and Analysis Center	MCAC LPR Integration	9/30/2013	Victor Williams	(443) 436-8804 victor.williams@mcac.marylan d.gov
Central California Intelligence Center	CCIC eGuardian Updates	10/31/2013	Melody Lafond	(916) 874-1327 mlafond@sacsheriff.com

5. 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 and the department for which Respondent provided those services.

For nearly four decades, SAS has delivered the latest technology to our government customers, taking their operations to new levels. Our U.S. government practice helps federal, state and local departments and agencies meet their missions and goals faster and more accurately than ever before. SAS' goal is to be the most valued competitive weapon in government decision making. As the leader in business analytics software and services, and the largest independent vendor in the business intelligence market, SAS serves more than 65,000 government, university, and business sites in over 130 countries, including 90 of the top 100 FORTUNE Global 500® companies. SAS solutions are used extensively by all 15 federal departments, approximately eighty-five percent (85%) of federal sub-agencies and quasi-governmental affiliates, and all 50 states.

Within a Law Enforcement context SAS has been delivering operational support systems to State and Local Police departments, its core market vertical in the US, since 1998. The platform that

has been proposed for the SWTFC has been implemented in nine large state level entities including State Police and State Departments of Public Safety and State Fusion Centers. Major cities and urban area customers include the cities of Phoenix, Philadelphia, Los Angeles, Kansas, Cincinnati and Cleveland.

6. If Respondent is proposing as a team or 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.
SAS will provide all services for this project. No sub-contractors will be used.

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

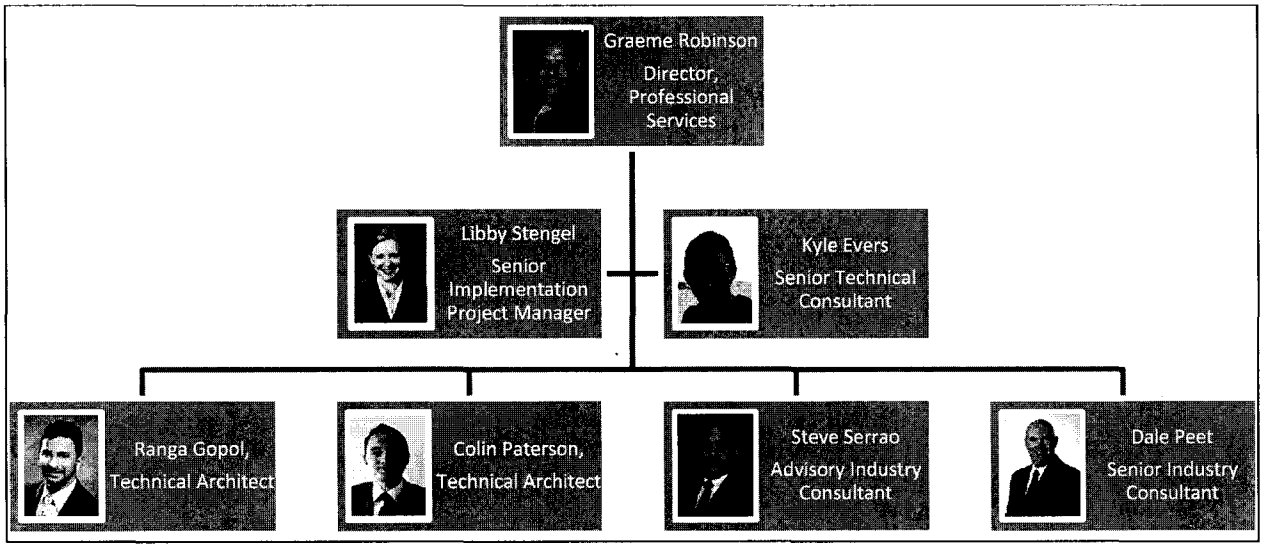


Figure 12: The proposed project team.

a. Identify each individual's relationship with the Respondents organization – employee, contractor, 3rd party service/software provider
All individuals assigned to this project are SAS employees. No contractors, 3rd party service or software providers will be used.

b. Identify the number and professional qualifications (to include licenses, certifications, associations)
Steve Serrao

- Certified Police Officer. NJ State Police
- Member, International Association of Chiefs of Police (IACP)
- Member, ASIS International – (ASIS is the largest international organization for professionals responsible for security, including managers and directors of security)
- International Association of Law Enforcement Intelligence Analysts (IALEIA)
- Member and Former Mid-Atlantic Chapter President

Dale Peet
- Certified Police Officer Michigan State Police
- Certificate, Northwestern University School of Police Staff and Command
- FBI National Academy Graduate 222
- Member, International Association of Chiefs of Police (IACP)
- Member, FBI National Academy Associates
- Member, Fraternal Order of Police

Graeme Robinson
- Microsoft Certified Solution Developer
- Advanced instructor level qualifications in small boat sailing
- Certificated Private Pilot

Kyle Evers
- Certificate of Applied Computer Science – Purdue University
- Certificate of Sound Engineering & Music Production – RECW

Libby Stengel
- Member, International Association of Crime Analysts (IACA)
- Member, International Association of Chiefs of Police (IACP)

Ranga Gopal
- Microsoft Certified Professional
- SAS Data Integration Studio Essentials
- Teradata Basics

Colin Paterson
- Bachelors of Science Honors in Computer Science – University of Glasgow

c. Identify relevant experience on projects of similar size and scope
Resumes with more detailed experience information are located in Appendix A.

Steve Serrao
Captain Steve Serrao (NJSP – Retired) serves as a subject matter expert for our fusion center, intelligence and law enforcement operations in support of current and new product development efforts, as well as being frequent trainers for deploying our intelligence management solutions. Steve is often published and quoted on topics ranging from establishing and managing fusion centers, data sharing and leveraging intelligence assets to combat crime.

Steve retired from the New Jersey State Police in 2006 at the rank of Captain after twenty-five years of service in several assignments – including, Intelligence Management & Analysis, Counter-Terrorism, and Special Assistant to the Superintendent – as well as mover than two dozen Letters of Commendation for work as an Intelligence Officer and Investigator. Steve has significant experience investigating traditional organized crime and has also supervised the State Police participation with the FBI - Joint Terrorism Task Force and held the position of Assistant Director of Operations at the NJ Office of Counter-Terrorism. He has held top secret security

clearances and has been involved in communicating with the US National Intelligence Community regarding intelligence on terrorists and support cells. Steve served as a Special Assistant to Colonel J.R. Fuentes, Superintendent of the NJ State Police, where he was instrumental in the early design and set-up of the State of New Jersey Fusion Center known as the Regional Operations and Intelligence Center (ROIC). Steve was also the Project Manager for the design, purchase and deployment of the multi-million dollar Statewide Intelligence Management System in New Jersey.

Michigan Intelligence Operations Center (MIOC)

- Hosted design working groups and provided assistance in the deployment and training of users for the Michigan Criminal Information System.

Nebraska Information Analysis Center (NIAC)

- Provided assistance in the deployment and training of users at the NIAC.

Philadelphia Police Department

- Hosted design working groups for the Intelligence Management and Confidential Informants Management Projects and provided training for all sworn user

Dale Peet

Besides his experience being a 23 year veteran of the Michigan State Police, Mr. Peet has worked with many law enforcement agencies in a consulting capacity. He has assisted our customers with design, configuration, deployment and ongoing support of all modules of SAS Memex software. Mr. Peet has also provided user training for SAS Memex Solutions at many customer sites. Mr. Peet has worked in local agencies with 10-20 users all the way up to agencies with 500+ users.

