CITY OF FONTANA, C A L I F O R N I A

REQUEST FOR PROPOSAL

FOR

Security Management System Platform

SP-38-IT-12

SUBMISSION DEADLINE

5/1/2012

BY 2:00PM

PROPOSAL MUST BE SUBMITTED ELECTRONICALLY
Hard Copies will NOT be accepted as a viable proposal

TABLE OF CONTENTS

1 SCOPE

1.1 INTRODUCTION

The City of Fontana wishes to procure and implement a software platform that will integrate the current and future security systems and devices in all city owned and operated facilities. Ultimately, it is the City's responsibility to provide a safe and secure environment for city staff, citizens, and property for all City owned and operated facilities. Having a set of standards and specifications that are used for all future construction, these technologies can be designed into City facilities instead of added on after the fact, which is always more costly. Tying all of the systems together through a central Security Management System (SMS) will provide the capability to effectively provide the necessary security for staff and citizens.

1.2 BACKGROUND

The City of Fontana has over 30 facilities scattered over 40 square miles in western San Bernardino County, California. It serves a population approaching 200,000 with a full service city of around 1000 full and part time employees. The security systems put into these facilities range from simple keyed door locks to electronic access control devices (Bosch ReadyKey), intrusion protection (Bosch alarms), and video surveillance (Bosch DVRs, OnSSI). Identity Management is primarily through Microsoft Active Directory. The purpose of this RFP is to establish a security platform standard to which all future security systems and devices will connect and which can be easily retrofitted in the older facilities. One of the intended outcomes of this project is to finalize the City's Security Master Plan and establish the standards for all future security related devices and technologies. Following is an excerpt from the executive summary of that Plan:

1.2.1 Security Systems

The evolution of technology surrounding security systems (alarms, door locks, video surveillance) has changed the framework for building design. Construction of new buildings has typically been completely in the purview of the construction trades and within the City fell to the Development Services Organization and the skills and disciplines in the various departments: Planning, Engineering, Building & Safety and Public Works (Facilities). The rapid and accelerating growth of technology has added another element to building design that is often misunderstood or overlooked by architects in the initial design phase and this resulted in the injection of technology around a buildings infrastructure instead of being design into it.

Realizing that technology is an integral part of building design, Information

Technology experts are now being called in during the initial stages of planning a building or a campus so that computer cabling, data closets, HVAC and power requirements can be provided where computers are needed. In recent years, this accelerating change in technology has entered into the area of security as well.

Managing keyed doorlocks in a City with over 30 different facilities, 1000 part time and full time employees is labor intensive at best and only marginally secure. With either high growth as the City has experienced in recent years or just normal staff turnover, using coded keypad locks become a problem as well.

Intrusion alarms are successful only if police can quickly respond to all incidents, which is logistically impossible in a city that occupies over 30 square miles. Remote video surveillance will only work if there is someone to monitor the cameras 24/7. With the City's recently adopted policy of "Verified Response," without a visual verification of a crime in progress, this becomes even more critical.

Recent advance in technology have made it possible and even financially feasible to integrate access control (doorlocks), alarms, and video surveillance and tie them to the City's informational databases for identity verification. New technologies in biometrics are making it possible to positively identify who is or is not an employee and access can be granted or denied to new or terminated employees in a matter of minutes.

These facts and circumstances resulted in the creation of a Video/Security Summit in early November 2008. Representatives from Public Works, Engineering, Traffic, Planning, Building & Safety, and Information Technology met to discuss these issues and the development of security standards for the city that would integrate these new technologies into future building projects and enable retrofitting them into existing structures.

1.2.2 Objectives

A. Develop a Fontana Security Master Plan to define a strategy for securing all City facilities;

B. Develop standards and specifications for inclusion in future building projects for:

   1. Access Control (building access as well as digital infrastructure)
   2. Alarm Systems
   3. Video surveillance
   4. Data and Document Protection

C. Define the unique requirements for the different types of facilities including:

1. City office buildings
2. Parks facilities
3. Community Centers
4. Police facilities
5. Fire facilities
6. Computer Networks

1.2.3 Overview

The City will have a Security Strategy that will employ integrated technologies to cost-effectively integrate access to city facilities with active employee database information to ensure that appropriate people will have access to appropriate facility areas. This will include identity management systems to ensure the system has positive ID on persons needing access as well as their current status in relationship to the City.

In concept, security starts with employees (Identity Management) and ends with citizen safety and security (Video Surveillance). As soon as someone begins the application process to become a Fontana employee, the process begins:

Process	Primary responsibility	Process Description
Employment Application	HR	Vet the application, check references, corroborate application data.
Job offer	Dept Head	Match skills to job requirements
Hiring	HR, PD	Complete employment papers, background check.
Badge issuance	HR	Photo ID in AD database, Fingerprint in AD database, name/photo/badge coordination
Work assignment(s)	Dept Head	Determine what facilities and what systems access are required.
Access permissions (facilities)	Dept Head, PW	Determine what keys and room or building access is required.

Process	Primary responsibility	Process Description
Access permissions (technology)	Dept Head, IT	Update AD group policy memberships for the Access Control system (badge/door keypad pin), network access, and whatever systems are necessary for the work assignments.