Michigan Intelligence Operations Center (MIOC)

- Provided assistance in the deployment and training of users for the Michigan Criminal Information System to include RFS, CIM and SAR.

Nebraska Information Analysis Center (NIAC)

- Provided assistance in the deployment and training of users at the NIAC.

Arizona Counter Terrorism Information Center (ACTIC)

- Provided assistance with the implementation of a city wide SAS Memex CIM, CI, Case Management and federated search of RISS

Graeme Robinson

Mr. Robinson has been with SAS Memex for 12 years. In that time, he has implemented all SAS Memex modules available at numerous customer sites, small to very large. Now as Director of Professional Services, Mr. Robinson oversees all projects to ensure proper implementation.

Kyle Evers
Mr. Evers has successfully led the technical consultation, deployment and administrator training efforts for SAS Memex Solutions at many customer sites. Below are examples of customers similar in size and scope to SAPD.

Nebraska Information Analysis Center (NIAC)
- Responsible for state wide technical implementation of SAR, CIM, RFS, four unique RMS/CAD integrations and a federated search to Regional Intelligence Sharing System.
- 400+ users

Arizona Counter Terrorism Information Center (ACTIC)
- Responsible for the technical implementation of a city wide SAS Memex deployment of CIM, CI, Case Management and federated search of RISS
- Designed curriculum and presented all SAS Memex administrator training at customer site
- 400+ users

Pennsylvania Criminal Intelligence Center (PACIC)
- Responsible for technical implementation of RISS searching capability and Lehigh County federated search module
- 200+ users

Kansas City Regional Terrorism Early Warning Group (KCTEW)
- Responsible for implementing a Field Interview data integration. This integration is functioning as a statewide repository for intelligence information
- 200+ users

Libby Stengel
Ms. Stengel has successfully led the consultation, managed deployment and conducted user training efforts for SAS Memex Solutions at a wide range of local, regional, national and international customer sites. Below are examples of customers similar in size and scope to SAPD.

Nebraska Information Analysis Center (NIAC)
- Managed a state wide SAS Memex deployment of SAR, CIM, CI, RFS, four unique RMS/CAD integrations and a federated search to Regional Intelligence Sharing System
- Designed curriculum and presented all user and train-the-trainer instruction modules at customer site
- 400+ users

Arizona Counter Terrorism Information Center (ACTIC) – Phoenix Police Department
- Managed a city wide SAS Memex deployment of CIM, CI, Case Management and federated search of RISS
- Designed curriculum and presented all user and train-the-trainer instruction modules at customer site
- 400+ users

Roanoke Area Criminal Justice Information Network (RACJIN)

- Managed the deployment of CIM and the integration of six unique data integration sources into Memex SAS
- Designed curriculum and presented all user and train-the-trainer instruction modules at customer site
- 300+ users

Ranga Gopal

Mr. Gopal has made significant contributions to SAS's Justice and Public Safety practice through customer specific services work on the design and development of complex solutions and data integration projects. Below are examples of customers similar in size and scope to SAPD.

Nebraska Information Analysis Center (NIAC)

- Responsible for a number of the data integration and federated search interfaces for the multi-agency Nebraska Fusion Intelligence Network system.
- Responsible for the technical implementation and configuration of the SAS Confidential Informant Management Module
- 400+ users

Michigan Intelligence Operations Center (MIOC)

- Primary technical lead and responsible for the technical implementation of the SAS Fusion Center Solution at MIOC
- Responsible for the development of SAS's RISS Connect interface that supports the connection to the RISSNET environment and allows secure bi-directional access to data between RISS and the Michigan State Police
- 400+ users

Confidential Informant Management Solution

- Sole responsibility for the development and implementation of the SAS Confidential Informant Management System which he has successfully deployed at the following agencies over the past 12 months
- Phoenix Police Department / Arizona Counter Terrorism Intelligence Center
- Nebraska State Police / Nebraska Information and Analysis Center
- Delaware State Police / Delaware Information and Analysis Center
- Philadelphia Police Department

Colin Paterson

Mr. Paterson has successfully led enterprise level development, architectural design, deployment, training, requirements gathering, installation and project management at a number of customer sites. Below are some examples

Surry Police Department

- Led a team of 30 engineers, project managers, software testers, technical authors and support engineers during the design, development and implementation of Enterprise System at a major police department.
- 3,000+ users

Tennessee Bureau of Investigation

- Responsible for design and development of file and data import module at TBI as well as onsite implementation and training.

New Jersey State Police

- Responsible for user and administrator training of Intelligence Module to over 50 users during the roll out of statewide operational intelligence module

Pennsylvania State Police

- Responsible for training over 60 users on site at Pennsylvania state police in the use and continual operation of operational intelligence system.

British Transport Police

- Led team responsible for the implementation the Covert Informants Module at British Transport Police including architectural design, development, deployment and training.

Albanian Ministry of Public Order

- Responsible for roll out of Intelligence module and Data Warehousing solution including implementation, and training for the national police department of Albania.

Her Majesty's Prison Service

- Responsible for the implementation, training and roll out of Covert Informants Module throughout the London HQ of the UK Prison Service.

d. State the primary work assignment and the percentage of time to be devoted to the project.

Libby Stengel, Project Manager, Configuration Consultant – 95%
Role/Responsibility for this Contract

- Libby will be leading this project in a capacity of a Project Manager and Configuration Consultant. She will work to keep the project on time, within budget and meeting the customer's expectations. Libby will work with the customer to identify configuration requirements and manage the implementation of the SMP, SAR, CI, CIMS and RFS as well as any data migration/integrations. She will also oversee and/or conduct all user training associated with SAS Memex.

Kyle Evers, Technical Lead – 95%
Role/Responsibility for this Contract

- Kyle will be leading this project in a capacity of a Technical Lead. Kyle will be designing/managing configuration changes of the SMP, SAR, CI, CIMS and RFS modules.

Ranga Gopal, Technical Architect – 80%
Role/Responsibility for this Contract

- Due to Ranga's experience with the Confidential Informants Management module he will be primarily focused on the successful deployment of the that module into the SWTFC environment

Colin Paterson, Technical Architect – 80%
Role/Responsibility for this Contract

- Colin will be primarily focused in integration with the ESRI GIS and MS SQL Server environments

Dale Peet, Industry Consultant – 75%
Role/Responsibility for this Contract

- Dale will be the main consultant for this project. Dale will be lead working groups that help outline the design and workflow of the SMP, SAR, CI, CIMS and RFS. He will also assist leadership in defining key decision points.

Steve Serrao, Industry Consultant – 50%
Role/Responsibility for this Contract

- Steve will be assisting Dale with consultation on this project. Steve will be lead working groups that help outline the design and workflow of the SMP, SAR, CI, CIMS and RFS. He will also assist leadership in defining key decision points.

Graeme Robinson, Director of Professional Services – 35%
Role/Responsibility for this Contract

- Graeme will provide oversight for all activities associated with this project. He will assist with any technical or configuration issues, as needed.

e. Identify the length of service individual has been employed by the Respondent's organization

- Graeme Robinson—12 years
- Steve Serrao—7 years, 5 months
- Dale Peet—2 years, 11 months
- Kyle Evers—3 years, 5 months
- Libby Stengel—5 years, 10 months
- Ranga Gopal—3 years, 6 months
- Colin Paterson—13 years, 1 month

f. Provide resumes as an appendix to submitted proposal

Resumes are provided in Appendix A.

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

SAS has over 13,000 SAS employees in 400 SAS offices in more than 50 countries. SAS has a large staff of experienced technical representatives, including more than 1,500 expert consultants worldwide. SAS has a dedicated state and local government practice to help departments and agencies meet their missions and goals faster and more accurately than ever before. The SAS state and local government practice draws upon the talents of many other SAS consulting and research and development organizations to provide specific technical expertise when needed. This includes over 1,000 technical resources available to provide implementation assistance as needed.

In addition SAS has a dedicated customer loyalty team with the express purpose of helping customers get the most out of their SAS investment. This team is committed to responding quickly to customers' urgent needs and making certain long-term needs are addressed. Often, the customer loyalty team serves as a liaison to other support service teams at SAS. The customer loyalty team is also charged with understanding how customers are using SAS solutions, which contributes to SAS' ability to create innovative software that solves real business issues.

SAS technical support handles about 15,000 inquires per month. SAS has won numerous awards from software publications for the quality and responsiveness of its technical support. A recent survey found that over 83% of SAS users rated SAS' technical support as "better" or "much better" than other software support. On average, more than 58 percent of the questions for technical support in the U.S. are resolved on the first phone call; 77 percent are resolved within one day; and 87 percent are resolved within five days.

9. List the number of customers currently using the proposed solution. Include company name, type of business, city & state.

The names and project details of our customers, remain confidential until we have received their permission to release specific information about their applications. The following are some of our customers who are currently using the proposed solution.

No.	Name	Type	City	State
1	Belize Police Department (BPD)	Law Enforcement	Belize City	Belize
2	Bermuda Police Service (BPS)	Law Enforcement	Hamilton	Bermuda
3	Bibb County SO	Law Enforcement	Macon	Georgia
4	Chandler Police Department (CPD)	Law Enforcement	Chandler	Arizona
5	Cherokee County SO, GA	Law Enforcement	Canton	Georgia
6	Cobb County Police Dept. GA.	Law Enforcement	Marietta	Georgia
7	Delaware State Police (DSP)	Law Enforcement	Dover	Delaware
8	Gwinnett County Police Department	Law Enforcement	Lawrenceville	Georgia
9	Hamilton County Ohio Homeland Security (HCOHS)	Law Enforcement	Cincinnati	Ohio
10	Kansas City Police Department	Law Enforcement	Kansas	Missouri
11	Kansas City Terrorism Early Warning Group (KCTEW)	Law Enforcement	Kansas	Missouri
12	Maryland Coordination and Analysis Center (MCAC)	Law Enforcement	Baltimore	Maryland
13	Mexico City Federal District Police	Law Enforcement	Mexico City	Mexico
14	Motion Picture Association of America (MPAA)	Commercial Anti-Piracy	Encino	California
15	National Insurance Crime Bureau (NICB)	Commercial Insurance Fraud	Chicago	Illinois
16	NE Ohio Regional Fusion Center (Cleveland Area TEW)	Law Enforcement	Cleveland	Ohio
17	Nebraska State Police / Nebraska Information and Analysis Center	Law Enforcement	Lincoln	Nebraska
18	New Hampshire State Police (NHSP)	Law Enforcement	Concord	New Hampshire
19	Ohio Office Of The Attorney General (BCI)	Law Enforcement	Dublin	Ohio
20	Ohio DPS – Strategic Analysis and Information Center	Law Enforcement	Columbus	Ohio
21	Overseas Territories Regional Criminal Intelligence System (OTRCIS)	Law Enforcement	Miami	Florida
22	Pennsylvania State Police (PSP)	Law Enforcement	Harrisburg	Pennsylvania
23	Phoenix PD / Arizona Counter Terrorism Information Center	Law Enforcement	Phoenix	Arizona
24	Philadelphia Police Department	Law Enforcement	Philadelphia	Pennsylvania

25	Central California Intelligence Center	Law Enforcement	Sacramento	California
26	Michigan State Police / Michigan Intelligence Operations Center	Law Enforcement	Lansing	Michigan
27	Roanoke Area Criminal Justice Information Network	Law Enforcement	Roanoke	Virginia
28	Richmond County Police Dept. GA	Law Enforcement	Augusta	Georgia
29	Tennessee Bureau of Investigation / Fusion Center	Law Enforcement	Nashville	Tennessee
30	Farmers Insurance	Commercial Insurance Fraud	Irvine	California

10. List a least three (3) references for customers which Respondent has recently been engaged with on similar projects. Include company name, type of business, city & state. Describe high level business function delivered as part of the project.

To ensure the most effective use of the State's and our customers' time, SAS would be happy to arrange a mutually convenient time for representatives of your organization to speak with a reference customer. Please contact our Customer Reference Manager, Donna Daniels, at (919) 531-6174 or Donna.Daniels@sas.com to coordinate customer reference calls.

Company name	Pennsylvania State Police
Type of business	State police
City & State	Harrisburg, PA
High level business function delivered	COTS agency-wide intelligence management solution supporting agency's intelligence-led policing philosophy and Fusion Center operations

Company name	Michigan State Police
Type of business	State police
City & State	Lansing, MI
High level business function delivered	COTS state-wide intelligence management solution supporting agency's intelligence-led policing philosophy and Fusion Center operations

Company name	State of Nebraska
Type of business	State Information and Analysis Center
City & State	Lincoln, NE
High level business function delivered	COTS state-wide intelligence management solution supporting agency's intelligence-led policing philosophy, Fusion Center operations and regional Law Enforcement data sharing needs

11. What percentage of existing customers are in the annual support phase of the contract?
Current figures from the SAS Customer Retention team indicates that out of all customers currently using the SAS Memex Platform software, at least 96% are current on their annual support and maintenance contracts.

Contracts Disclosure form: Attachment C

The Contracts Disclosure form: Attachment C (including the conflict of interest questionnaire) is provided on the following pages in hard copy and as a separate PDF file on the CD.

* = Required fields

City of San Antonio
Contracts Disclosure Form

Office of the City Clerk

Please fill out this form online, print completed form and submit with proposal to originating department. All questions must be answered.

For details on use of this form, see Section 2-59 through 2-61 of the City's Ethics Code.

This is a ◉ New Submission or ◯ Correction or ◯ Update to previous submission.

1. Name of person submitting this disclosure form.

First: Victoria M.I. P. Last: Clayton Suffix:

2. Contract information.

a) Contract or project name: Request for Competitive Sealed Proposal No. 6100003495 (RFCSP-013-096)

b) Originating department: San Antonio Police Department

3. Name of individual(s) or entity(ies) seeking a contract with the city (i.e. parties to the contract).

SAS Institute Inc.

4. List any individual(s) or entity(ies) that is a partner, parent, joint venture, or subsidiary entity(ies) of the individual or entity listed in Question 3.

☑ Not applicable. Contracting party(ies) does not have partner, parent, joint venture, or subsidiary entities.

☐ Names of partner, parent, joint venture or subsidiary entities, and all the board members, executive committee members, and officers of each entity:

5. List any individuals or entities that will be subcontractors on this contract.

☑ Not applicable. No subcontractors will be retained for this contract.

☐ Subcontractors may be retained, but have not been selected at the time of this submission.

☐ List of subcontractors, including the name of the owner(s), and business name:

6. List any attorneys, lobbyists, or consultants retained by any individuals listed in Questions 3, 4, or 5 to assist in seeking this contract.

☑ Not applicable. No attorneys, lobbyists, or consultants have been retained to assist in seeking this contract.