Of course, in order for these processes to work, the security profiles for facilities, networks, systems, and databases must be set up. In the City of Fontana, there are over 30 facilities and over 50 different computer systems. Each department has requirements to access some or all of these different facilities and computer systems and it is up to the Department Heads to determine who will be the custodian for each. In a cooperative effort, the IT Department will work with Department Heads and the Application Leads (the computer system "power users" for the applications used by that department). Based on position title and attributes, employees are added to the AD database and specific group memberships associated with the department and the specific position they hold. In addition, there are several City-wide (Enterprise) applications to which employees may require access such as email, Document Management, and Internet access. A chart showing how these various aspects are handled is as follows:

Security Area	Primary responsibility	Process Description
Facility Access	Dept Head, IT NW Admin	Set up position group access definitions to be used by ReadyKey for each facility.
Facilities FF&E	Public Works, IT NW Admin	Installation and maintenance of security devices including door keypads, alarms, alarm panels and controls, video cameras. Power and low voltage cabling.
Network/Enterprise Access	NW Admin	Set up standard employee network access for enterprise applications and specific groups for special classes (e.g. Department Head)

Security Area	Primary responsibility	Process Description
Application/Database Access	Dept App Lead, IT App Analyst	Many applications have their own security layer that may or may not be coordinated through Active Directory. Most require set up to be for a specific individual rather than position. Workflow rules must also be setup in similar fashion for those applications using a workflow engine.

Many applications have their own security layer that may or may not be coordinated through Active Directory. Most require set up to be for a specific individual rather than position. Workflow rules must also be setup in similar fashion for those applications using a workflow engine.

Intrusion protection will integrate alarms with video surveillance so that all City facilities can be protected remotely with a minimum of staff. This will also include monitoring and video data storage policies appropriate to each type of facility. All facility security technologies will be connected via the City's fiber I-Net system that is separate from other data and voice networks, but with the same redundancy and backup systems in place.

The use of other video technologies for broadcast of meetings on KFON and/or the Internet will be used to make government more accessible to the citizens and facilitate dialog between and among vendors and City staff more cost effectively.

1.3 COMPUTING ENVIRONMENT

The proposed system will be a premise based system residing in the City's current network/server environment located on the City Hall campus in the City of Fontana. This section outlines a high level overview of that environment and the technical standards to which the successful vendor must conform.

The City's network infrastructure consists of several buildings within the city limits. The network equipment in use is either Cisco or Foundry/Brocade, with the majority being Cisco. All buildings on the main campus are connected via multi-mode fiber optic cabling, while buildings outside of the immediate campus area are connected via either single-mode fiber optic cabling or point-to-point leased lines.

The City's server infrastructure consists of two data centers, each in a different building on the same campus. The first data center is in the Police Department building. The second data center is in the Lewis Library and Technology Center. Server hardware is all Hewlett Packard. The main server platform is a HP BladeSystem c7000 chassis, one in each data center, populated with HP ProLiant DL460c G1 blades running VMware vSphere 4. With the exception of two hosts with 64GB of RAM, each host contains two quad-core processors and 32GB of RAM. The Police Department data center has six blades and the Library data center has nine blades. Traditional servers, also various HP ProLiant models, are still in use in both data centers to support legacy applications or unique hardware requirements.

Storage for the servers consists of a XIOtech Emprise 7000 array connected to a 4Gbps fiber channel SAN network. The SAN consists of two switched fabrics with two fiber channel switches per fabric. Both fabrics are available in both data centers. Other disk array systems exist on the SAN supporting specific applications.

The City's database infrastructure is built on Microsoft SQL Server. The current database engines supported by the City's Information Technology department are a 2-node cluster running SQL Server 2005 Enterprise Edition, 64-bit, and a single virtualized server SQL Server 2008 Enterprise Edition, 64-bit. The database environment is consolidated so as to reduce cost and management overhead.

2 INSTRUCTIONS TO PROPOSERS

2.1 PROPOSAL TIMELIME

RELEASE DATE: 3/27/2012
CLOSING DATE: 5/1/2012

2.2 PROPOSER'S EXAMINATION

Before submitting a proposal, the proposer shall carefully examine the scope of services and other contract documents, and ensure that he/she has a clear understanding of the requirements of the contract work regarding the performance of work.

By submitting a response, the applicant represents that it has thoroughly examined and become familiar with the contents of the solicitation and conditions of the standard City contract documents, and that it is capable of performing quality work to achieve the City of Fontana's objectives.

2.3 INTERPRETATION OF PROPOSALS AND DOCUMENTS

If any person contemplates submission of a proposal for the proposed contract and is in doubt as to the true meaning of any part of the scope of services, or other proposed contract documents, or finds discrepancies in, or omissions from the proposal, shall be immediately brought to the attention to the City by using the electronic bid system. Such submission, if any, must be sent using the Q&A tab of the electronic bid system. Any interpretation or correction of the proposed documents shall be made only by addendum duly issued electronically to each person registered on the prospective bidder's list. The Purchasing Office will not be responsible for any other explanation or interpretation of the proposed documents.