☐ List of attorneys, lobbyists, or consultants retained to assist in seeking this contract:

* = Required fields

City of San Antonio
Contracts Disclosure Form

Office of the City Clerk

7. Disclosure of political contributions.

List any campaign or officeholder contributions made by the following individuals in the past 24 months totaling more than $100 to any current member of City Council, former member of City Council, any candidate for City Council, or to any political action committee that contributes to City Council elections:

a) any individual seeking contract with the city (Question 3)
b) any owner or officer of entity seeking contract with the city (Question 3)
c) any individual or owner or officer of an entity listed above as a partner, parent, or subsidiary business (Question 4)
d) any subcontractor or owner/officer of subcontracting entity retained for the contract (Question 5)
e) the spouse of any individual listed in response to (a) through (d) above
f) any attorney, lobbyist, or consultant retained to assist in seeking contract (Question 6)

☑ Not applicable. No campaign or officeholder contributions have been made in preceding 24 months by these individuals.

☐ List of contributions:

Updates on Contributions Required

Information regarding contributions must be updated by submission of a revised form from the date of the submission of this form, up through the time City Council takes action on the contract identified in response to Question 2 and continuing for 30 calendar days after the contract has been awarded.

Notice Regarding Contribution Prohibitions for "High-Profile" Contracts

Under Section 2-309 of the Municipal Campaign Finance Code, the following listed individuals 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:

a) Legal signatory of a high-profile contract
b) Any individual seeking a high-profile contract
c) Any owner or officer of an entity seeking a high-profile contract
d) The spouse of any of individual listed in response to (a) through (c) above
e) Any attorney, lobbyist, or consultant retained to assist in seeking a high-profile contract

Penalty. 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 contribution "black-out" period, which is the 10th business day after a solicitation has been released until 30 calendar days after the contract has been awarded.

8. Disclosure of conflict of interest.

Are you aware of any fact(s) with regard to this contract that would raise a "conflict of interest" issue under Sections 2-43 or 2-44 of the City Ethics Code for any City Council member or board/commission member that has not or will not be raised by these city officials?

☑ I am not aware of any conflict(s) of interest issues under Section 2-43 or 2-44 of the City Ethics Code for members of City Council or a city board/commission.

☐ I am aware of the following conflict(s) of interest:

= Required fields

City of San Antonio
Contracts Disclosure Form

Office of the City Clerk

9. Prohibited Interest in Contracts.

Currently, or within the past twelve (12) months, have you, your spouse, sibling, parent, child or other family member within the first degree of consanguinity or affinity served on a City board or commission?

Currently, or within the past twelve (12) months, has an owner, partner or employee of a business entity in which you, your spouse, parent, child own 10% or more of the voting stock or shares, or 10% or more of the fair market value served on a City board or commission?

Currently, or within the past twelve (12) months, has an owner, partner, or employee of a business entity who owns 10% or more of the voting stock or shares, or 10% or more of the fair market value, that will be a subcontractor for this contract, served on a City board or commission?

☑ No

☐ Yes

Notice Regarding Prohibited Interest in Contracts.

Please be aware, the City's Charter and Ethics Code prohibits members of certain more-than-advisory boards and commissions, as well as their close family members and any businesses they or their families hold a 10% or greater ownership interest from obtaining a contract with the City during their board or commission service. The prohibition extends to subcontracts on City contracts, and would also apply to parent, subsidiary or partner businesses owned by the member of the board or commission and their family. Please see Section 141 of the City Charter and Section 2-52 of the City Ethics Code (Prohibited Interests in Contracts) for complete information.

Former members of certain more-than-advisory boards and commissions, their family members and the businesses they own will continue to be prohibited from obtaining any discretionary contracts for one year after leaving City service. Please see Section 2-58 of the City Ethics Code (Prohibited Interest in Discretionary Contracts) for complete information.

Please note that any contract in place at the time the applicant becomes a City officer may remain in effect, but cannot be amended, extended, modified, or changed in any manner during the officer's City service on the more-than-advisory board.

If you have any questions, please contact the Office of the City Attorney to request to speak with a member of the Ethics staff: (210) 207-8940.

Acknowledgements

1. **Updates Required**

☑ I understand that this form must be updated by submission of a revised form if there is any change in the information before the discretionary contract, housing and retail development incentive, or the purchase, sale,or lease of real estate to or from the City is the subject of action by the City Council, and no later than 5 business days after any change has occurred, whichever comes first. This includes information about political contributions made after the initial submission and up until 30 calendar days after contract has been awarded.

2. **No Contact with City Officials or Staff during Contract Evaluation**

☑ I understand that a person or entity who seeks or applies for a city contract or any other person acting on behalf of that person or entity is prohibited from contacting city officials and employees regarding the contract after a Request for Proposal (RFP), Request for Qualification (RFQ), or other solicitation has been released.

This no-contact provision shall conclude when the contract is posted as a City Council agenda item. If contact is required with city officials or employees, the contact will take place in accordance with procedures incorporated into the solicitation documents. Violation of this prohibited contacts provision set out in Section 2-61 of the City Ethics Code by respondents or their agents may lead to disqualification of their offer from consideration.

= Required fields

City of San Antonio
Contracts Disclosure Form

Office of the
City Clerk

3. Contribution Prohibitions for "High-Profile" Contracts

● This is not a high-profile contract.

○ This is a high-profile contract.

4. Conflict of Interest Questionnaire (CIQ)

Chapter 176 of the Local Government Code requires all contractors and vendors to submit a Conflict of Interest Questionnaire Form (CIQ) to the Office of the City Clerk, even if contract is not designated as "High Profile".

☑ I acknowledge that I have been advised of the requirement to file a CIQ form under Chapter 176 of the Local Government Code.

***Oath**

☑ I swear or affirm that the statements contained in this Contracts Disclosure Form, including any attachments, to the best of my knowledge and belief are true, correct, and complete.

Your Name: Victoria P. Clayton LEGAL **Title:** Senior Contracts Manager

Company Name or DBA: SAS Institute Inc. **Date:** 09/23/2013

Please fill this form out online, print completed form and submit with proposal to originating department. All questions must be answered.
If necessary to mail, send to:
Purchasing
P.O. Box 839966
San Antonio, Texas 78283-3966

CONFLICT OF INTEREST QUESTIONNAIRE

FORM CIQ

For vendor or other person doing business with local governmental entity

This questionnaire reflects changes made to the law by H.B. 1491, 80th Leg., Regular Session.

This questionnaire is being filed in accordance with Chapter 176, Local Government Code by a person who has a business relationship as defined by Section 176.001(1-a) with a local governmental entity and the person meets requirements under Section 176.006(a).

By law this questionnaire must be filed with the records administrator of the local governmental entity not later than the 7th business day after the date the person becomes aware of facts that require the statement to be filed. *See* Section 176.006, Local Government Code.

A person commits an offense if the person knowingly violates Section 176.006, Local Government Code. An offense under this section is a Class C misdemeanor.

OFFICE USE ONLY

Date Received

1 **Name of person who has a business relationship with local governmental entity.**

SAS Institute Inc.

2 ☐ **Check this box if you are filing an update to a previously filed questionnaire.**

(The law requires that you file an updated completed questionnaire with the appropriate filing authority not later than the 7th business day after the date the originally filed questionnaire becomes incomplete or inaccurate.)

3 **Name of local government officer with whom filer has employment or business relationship.**

*Lisa Mendoza

Name of Officer

*Procurement Officer in connection with Request for Competitive Sealed Proposal 6100003495 (RFCSP-013-096)

This section (item 3 including subparts A, B, C & D) must be completed for each officer with whom the filer has an employment or other business relationship as defined by Section 176.001(1-a), Local Government Code. Attach additional pages to this Form CIQ as necessary.

A. Is the local government officer named in this section receiving or likely to receive taxable income, other than investment income, from the filer of the questionnaire?

☐ Yes ☒ No

B. Is the filer of the questionnaire receiving or likely to receive taxable income, other than investment income, from or at the direction of the local government officer named in this section AND the taxable income is not received from the local governmental entity?

☐ Yes ☒ No

C. Is the filer of this questionnaire employed by a corporation or other business entity with respect to which the local government officer serves as an officer or director, or holds an ownership of 10 percent or more?

☐ Yes ☒ No

D. Describe each employment or business relationship with the local government officer named in this section.

4 ** On behalf of SAS Institute Inc.

**Signature of person doing business with the governmental entity
Victoria P. Clayton, Senior Contracts Manager

LEGAL

September 23, 2013

Date

Adopted 06/29/2007

Litigation Disclosure: Attachment D

Litigation Disclosure: Attachment D is provided on the following pages in hard copy and as a separate PDF file on the CD.

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 X*

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 X*

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 X*

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.

*SAS' responses to these questions are made based on commercially reasonable investigation of those individuals currently anticipated to work on any resulting contract with the City. Personnel ultimately delivering any services to the City may change and SAS will notify the City of any subsequent change to such representations. SAS Institute Inc. makes only those second ar third representations.

SBEDA Form: Attachment E

The SBEDA Form: Attachment E is provided on the following pages in hard copy and as a separate PDF file on the CD.

CITY OF SAN ANTONIO
SUBCONTRACTOR/SUPPLIER UTILIZATION PLAN

SOLICITATION NAME: ***Intelligence Management Solution for SAPD/Southwest Texas Fusion Center***

RESPONDENT NAME: SAS Institute Inc.

SOLICITATION API: ***Emerging Small Business Enterprise (ESBE) Prime Contract AND Small Business Enterprise (SBE) Prime Contract Programs***

API REQUIREMENTS: In order to receive the **ten (10)** evaluation preference points associated with the ESBE Prime Contract program and/or **ten (10)** evaluation preference points associated with the SBE Prime Contract program on this solicitation, ESBE and SBE Prime Respondents must document on this form that at least 51% of this contract shall be self-performed or shall be subcontracted to other certified Emerging Small Business Enterprises and/or Small Business Enterprises with a Significant Business Presence within the San Antonio Metropolitan Statistical Area.

ESBEs and/or SBEs must be certified with the South Central Texas Regional Certification Agency and be headquartered or have Significant Business Presence in the San Antonio Metropolitan Statistical Area to receive preference points. For further clarification, please contact Catherine Olukotun at (210) 207-8088.

Section 1. Enter Respondent's (Prime) proposed contract participation level. Leave blank for revenue generating contracts.

Section 2. List ALL subcontractors / suppliers that will be utilized for the entire contract period, excluding possible extensions, renewals and/or alternates. Use additional sheets if necessary.

	PARTICIPATION DOLLAR AMOUNT	% LEVEL OF PARTICIPATION	CERTIFICATION TYPE AND NUMBER	TYPE OF WORK TO BE PERFORMED (BY NIGP CODE)
SECTION 1. PRIME				
Name: SAS Institute Inc.	$	100%	#:	
SECTION 2. SUBCONTRACTOR(s):				
1.Name:	$	%	#:	
2. Name:	$	%	#:	
3. Name:	$	%	#:	
4. Name:	$	%	#:	
5. Name:	$	%	#:	
6. Name:	$	%	#:	
Total Prime Participation:	$	%	#:	
Total Sub Participation:	$	%	#:	
Total Prime & Sub Participation*:	$	%	#:	
Total Certified Sub Participation:	$	%	#:	

Total Prime & Sub participation must equal your base bid amount.

If a business is not certified, please call the Small Business Program Office at (210) 207-3900 for information and details on how subcontractors and suppliers may obtain certification.

I HEREBY AFFIRM THAT I POSSESS DOCUMENTATION FROM ALL PROPOSED SUBCONTRACTORS/SUPPLIERS CONFIRMING THEIR INTENT TO PERFORM THE SCOPE OF WORK FOR THE PRICE INDICATED ABOVE. I FURTHER AFFIRM THAT THE ABOVE INFORMATION IS TRUE AND COMPLETE TO THE BEST OF MY KNOWLEDGE AND BELIEF. I UNDERSTAND AND AGREE THAT, IF AWARDED THE CONTRACT, THIS DOCUMENT SHALL BE ATTACHED THERETO AND BECOME A BINDING PART OF THE CONTRACT.

SIGNATURE OF AUTHORIZED AGENT

Victoria P. Clayton
Senior Contracts Manager

LEGAL

TITLE

September 25, 2013

DATE

(919) 677-8000

PHONE

****

FOR CITY USE

Action Taken: **Approved**_____ **Denied**_____

DIRECTOR
ECONOMIC DEVELOPMENT

Pricing Schedule: Attachment F

The Pricing Schedule: Attachment F is provided on the following pages in hard copy and as a separate PDF file on the CD.

ATTACHMENT F - City Hosted Solution Cost Detail

er all one-time, re-occuring and ala carte costs that are associated with proposed solution. Repondent only needs to complete items that apply to proposed solution. If there no costs associated with those listed below, enter a value of 0. If costs are based on a named user or concurrent user fee, indicate it in the notes column. If concurrent user cate the ratio. i.e. 1 concurrent user = 10 users.

	Occurrence (1)	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5	Notes
TING COST (If Vendor hosted Solution)							
TWARE LICENSE AND FEES WITH ONE R WARRANTY	One-Time	103,590					SAS Fusion Center Solution includes: Fourteen (14) named user license Includes the following modules: • Request for Service (RFS) Module • Intelligence Management Module Suspicious Activity Reporting (SARS) module (10 named user license) Confidential Informant Management Module (8 named user license)
FESSIONAL SERVICES							
ROJECT EXECUTION PLANNING	One-Time	10,540					
ONFIGURATION	One-Time	6,080					
NTERFACES	One-Time	75,410					
ESTING	One-Time	16,840					
RAINING	One-Time	37,240					
UAL MAINTENANCE & SUPPORT	Annual	included	included	23,793	24,983	26,232	
AL COSTS	**-**	**249,700**	**-**	**23,793**	**24,983**	**26,232**	

er/Growth Costs	Occurrence (1)	Cost	M&S (3)	Notes

TES:

- One-Time, Monthly, Bi-Monthly, Qrtrly, etc
- Field device monitoring, management reporting, AVL tracking/reports, ??
- Maintenance & Support costs asosciated with addition of software licenses, hardware components and/or optional features.
- List any additional features that may be considered with solution yet not requested.
- Include any additional costs for growth in hardware, software components.

Functional Requirements: Attachment G

The Functional Requirements: Attachment G is provided on the following pages in hard copy and as a separate PDF file on the CD.

Respondent must enter a valid response under column labeled "Vendor Response" and any applicable comment. Reference legend below matrix for vendor response options. Respondent must submit this file in native unprotected excel format along with hardcopy version.