2.4 NOTICE TO PROPOSERS

The proposers shall be considered based on the best overall value to the City. The City Council shall decide in its sole and absolute discretion whether to enter into a contract at all, even if there are one or more qualified proposers. **The City shall not be limited to awarding to the lowest responsive proposer, but instead shall be entitled to negotiate for the best overall value to the City.** The City staff may, but is not obligated to, conduct interviews with proposers.

The City may automatically disqualify any proposal that does not meet the terms and conditions set forth in these "Instructions to Proposers."

2.5 LEGAL RESPONSIBILITIES

All proposals must be submitted, filed, made, and executed in accordance with

State and Federal laws relating to proposals for contracts of this nature whether the same are expressly referred to herein or not. Any Proposer submitting a proposal shall by such action thereby agree to each and all of the terms, conditions, provisions, and requirements set forth, contemplated, and referred to in scope of services, contract documents, and to full compliance therewith.

2.6 WITHDRAWAL OF PROPOSALS

Prior to proposal opening, a proposal may be withdrawn by the Proposer only by using the City's electronic bidding system. The withdrawal of a proposal will not prejudice the right of the proposer to submit a new proposal, providing there is time to do so.

2.7 IRREGULAR PROPOSALS

Unauthorized conditions, limitations, or provisions attached to a proposal will render it irregular and may cause its rejection. The completed proposal forms shall be without interlineations, alterations, or erasures. Alternative proposals will not be considered unless specifically requested. No oral, telegraphic, or telephonic proposal, modification, or withdrawal will be considered.

2.8 ADDENDA OR BULLETINS

All proposers are advised as to the possibility of issuance of addenda affecting the items, scope or quantity of the service required for this project. Each proposer shall be fully responsible for informing themselves as to whether or not any such addenda have been issued. The effect of all addenda to the contract documents shall be considered in the proposal, and said addenda shall be made a part of the contract documents and shall be returned with them.. Failure to cover in the proposal any such addenda issued may render the proposal irregular and may result in its rejection by the City.

2.9 NON-COLLUSION DECLARATION

Proposer shall declare that the only persons or parties interested in the proposal as principals are those named therein; that no office, agent, or employee of the City of Fontana is personally interested, directly or indirectly, in the proposal; that the proposal is made without connection to any other individual, firm, or corporation making a proposal for the same work; and that the proposal is in all respects fair and without collusion or fraud. The Non-Collusion Declaration shall be executed and submitted with the proposal.

2.10 AFFIDAVIT OF CONFIDENTIALITY AND INDEMNIFICATION AGREEMENT

Vendors may designate selected portions of their proposal not on the supplied Microsoft EXCEL response forms as confidential, such as financial statements and proprietary information not publicly disclosed about their products. Any portion of the proposal which is to be held confidential should be included in separate document and clearly marked as such. Items such as the price offering may not be designated as confidential. The final decision as to any materials that will be held confidential will be made by the City Clerk. However, if a claim to release the confidential portion is made under the California Public Records Act, the City will notify the vendor of such a claim but will not defend the vendor's rights to privacy.

2.11 CONFIDENTIAL

The proposer shall identify those portions of their proposal that they deem to be confidential, proprietary information or trade secrets, and provide justification why such materials shall not be disclosed by the City. All materials the proposer desires to remain confidential shall be clearly indicated by stamping the pages on which such information appears, at the top and bottom thereof with the word "Confidential". All such materials so indicated shall be reviewed by the City and any decision not to honor a request for confidentiality shall be communicated in writing to the proposer. For those proposals which are unsuccessful, all such confidential materials shall be returned to the proposer. Prices, makes and model or catalog numbers of the items offered, deliveries, and terms of payment SHALL NOT be classified as confidential.

2.12 COMPETENCY OF PROPOSER

No proposal will be accepted from or contract awarded to a proposer who is not licensed in accordance with the law, who does not hold a license qualifying them to perform work under this contract, to whom a proposal form has not been provided and who has not successfully performed on projects of similar character and scope. The proposer may be required, before the award of any contract, to show, to the complete satisfaction of the City, that it has the necessary facilities, ability, experience, and financial resources to provide the services specified herein in a satisfactory manner. Generally, contractor history and references are required at a minimum. The City may make reasonable investigations deemed necessary and proper to determine the ability of a contractor to perform the work, and the contractor shall furnish the City all

information requested for this purpose.

2.13 QUESTIONS AND COMMENTS

Questions and comments regarding this solicitation must be submitted online using the City's bid system by clicking the Q&A tab of the, no later than five (5) days before the Submittal Deadline. Answers, if any, made by the City will be sent using the online bid system to known prospective bidders.

There will be a pre-bid webinar at 10:00 AM (PDT) on Tuesday, April 3, 2012 at which time instructions for the completion of the forms will be presented. Vendors will be able to submit their questions at that time either verbally or via the webinar's Q&A system and they will be answered during the conference. It will be recorded for playback within 48 hours after the live conference.

2.14 CORRESPONDENCE

All correspondence is to be submitted to:

Sid Lambert
Purchasing Office
8353 Sierra Avenue
Fontana, CA 92335
slambert@fontana.org
(909) 350-7678

2.15 AWARD OF CONTRACT

Issuance of this Request for Proposal and receipt of proposals does not commit the City to award a contract. The City reserves the right to reject any or all proposals to accept any proposal or portion thereof, to waive any irregularity, and to take the proposals under advisement for the period of time stated in the "Request for Proposals", as may be required to provide for the best interests of the City of Fontana. In no event will an award be made until all necessary investigations are made as to the responsibility and qualifications of the proposer to whom the award is contemplated. All responses to this solicitation shall become the property of the City and will be retained or disposed of accordingly.

No proposer may withdraw his proposal for a period of ninety (90) days after the time set for opening thereof.

2.16 TERM OF CONTRACT

Contract period shall be limited to the respective project. Proposer understands that this contract shall not bind nor purport to bind the City of Fontana for any contractual commitment in excess of the original contract period. In the event the City exercises its options, all terms, conditions, and provisions of the original contract shall remain the same and apply during the extension period, unless otherwise mutually agreed to in writing by both parties.

2.17 WORKMAN'S COMPENSATION CERTIFICATE

Section 3700 of the State Labor Code requires that every employer shall secure the payment compensation by either being insured against liability to pay compensation with one or more insurers or by securing a certificate of consent to self-insure from the State Director of Industrial Relations.

In accordance with the section and Section 1861 of the State Labor Code, the consultant shall sign a Compensation Insurance Certificate which is included with the Contract Agreement, and submit same to City of Fontana along with the other required contract documents, prior to performing any services. Reimbursement for this requirement shall be considered as included in the various items of services.

2.18 INSURANCE

Prior to the commencement of any services hereunder, Consultant shall provide to the City certificates of insurance with the City named as additional insured. Such policies shall be subject to approval by the City and shall require thirty days notice to the City before any cancellation. Failure to furnish such evidence, if required, may be considered default of the Consultant.

A. Worker's Compensation Insurance covering all employees and principals of the Consultant, in a minimum amount of $1 million per accident, and meeting the laws of the State of California;

B. Commercial General Liability Insurance covering third party liability risks; including without limitation contractual liability, in a minimum amount of $1 million per occurrence for bodily injury, personal injury, and property damage. If commercial general liability insurance or other form with a general aggregate limit is used, either the general aggregate shall apply separately to this project, or the general aggregate limit shall be twice the occurrence limit;

C. Commercial Auto Liability and Property Insurance covering "any auto" with a minimum amount of $1 million combined single limit per accident for bodily injury and property damage.

3 PROPOSAL DOCUMENTS

3.1 PROPOSAL SUBMITTAL INFORMATION

A. Submittal of Proposal: A digital zip file containing the required files shall be submitted in response to this RFP at www.fontanapurchasing.org per the instructions entitled "Submitting RFP (Proposal Only)" included with the downloaded materials. The proposal(s) shall be submitted no later than 2:00 p.m. (PST) on 5/1/2012.

B. Supplemental Materials: In addition to the RFP Response Forms as indicated above, vendor must include contracts for professional services and the service level agreement(SLA) associated with their on-going services. Award is subject ot City's legal counsel approval of contract terms and conditions and staff acceptance of the terms of the SLA.

C. Examination of the content of the RFP: By submitting a response, the applicant represents that it has thoroughly examined and become familiar with the contents of the and that it is capable of performing quality work to achieve the City of Fontana's objectives.

D. Pre-Contractual Expenses: The City shall not be liable to pay any cost incurred by any firm or persons in submitting a proposal(s) in response to this request for qualification/request for proposal.

E. Contract Award: Issuance of this RFP and receipt of proposals does not commit the City to award a contract. The City reserves the right to accept or reject any or all responses received in reply to this RFP; reject or cancel in part or in its entirety this request for proposal and/or waive any irregularities. Similarly, all responses to this request for qualifications/request for proposal shall become the property of the City and will be retained or disposed of accordingly.

3.2 EVALUATION AND SELECTION PROCESS

A. Responsiveness Review: A committee will review and evaluate each submittal to determine if it meets the "Responsive" requirements for the project. Failure to meet the requirements will be cause for eliminating the applicant from further consideration. The criteria used for determining a Responsive proposal are:

B. Compliance with Required Forms, Bonds and Certificates.

C. Adherence to the RFP Response Forms and format.

D. Acceptance of Fontana's legal contracting requirements

E. Responsible/Qualification Review: Once a proposal has been deemed Responsive, the Evaluation Committee will review the vendor's qualifications to engage in a project of the scope called for in this RFP. Though largely subjective, the same criteria and process will be used to assess each vendor. If the Committee determines that a vendor is "Not Responsible," the vendor will be contacted and advised of the reasons for the determination. While the vendor

will be given an opportunity to provide additional information that may mitigate the Committee's original finding, the Committee will determine which of the vendors meet the minimum qualification levels to continue to the next phase of evaluation. The criteria used for determining a "Responsible" vendor are as follows:

a. The ability to provide sufficient public sector references that can demonstrate organizational and fiscal similarity to Fontana with a functionally similar configuration to that proposed. [REFERENCABILITY]

b. Vendor's experience (both as a company and the particular individuals involved) with the systems and/or services proposed [EXPERIENCE].