No.	Requirement	Priority Mandatory=	Vendor Response	Comments
1	**General**			
1.1	Single platform that includes functionality for suspicious activity reporting, service request			
	management, intelligence management and confidential informant management	M	Y	
1.2	Multi-level security user groups	M	Y	
1.3	Security and audit capability	M	Y	
1.4	Customizable data entry forms	M	Y	
1.5	Document indexing and archiving	M	Y	
1.6	Single sign-on	M	Y	
1.7	Supports active directory authentication	D	Y	
1.8	Deployable via thin client, i.e., web browser	D	Y	
1.9	Supports duplication of data to MS SQL environment	D	Y	
1.10	Currently deployed and operational in Major City Intelligence Unit or recognized Fusion Center	M	Y	
2	**Suspicious Activity Reporting (SAR) Functionality**			
2.1	Software must be compliant and integrate with the National SAR Initiative (NSI)	D	Y	
2.2	Software must have ability to interface with NSI Shared Space and/or eGuardian	D	Y	
2.3	Software must have capability to interface with ESRI GIS platform	M	Y	
2.4	Currently deployed and operational in Major City Intelligence Unit or recognized Fusion Center	M	Y	
3	**Service Request Functionality**			
3.1	Records, manages, and monitors service calls	M	Y	
3.2	Provides performance metrics at organizational and individual levels	M	Y	
3.3	Currently deployed and operational in Major City Intelligence Unit or recognized Fusion Center	M	Y	
4	**Intelligence Management Functionality**			
4.1	Supports 28 CFR Part 23 compliance	M	Y	
4.2	Single federated search capability	M	Y	
4.3	Real time electronic alerts and notifications	D	Y	
4.4	Supports customization of data entry and input	M	Y	
4.5	Supports multiple level review and approval process	M	Y	
4.6	Currently deployed and operational in Major City Intelligence Unit or recognized Fusion Center	M	Y	
5	**Confidential Informant Management Function**			

5.1	Supports the vetting, approval, and handling of registered informants	M	Y	
5.2	Single federated search with anonymous pointer	M	Y	
5.3	Supports deconfliction process	D	Y	
5.4	Informant interaction tracking and payment audit process	M	Y	
5.5	Supports ESRI GIS tracking/mapping	D	Y	
5.6	Currently deployed and operational in Major City Intelligence Unit or recognized Fusion Center	M	Y	

(1) - Vendor Response Legend

Y	Functionality is resident in the software solution, neither configuration nor customization is required Requested information has been submitted within proposal.
C	Functionality is not currently resident but vendor is willing to provide functionality by configuration (not custom development)
C$	Functionality is not currently resident but vendor is willing to provide functionality by configuration (not custom development) at a cost to the client. Respondent must provide cost details within proposal section.
D	Functionality is not currently resident but vendor is willing to provide fnctionality by additional custom development.
D$	Functionality is not currently resident but vendor is willing to provide functionality by additional custom development at a cost to the client. Respondent must provide cost details within proposal section.
N	Functionality is not resident in the software solution and vendor is not willing to provide this functionality.

Signature Page: Attachment H

The Signature Page: Attachment H is provided on the following pages in hard copy and as a separate PDF file on the CD.

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/.

By submitting a proposal, whether electronically or by paper, 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 will be able and willing to comply with the insurance and indemnification requirements set out in RFCSP Exhibits 1 & 2.

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.

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.

SAS Institute Inc.
Respondent Entity Name

*Signature: _____

Printed Name: Victoria P. Clayton

Title: Senior Contracts Manager

*SAS Institute Inc.'s signature hereto does not indicate acceptance of the terms and conditions included in the RFP, and any resulting contract with the City of San Antonio will be subject to mutual agreement by the parties.

LBF LEGAL

(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.)

If submitting your proposal electronically, through City's portal, Co-Respondent must also log in using Co-Respondent's log-on ID and password, and submit a letter indicating that Co-Respondent is a party to Respondent's proposal and agrees to these representations and those made in Respondent's proposal. While Co-Respondent does not have to submit a copy of Respondent's proposal, Co-Respondent should answer any questions or provide any information directed specifically to Co-Respondent.

_____
Co-Respondent Entity Name

Signature: _____

Printed Name: _____

Title: _____

Proposal Checklist: Attachment I

The Proposal Checklist: Attachment I is provided on the following pages in hard copy and as a separate PDF file on the CD.

RFCSP ATTACHMENT I

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	LD
Proposal RFCSP Attachment A	LD
Respondent Questionnaire RFCSP Attachment B	LD
*Contracts Disclosure form RFCSP Attachment C	LD
Litigation Disclosure RFCSP Attachment D	LD
*SBEDA Form RFCSP Attachment E; and Associated Certificates, if applicable	LD
Pricing Schedule RFCSP Attachment F	LD
Functional Requirements RFCSP Attachment G	LD
*Signature Page RFCSP Attachment H	LD
Proposal Checklist RFCSP Attachment I	LD
Proof of Insurability (See RFCSP Exhibit 1) Insurance Provider's Letter Copy of Current Certificate of Insurance	LD
Financial Information	LD → Separate Mailing
One (1) Original, ten copies, and one (1) CD of entire proposal in PDF format if submitting in hard copy.	LD

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

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.

A copy of SAS' current certificates of insurance is provided on the following pages in hard copy and as a separate PDF file on the CD. SAS looks forward to negotiating an acceptable form of contract with the City and as part of such negotiation, will work with the City to put in place mutually agreeable insurance coverage for the types of services described in this response.

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY) 04/29/2013

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Aon Risk Services South, Inc.
Atlanta GA Office
3565 Piedmont Rd NE,Blg1,#700
Atlanta GA 30305 USA

CONTACT NAME:
PHONE (A/C. No. Ext): (866) 283-7122 FAX (A/C. No.): 800-363-0105
E-MAIL ADDRESS:

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A:	Lloyd's Syndicate No. 2623	AA1128623
INSURER B:	Zurich American Ins Co	16535
INSURER C:		
INSURER D:		
INSURER E:		
INSURER F:		

INSURED
SAS Institute Inc.
SAS Campus Dr.
Cary NC 27513 USA

COVERAGES **CERTIFICATE NUMBER:** 570049746674 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS. Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	GENERAL LIABILITY						EACH OCCURRENCE	
	COMMERCIAL GENERAL LIABILITY						DAMAGE TO RENTED PREMISES (Ea occurrence)	
	CLAIMS-MADE OCCUR						MED EXP (Any one person)	
							PERSONAL & ADV INJURY	
							GENERAL AGGREGATE	
	GEN'L AGGREGATE LIMIT APPLIES PER: POLICY PRO-JECT LOC						PRODUCTS - COMP/OP AGG	
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	
	ANY AUTO						BODILY INJURY (Per person)	
	ALL OWNED AUTOS / SCHEDULED AUTOS						BODILY INJURY (Per accident)	
	HIRED AUTOS / NON-OWNED AUTOS						PROPERTY DAMAGE (Per accident)	
	UMBRELLA LIAB / OCCUR						EACH OCCURRENCE	
	EXCESS LIAB / CLAIMS-MADE						AGGREGATE	
	DED / RETENTION							
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY						WC STATU-TORY LIMITS / OTH-ER	
	ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? Y / N (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N / A					E.L. EACH ACCIDENT	
							E.L. DISEASE-EA EMPLOYEE	
							E.L. DISEASE-POLICY LIMIT	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)

CERTIFICATE HOLDER

SAS Institute Inc
SAS Campus Drive
Cary NC 27513 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Services South Inc

©1988-2010 ACORD CORPORATION. All rights reserved.