c. Vendor's commitment to the product lines and the market [COMMITMENT].

d. Vendor's resources that demonstrate adequate financial and resource capacity to perform the tasks as proposed [CAPACITY].

e. The synergy of relationship between the various vendors in a multi-vendor proposal. [SYNERGY]

F. Value: The value (to the city) of a vendor's proposal will be determined through a point scoring formula that includes the vendor's responses to the features listing in the RFP Response Forms and the pricing for both initial and on-going costs. The Compliance responses will become part of the final agreement so if any features cannot be validated during Acceptance Testing, vendor may be deemed in breech. The criteria used for the Value computation are as follows:

a. Initial (first year) price and comprehensiveness of the proposed subsystems.

b. Five year total cost (with inflation adjustment according to the cap percentage submitted) for the system operation for the proposed subsystems.

c. Total points scored as proposed in the Price Form (Compliance Scores) document.

G. On-site Demonstration/Oral Interview: The Evaluation Committee may select two, three, or more finalists (i.e. best value, responsive, responsible proposals) for an on-site demonstration of the proposed solution. They may be asked to demonstrate specific features and/or a script of transactional scenarios to validate their proposed solution in front of the Evaluation Committee and other interested City staff. The Committee will then name their 1st, 2nd, and 3rd choice preferred vendor to begin contract discussions.

H. Contract and Award: The City will designate a person to begin contract discussions with the Preferred Vendor. The final negotiated contract will need to be reviewed and approved by the City Attorney after which, an award recommendation will be made to City Council at the next regularly scheduled Council meeting. Following award by the City Council and authorization given to enter into the contract, the award and contract will be executed by the City Manager.

3.3 RESPONSE TO PROPOSAL

The RFP Response Forms, located in the "RFP Forms.xlsm" electronic Excel document, must be submitted (uploaded) through the online bid process. All proposal materials should be collected into a single zip file which should include the following files:

A. Proposal Cover letter, signed and scanned in PDF format.
B. Proposal Narrative in MS WORD or PDF format.
C. Completed RFP Forms EXCEL document.

d.

D. Electronic versions of contract templates (professional services, software license, maintenance and support, and service level agreements).
E. Any brochures or literature relevant to the proposed solution.
F.

3.4 PRE-BID CONFERENCE

There will be a mandatory pre-bid webinar offered at 10:00AM, Tuesday April 3, 2012 to present background information on the RFP and filling out the electronic (EXCEL) forms. Questions submitted prior to that date will be answered during the webinar and any questions submitted during the webinar will be answered live if possible. The webinar will be recorded for vendors unable to attend the live conference, but vendors must sign a declaration that they have received and read any and all addenda to the RFP including listening to the entire webinar.

4 TECHNICAL SPECIFICATIONS

4.1 GENERAL REQUIREMENTS

4.1.1 Skilled Technicians

Skilled technicians are to perform all commissioning, programming and testing and are, at a minimum, to be manufacturer trained and certified to work with the security system software.

4.1.2 Local Resources

Local branch office personnel directly employed by the Contractor shall perform all work including, but not limited to, the engineering, design, installation checkout, startup, programming and pre-testing and final acceptance testing.

4.1.3 Subcontractors

C. Contractor must identify all indirect employees or Subcontractors that they propose to use to perform any of the work specified herein in the Designation of Names section and obtain prior approval for this work by the City..

4.1.4 Background Checks

Contractor shall perform background checks on all of the Contractor's employees working on the project. The Contractor shall provide all documentation showing that a background check was executed for the employees working on this project. This includes all Subcontractors and indirect employees that will be utilized by the Contractor to execute the project.

4.1.5 Latest Software Version(s)

Software shall be of the latest revision available by the manufacturer upon final acceptance of the system. This includes any Microsoft product installed on the system when purchased. All of the latest software updates and patches approved by the manufacturer must be installed at the time of system acceptance.

4.1.6 Installation Support

The Contractor will be required to maintain the integrity of all system programming before final acceptance of the security system platform. The Contractor will be permitted to add new data into the system databases, but will be required to perform system re-testing in accordance with the City's

requirements if any portion of the existing database is re-installed on the system.

4.1.7 Knowledge Transfer

A key element of this project is the knowledge transfer of the technical configuration and setup performed and training for the on-going self-management of the SMS environment. Training must be provided in a hands on lab (provided by the City) for up to 4 system level technicians and 10 end users. A minimum of 24 classroom hours of technical training and 12 hours of user training shall be included.

4.1.8 Experience

The scope of work shall be performed by a licensed Contractor of established reputation and experience who has been regularly engaged in the installation of this type of software for a period of not less than five (5) years.

4.1.9 Repairs

Repairs due to the Contractor's or their Subcontractor's negligence or improper installation of software shall be performed at no additional cost to the City.

4.1.10 Coordination

Contractor shall coordinate and be wholly responsible for coordinating all work through the City.

4.1.11 Project Management

Contractor shall provide project management resources to work in concert with the City's appointed Project Manager and coordinate all scheduling and task assignements for all Contractor resources and subcontractors, including monitoring of task work and completion for input into the project status reports.

4.1.12 Warranty of Work

Contractor shall support and warranty their work for one year after acceptance by the City and thereafter may offer annual support and maintenance including the installation and testing of manufacturer patches and updates.

4.2 PROJECT SCOPE OF WORK

4.2.1 GENERAL

A. All work detailed in this specification, or as required to facilitate the intent of the project, is to be part of the work.

B. The contract for this project shall be issued with the understanding that the Contractor is to provide all items required for the completion of the work without adjustment to the contract price. It is intended that the Contractor shall be solely responsible for the inclusion of adequate amounts to cover all work indicated, described or implied, subject to the intent of the City.

4.2.2 INCLUDED TASKS

A. The Contractor shall provide coordination, planning, scheduling, supervision, software, installation labor and programming and testing to complete the installation of the security system software platform. As further clarification, the following work is included:

B. Installation of SMS software platform on server and client equipment provided by the City;

C. Programming new SMS software platform with existing naming conditions utilized on existing Bosch ReadyKey Security Software;

D. Documenting all configuration and programming work and demonstration of what was done and how it was done for City technical staff;

E. SMS software platform shall provide all licenses necessary to support two hundred and fifty-six (256) card readers, OnSSI Video Management System Integration, Video Badging, up to nine (9) Operator workstations, integration to Bosch Alarm System panels at a minimum;

F. All equipment and licensing to support installation of a new, fully integrated Identity Management (Video Badging) system. Reuse of existing equipment is preferred. If the Contractor cannot use existing badging equipment, including printers, Contractor shall note in proposal and provide optional pricing for new badging equipment;

G. Contractor shall provide all necessary labor for programming of naming conventions, Identity Management configuration and integration and Active Directory configuration and integration;

H. Pre-installation planning is to be performed by the Contractor to insure that all installed software integrates into City of Fontana's IT Department environment including the utilization of Active Directory;

I. The City of Fontana shall provide all servers, clients and related networking hardware. The City of Fontana IT Department shall cooperate with the installation of the SMS software platform and requires the Contractor to participate as and advise for oversight.

J. Contractor will provide a maintenance and support plan and agreement for the delivered and installed system(s) that will warranty all work for one year after acceptance at no additional cost and provide a fixed fee for support and maintenance on an annual basis thereafter. Increases to the annual maintenance and support fees shall not exceed the BLS COLA for the San Bernardino/Riverside/Los Angeles area for the preceding 12 month period.

4.3 SOFTWARE FUNCTIONALITY

4.3.1 Platform

A. The SMS software shall not limit the number of cardholders, visitors, and assets. If additional licenses are needed to support additional units than those included in the base pricing herein, they must be included in the Price Form using the lowest increment available.

B. The database server shall not limit the number of system events and System Operator transactions in the history file limited only by available disk space.

4.3.2 Access Control

A. One of the SMS's primary purposes shall be to provide access control. The SMS shall be able to make access granted or denied decisions, define access levels, and set timezones and holidays. An input or output linkage feature shall allow linking of monitor zone points to output control points within Intelligent System Controllers (ISCs). The SMS shall support features such as area control (two man control, hard, soft, and timed anti-passback), database segmentation, and timezone or holiday overrides.

4.3.3 Alarm Monitoring

B. The main Alarm Monitoring window shall provide information about the time and location of the alarm, along with its priority. The main Alarm Monitoring display window must be able to filter and sort pending and/or insert new alarms based on any of the following attributes: priority, date or time, alarm description, Intelligent System Controller, Card Reader, Input Control Module, asset name, or cardholder. Date or time sorts must be System Operator selectable to be either ascending or descending and must have the option of displaying the seconds of the minute in which the alarm arrived into the SMS. All columns of information in the main Alarm Monitoring window shall be able to be arranged in any order by the System Operator.

C. The SMS must allow unique emergency instructions to be specified for each

type of alarm. It shall also allow for the automatic sending of alphanumeric pages or e-mail messages upon alarm arrival. A real-time graphical system status tree on the screen shall indicate if card readers, alarm panels, digital video recorders, video cameras, intrusion detection panels, or Intelligent System Controllers are secured, unsecured, in alarm, or offline. Output control operations must be available to lock, unlock or pulse control points as a standard feature. An automatic cardholder call-up feature shall allow the quick search and display of images in the database. A System Operator journal shall be available to log important daily events. A trace function shall be available for System Operators to locate and track activity on specific cardholders, assets, video cameras, or card readers. An image comparison feature must be provided for use in conjunction with a CCTV interface. All alarms and hardware icons MUST have the ability to control the associated hardware via right-mouse clicks.

D. The SMS must provide the option to be used as a UL 1981 Classified Central Station Automation System. This option must be classified by Underwriters Laboratories for use as a Commercial Burg Central Station Automation System, to allow the monitoring station where it is used to be made compliant with the UL 1981 standard and listed by UL. This classification shall apply to alarm panels monitored through a connected, UL approved Central Station Alarm Receiver.