The ACORD name and logo are registered marks of ACORD

Holder Identifier : Errors_1 mil
Certificate No : 570049746674

AGENCY CUSTOMER ID: 220000000026
LOC #:

ADDITIONAL REMARKS SCHEDULE

AGENCY	NAMED INSURED
Aon Risk Services South, Inc.	SAS Institute Inc.
POLICY NUMBER: See Certificate Number: 570049746674	
CARRIER: See Certificate Number: 570049746674 — NAIC CODE:	EFFECTIVE DATE:

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,
FORM NUMBER: ACORD 25 FORM TITLE: Certificate of Liability Insurance

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER	
INSURER	
INSURER	
INSURER	

ADDITIONAL POLICIES If a policy below does not include limit information, refer to the corresponding policy on the ACORD certificate form for policy limits.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFFECTIVE DATE (MM/DD/YYYY)	POLICY EXPIRATION DATE (MM/DD/YYYY)	LIMITS	
	OTHER							
A	E&O-MPL-Primary			QK1302121 E&O / Prof Liab	04/01/2013	04/01/2014	Each Occurrence	$1,000,000
							Aggregate	$1,000,000

© 2008 ACORD CORPORATION. All rights reserved.
The ACORD name and logo are registered marks of ACORD

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY) 04/01/2013

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Aon Risk Services South, Inc.
Atlanta GA Office
3565 Piedmont Rd NE,Blg1,#700
Atlanta GA 30305 USA

CONTACT NAME:
PHONE (A/C. No. Ext): (866) 283-7122 FAX (A/C. No.): (847) 953-5390
E-MAIL ADDRESS:

INSURED
SAS Institute Inc.
SAS Campus Drive
Cary NC 27513 USA

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A:	Travelers Property Cas Co of America	25674
INSURER B:	Phoenix Ins Co	25623
INSURER C:	The Travelers Indemnity Co.	25658
INSURER D:		
INSURER E:		
INSURER F:		

COVERAGES CERTIFICATE NUMBER: 570049466309 REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS. Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	GENERAL LIABILITY X COMMERCIAL GENERAL LIABILITY CLAIMS-MADE X OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: X POLICY PRO-JECT LOC			HJGLSA5510P91413	04/01/2013	04/01/2014	EACH OCCURRENCE	$1,000,000
							DAMAGE TO RENTED PREMISES (Ea occurrence)	$1,000,000
							MED EXP (Any one person)	$10,000
							PERSONAL & ADV INJURY	$1,000,000
							GENERAL AGGREGATE	$2,000,000
							PRODUCTS - COMP/OP AGG	$2,000,000
A	AUTOMOBILE LIABILITY X ANY AUTO ALL OWNED AUTOS SCHEDULED AUTOS HIRED AUTOS NON-OWNED AUTOS			HJ-CAP-117D7878-13	04/01/2013	04/01/2014	COMBINED SINGLE LIMIT (Ea accident)	$1,000,000
							BODILY INJURY (Per person)	
							BODILY INJURY (Per accident)	
							PROPERTY DAMAGE (Per accident)	
A	X UMBRELLA LIAB X OCCUR EXCESS LIAB CLAIMS-MADE DED X RETENTION $10,000			HSMJCUP162D870113 SIR applies per policy terms & conditions	04/01/2013	04/01/2014	EACH OCCURRENCE	$5,000,000
							AGGREGATE	$5,000,000
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? Y/N N (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A		TC2NUB487D874413 AOS	04/01/2013	04/01/2014	X WC STATU-TORY LIMITS OTH-ER	
C				TRKUB487D876813 AZ, MA, OR, WI	04/01/2013	04/01/2014	E.L. EACH ACCIDENT	$1,000,000
							E.L. DISEASE-EA EMPLOYEE	$1,000,000
							E.L. DISEASE-POLICY LIMIT	$1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)

Physical Damage Limit $2,500 per occurrence / $50,000 aggregate / with $1,000 Comprehensive and $1,000 Collision deductibles. "The General Liability Policy certified above, is written under The St. Paul Travelers Companies form number CG D4 17 07 08, which includes the following language: Any organization that the named insured agrees in a written contract to add as an additional protected person under this agreement is a protected person, but only for covered bodily injury or property damage that results from the named insureds work."

CERTIFICATE HOLDER

SAS Institute Inc.
SAS Campus Drive
Cary, NC 27513 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Services South Inc.

Holder Identifier : sas5403

Certificate No : 570049466309

©1988-2010 ACORD CORPORATION. All rights reserved.

The ACORD name and logo are registered marks of ACORD

Financial Information

Submit a recent copy of a Dun and Bradstreet financial report, or other credit report, on Respondent and its partners, affiliates and subtenants, if any.
SAS has the necessary financial resources to meet the performance requirements of this contract. SAS has maintained its unbroken chain of growth and profitability since the company was founded over 37 years ago. SAS' worldwide annual revenue was $2.87 billion in 2012 and has topped $1 billion for each of the last 14 years. Our consistent growth and profitability mean you can depend on SAS, not only today, but into the future as well.

Dun and Bradstreet financial reports are copyrighted and SAPD must request this report directly from D&B. SAS' DUNS Number is 04-004-6724. Alternatively SAS can provide you with financial information that is comparable to the data we provide to D&B each year. SAS policies require that Finance provide this data directly to government customers as we do not release this information to our internal employees outside of Finance. This information has been mailed separately directly to SAPD. This data is intended solely for your use in considering our RFCSP response.

Appendix A: Resumes

Steve Serrao, Advisory Industry Consultant

Education

- Thomas Edison State College, Trenton, New Jersey
- Pursuing Bachelor of Science Degree (Completed Approx. 106 Credits towards BS)
- New Jersey State Police Academy, Sea Girt, N.J.
- Certified Police Officer Training, Graduated April 3, 1981

Role/Responsibility for this Contract

- Steve will serve as the Subject Matter Expert (SME) for this project. Working with the different user populations to ensure that the system configuration and any data migration/integrations meet the needs of the DPS.

Experience

- Advisory Industry Consultant For Law Enforcement Solutions, SAS Institute Inc. Memex Solutions Team, May 2, 2006 to the present
  - Kansas City Regional Terrorism Early Warning Group
  - Philadelphia Police Department – Intelligence Division
  - Los Angeles Regional Intelligence Center
  - Northern California Regional Intelligence Center
  - Central California Regional Intelligence Center
  - Roanoke Area Criminal Justice Information Network
  - Mountain Empire Criminal Justice Information Network
  - Pennsylvania Criminal Intelligence Center
  - Michigan Criminal Information System
  - Ohio Department of Public Safety
  - Nebraska Information Analysis Center
  - Arizona Counter Terrorism Information Center
  - Philadelphia Police Department – Integrity Control Office
  - Bermuda Police Force
  - Belize National Police Department
  - Jamaica Constabulary Force
  - Mexico City Federal District Police

  Captain - Bureau Chief, New Jersey State Police, West Trenton, New Jersey, April 3, 1981 to May 1, 2006

Dale Peet, Senior Industry Consultant

Education

- Bachelors of Science, Business Management, University of Phoenix
- Certificate, Northwestern University School of Police Staff and Command
- FBI National Academy Graduate 222

Experience

- SAS Institute Inc. - Memex Solutions Team
- Senior Industry Consultant – 2 years, 11 months
  - Nebraska Information Analysis Center (NIAC)
  - Arizona Counter Terrorism Information Center (ACTIC)
  - Michigan Criminal Information System (MCIS)
  - Georgia Terrorism Intelligence Project (GTIP)
  - Northeast Ohio Regional Fusion Center (NEORFC)