E. The SMS must provide signal output for either IP based or ASCII feeds.

F. The TWIC System shall be able to connect to and interface bi-directionally with external data sources utilizing all of the following methods:

1. ASCII with support for XML formatted text exchange of data activated both manually and automatically.
2. ASCII with support for XML formatted text exchange of data using a direct table interface activated both manually and automatically.
3. Real-time exchange of data via Active Directory or LDAP utilizing an API (Application Programming Interface) written by the SMS manufacturer. The live exchange of data shall expose SMS events and transactions to other data sources in real-time and allow for receipt of data into the SMS where this data may be acted upon and trigger linked events in the SMS in real-time.

4.3.4 Credential Management

A. The SMS shall include a seamlessly integrated credential management module. The credential management functionality must allow the

enrollment of cardholders into the database, capturing of images, biometric data, and signatures, as well as the import or export of employee data. This functionality shall also allow the System Operator to assign and/or modify the access rights of a cardholder.

B. This shall allow for the creation of different badge types based on a database field, the linking of that field to a badge type to automate the process of credential production, and the use of security colors, chromakey, and ghosting, to allow officers to quickly identify personnel access authority.

C. The SMS shall have capabilities for biometric verification. Through the enrollment and comparison of hand geometry (the size and shape of an individual's hand and fingers), or fingerprints, the identity of an individual shall be verified.

D. The SMS shall have the ability to crop and rotate an image. This shall include photographs captured from digital cameras, live cameras, scanned images and imported images.

4.3.5 Digital Video Management

A. The SMS shall include a seamlessly integrated digital video management module. It shall support real-time linkage of digital video clips to their associated alarms as well as those from linked devices in the SMS database; Access Control hardware for example. This linkage shall happen automatically as defined by the configuration.

B. System Administrators shall define parameters for video segment creation by specifying pre-alarm and post-alarm durations. The system shall automatically associate alarms from linked hardware with the linked camera's pre- and post-alarm durations.

C. System Administrators shall configure video segments by specifying pre- and post-alarm time marks, then link those defined video segments to specific alarms. Each camera shall be configured to have its own unique set of pre- and post-alarm time marks, video quality settings, and failover recorder. The SMS shall allow for the central administration, monitoring, and archiving of digital video and the associated cameras. The SMS shall have the ability to launch video on alarm.

D. The SMS shall support the ability to define video behavior by alarm type. The SMS will dynamically apply the behavior in real-time as alarms come in.

E. The SMS shall support Digital Video Recorders from multiple

manufacturers. The SMS shall also support IP-based digital cameras and digital video encoders or servers from multiple manufacturers for advanced video surveillance. The SMS shall support MJPEG, MPEG4 simple profile encoding standards and frame rates to include both PAL and NTSC respectively at maximum of 25/30 frames per second. In addition, the SMS shall support a network-based digital video recorder.

4.3.6 Intrusion Detection Management

A. The Intrusion Detection Management System shall provide advanced, seamless integration with Intrusion Detection Panels from BOSCH (D9412 and D7412), Detection Systems (7400xi and 7400xi 4+), Honeywell (Galaxy 8, 18, 60, 128, 500, 504, 512, Galaxy Dimension GD48, Galaxy Dimension GD520), Lenel NGP, and Guardall PX, QX, RX, allowing customers to monitor intrusion detection alarms inside the SMS Alarm Monitoring application, in addition to giving CUSTOMER command and control of supported intrusion detection devices (such as arming and disarming an area). Once alarms are brought into the SMS, they shall be linked to digital video, global I/O activity can be triggered, and they shall be stored in the SMS audit trail. In addition, System Operators shall monitor the status of intrusion detection devices from the SMS Alarm Monitoring Workstation.

B. Any firmware updates to alarm panels in all facilities should be done remotely through the network for all panels already connected to the network. If such updates require physical modification to the panels, the cost should be included in the proposal and itemized as such.

4.3.7 Asset Management

A. The SMS shall include a seamlessly integrated asset management module to include real time management and tracking of CUSTOMER assets. The SMS shall allow for the centralized management of assets. System Administrators shall be able to generate reports on current asset assignments as well as the history of cardholder assignments for assets. The SMS shall also be able to restrict assets from passing through checkpoints with unauthorized personnel and report assets that pass through checkpoints with authorized personnel. The SMS shall also allow specified readers to require an authorized asset before granting access.

4.3.8 Visitor Management

A. The SMS shall include a visitor management module. The visitor management module shall be an application utilizing technology that allows a CUSTOMER to enroll and track visitors of the organization.

B. The visitor management module shall allow a CUSTOMER to enroll visitors, sign them in or out, capture a photo, and capture a driver's license or passport. The visitor management module shall allow System Operators to enter and pre-schedule visits. The visitor management module shall allow System Operators to print visitor badges.

C. Consultants hired for extended terms who require access to city facilities should be treated as long-term visitors and their access to facilities can be configured to be work-hours only, after hours, and programmed to expire at the end of the contract term.

4.3.9 Remote Access Level Management

A. The SMS shall include a seamlessly integrated remote access level management module. The remote access level module shall be a desktop-based application technology that allows CUSTOMER managers to assign and remove access levels to and from cardholders in the existing SMS database. All transactions relating to the adding and/or removal of access levels shall be recorded complete with a time and date stamp and the System Operator who made the change.

4.3.10 Third Party Interfaces

A. The SMS shall integrate with a number of third-party hardware and software products. The SMS shall provide an industry standard OPC Server utility to allow the export of any and all SMS alarms and events to industry standard OPC Clients, such as building automation and/or process control systems. The SMS shall also provide the ability for an Alarm Monitoring Workstation to function as an OPC Client that shall accept alarms and events from industry standard OPC Servers, such as those from Building Automation or Process Control Systems.

B. The SMS shall provide seamless integration with fire alarm systems such as Pyrotronics and Notifier, personal safety systems such as Visonic Spider Alert, intercom systems such as Zenitel Alphacom or AlphaNet, and central station alarm receivers such as BOSCH 6500 or 6600 and Osborne Hoffman 2020. The SMS shall allow alarms and events from the third-party systems to report into the same main Alarm Monitoring window as access control alarms. Third-party interface hardware shall be configured in the SMS access control module. In some cases, System Operators shall be able to control third-party hardware devices from the Alarm Monitoring Workstation. Third-party hardware alarms and events shall be stored in the SMS database for audit trail and reporting purposes

4.3.11 System Administration

A. System Administrative tasks such as defining client workstation and System Operator permissions set-up, access groups, timezones, reports, maps, etc. shall be provided from any client workstation on the network. Initial setup of the cardholder screen layout shall occur at the application server level . The SMS shall support the use of strong passwords.

4.3.12 Mobile Enterprise Solutions

A. The SMS shall support a Mobile Enterprise Architecture for customers with mobile computing needs. Mobile Enterprise functionality shall be a seamlessly integrated, robust solution that transports virtually all SMS client functions to a wearable, portable computer. The portable computer shall connect to the network and SMS Server via WiFi (802.11g or n), or shall be operated as a standalone solution that synchronizes with the SMS Server on an operational basis.

4.3.13 Badge Layout Creation

A. The SMS shall provide a Badge Layout Creation and Editing Module to allow for the creation of custom badge designs to be created by the CUSTOMER. The SMS shall support credit card, government, and custom credential sizes in either a landscape or portrait format and shall support double sided and edge-to-edge printing.

4.3.14 Screen of Forms Creation

A. The SMS shall provide a Forms Designing and Editing Module that gives System Administrators the ability to modify any standard field to customize any or all of the cardholder, asset, or visitor forms. The SMS shall also allow System Administrators to add custom fields in addition to any standard fields on a minimum of 32 pages each of information for cardholder, visitor, and visit related data. User-defined fields absolutely shall not be pre-defined, meaning only the labels can change while the properties cannot. System Administrators shall have a minimum of 96 pages of which to design their cardholder, visitor, and visit screens with standard and custom fields.

4.3.15 Graphical Map Creation

A. The SMS shall provide Graphical Map Creation and Editing Software that must allow System Administrators to import customized map backgrounds of their facility and to attach custom icons to those maps.

4.3.16 Application Programming Interfaces

A. The SMS shall provide a set of standard Application Programming Interfaces

(API's) and supporting documentation that allows hardware manufacturers and software application developers to integrate their products into the SMS. The Application Programming Interfaces shall allow requests from CUSTOMER to integrate a third-party hardware or software solution based on SMS open architecture and SMS device independence.

4.3.17 Data Import

A. The SMS shall support an import utility that will allow the CUSTOMER or VAR to import cardholder information into the SMS database. This shall allow the CUSTOMER or VAR to pre-populate the SMS database with existing cardholder data and/or add new records to the existing SMS database.

4.3.18 Bi-Directional Data Exchange

A. The SMS shall support a real time, bi-directional data interface to external databases such as Human Resources, Time and Attendance, or other systems. The interface shall allow data to be imported into or exported out of the SMS in real-time or in a batch mode basis. Data used for import shall be retrieved directly from an external database or through an import file. Data provided for export shall be applied directly to an external database or through an export file. Any data shall be imported or exported including image data. The file used for import or created by export shall have the ability to be structured in a wide variety of ways, but shall always be in ASCII text format.

B. The SMS shall also support a one step download and distribution process of cardholder and security information from the external database to the SMS database, all the way down to the Intelligent System Controller (ISC) database. This shall be a guaranteed process, even if the communication path between the SMS database server and the ISC is broken. If the communication path is broken, the data shall be stored in a temporary queue and shall be automatically downloaded once the communication path is restored.

4.3.19 Interfaces

A. The SMS shall allow System Administrators to expose specific SMS data and events that are relevant to IT information or other third-party systems. Conversely, the SMS shall allow System Administrators to accept and process information exposed from the IT information or other third-party systems. This shall permit System Administrators to develop scripts and applications that allow events in either the IT domain to cause appropriate

actions in the Security domain, and vice versa.

4.3.20 VMWare Compatible

A. The server must be able to function in a VMWare environment and use the VMWare tools for failover redundancy