- Michigan State Police – 23 years, Retired
  - Detective First Lieutenant
  - Fusion Center Commander, Michigan Intelligence Operations Center
  - MIOC IT Project Manager
  - RMS Unit Commander
  - Battle Creek Post Commander
  - Wayland Post Commander
  - Southwest Enforcement Team Leader
  - Battle Creek Post Detective
  - Tobacco Tax Team Detective
  - New Buffalo Post - Trooper

Graeme Robinson, Director of Professional Services

Education

- Bachelor of Science (with Honors) in Computer Science - The University of Strathclyde in Glasgow, Scotland

Experience

- SAS Institute Inc. - Memex Solutions Team
- Director of Professional Services – 12 years
  - Nebraska Information Analysis Center (NIAC)
  - Michigan Criminal Information System (MCIS)
  - Northeast Ohio Regional Fusion Center (NEORFC)
  - Ohio Department of Public Safety
  - Kansas City Terrorism Early Warning Group
  - Maryland State Police
  - State of Delaware
  - Philadelphia Police Department (PPD)
  - Northern California Regional Intelligence Center
  - Central California Regional Intelligence Center
  - National Insurance Crime Bureau
  - Roanoke Area Criminal Justice Information Network

Kyle Evers, Senior Technical Consultant

Education

- Bachelors of Science in Informatics – Indiana University
- Certificate of Applied Computer Science – Purdue University
- Certificate of Sound Engineering & Music Production – RECW
- Successful Project Management – PMI (Project Management Institute)
- Developing Business Processes and Integration Solutions Using MS BizTalk Server 2006

Experience

- SAS Institute Inc. - Memex Solutions Team
- Senior Technical Consultant – 3 years, 5 months
  - Kansas City Regional Terrorism Early Warning Group
  - Nebraska Information Analysis Center
  - Arizona Counter Terrorism Information Center
  - Pennsylvania Criminal Intelligence Center
  - Ohio Department of Public Safety
  - Michigan Criminal Information System
  - Philadelphia Police Department – Integrity Control Office

- Molina Healthcare, Programmer Analyst

- Perot Systems Government Service (PSGS), Application Developer / Analyst

Technical Expertise

Hardware	IBM, SUN, Compaq/HP, Dell servers and components
Software	Visual Studio.NET, Enterprise Manager, SQL Query Analyzer, MS SharePoint, Visual SourceSafe, MS SQL Server Management Studio, Eclipse, NetBeans, Subversion, and TextPad
Databases	MS SQL, Oracle, MySQL, MS Access
Programming Languages	NET Framework v2.0/v3.0/v3.5, WWF, WCF, ASP.NET, C#, JAVA (EE, SE, ME), JavaScript, AJAX, XML, VB.NET, BizTalk, PHP, SQL, HTML, and Action script
Operating systems/environments	Windows 3.x/95/98/2000/NT/XP/7, Linux/Unix, Mac

Libby Stengel, Senior Implementation Project Manager / Consultant

Education

- BS in Psychology, Minor in Military Science – South Dakota State University
- Certified Emergency Medical Technician – Basic
- United States Army Military Intelligence Officer Basic Course

Experience

- SAS Institute Inc. - Memex Solutions Team
- Project Manager, Consultant and Trainer – 5 years, 10 months
  - Kansas City Regional Terrorism Early Warning Group
  - Nebraska Information Analysis Center
  - Roanoke Area Criminal Justice Information Network
  - Trinidad and Tobago Police Intelligence
  - Arizona Counter Terrorism Information Center
  - Suriname Federal Police Intelligence
  - Northern California Regional Intelligence Center
  - Central California Regional Intelligence Center
  - Pennsylvania Criminal Intelligence Center
  - Bermuda Police Force
  - National Insurance Crime Bureau
  - Iraqi Ministry of Interior
  - Mountain Empire Criminal Justice Information Network

- United States Army Military Intelligence Officer – 4 years
  - Iraqi Criminal Intelligence Trainer
  - Logistics, Budget and Maintenance Officer
  - Company Executive Officer
  - Intelligence Analyst Team Leader, Intelligence Fusion Center

Ranga Gopal, Principal Technical Architect

Education

- Masters of Information Systems - Australian Catholic University, Sydney, Australia
- Bachelors of Business Administration - Annamalai University, India
- Microsoft Certified Professional

Role/Responsibility for this Contract

- Confidential Informant Management Solution Implementation

Experience

- SAS Institute Inc. - Memex Solutions Team
- Principal Technical Architect – 3 years, 7 Months
  - Michigan Criminal Information System
  - Nebraska Information Analysis Center
  - Philadelphia Police Department – Integrity Control Office
  - Maryland Coordination and Analysis Center
  - Delaware Information and Analysis Center

- Information Systems of Florida, Senior Technical Lead / Project Manager – 3 Years

- NCR Corporation, USA, Component Team Leader, Financial Solution Division (FSD) – 1 year

- NCR Australia Pty Ltd, Australia, Business Systems Support Specialist II, Worldwide Customer Services (WCS) – 6 years

- Lityan Holdings, Malaysia, Lead Technical Consultant, E-commerce Division – 1 year

- Angler Web Services, India, Senior Developer, E-commerce Division – 2 years

Technical Expertise

Operating systems	Windows 200x, UNIX, Vista, Windows 95/98/XP, LINUX, Solaris
Databases	MS SQL Server, MS-Access, Oracle, Mysql, Postgresql
Programing Languages	.NET, Perl, PHP, JAVA
Web Servers	IIS, Apache, JBoss
Security Toolset	IBM Appscan, Qualys PCI, Acunetix Web Vulnerability Scanner
Data Integration Platform	Microsoft SQL Server Integration Services, SAS Data Integration Studio

Colin Paterson, Principal Technical Architect

Role/Responsibility for this Contract

- Memex Platform Installation – MSSQL Serve Integration.

Experience

- SAS Institute Inc. - Memex Solutions Team
- Senior Software Engineer, Project Manager, Head of Research & Development, Senior Solution Manager Principal Technical Architect – 13 years, 2 months
  - Tennessee Bureau of Investigation
  - Michigan Criminal Information System
  - New Jersey State Police
  - Pennsylvania State Police
  - Los Angeles Joint Regional Intelligence Center
  - London Metropolitan Police Service
  - Surrey Police Force
  - Bermuda Police Service
  - British Transport Police
  - Her Majesty's Prison Service
  - Durham Police Force
  - Nottinghamshire Police Force

Technical Expertise

Hardware	SUN, Compaq/HP, Dell Servers
Software	Visual Studio 2002 - 2012, Full Microsoft Office Suite, Microsoft Sql Server Management Studio, Oracle Sql Developer, Esri Arcgis Desktop & Server, Subversion Source Control Management, Cruise Control.
Databases	MS SQL Server, Oracle, MySQL, MS Access, PostgreSQL, Informix, Firebird, FoxPro.
Programming Languages	NET Framework v2.0/v3.0/v3.5/v4.0, WCF, ASP.NET, C, C++, C#, JAVA, JavaScript, XML, VB.NET, VB6, SQL, PERL, HTML, TCL
Operating Systems/Environments	Windows 3.x/95/98/2000/NT/XP/7, Windows Server 2003, 2008, CentOS 5/6, Sun Solaris 8/9/10, Red Hat Enterprise Linux 4/5/6, Apple iOS, Symbian