Wireless MESH Network Pilot Project RFP

Santa Cruz Consolidated Emergency Communications Center

Representing:
Santa Cruz Metro Records System

April 3, 2006

Scotty A. Douglass
Systems Manager

“To plan, coordinate, and implement an agency operated Wireless MESH Network Pilot Project for Capitola, Santa Cruz, Scotts Valley, and Watsonville Police Departments to:

• Provide wireless access at each agency in and around their individual police departments
• Provide a cost-effective solution
• Demonstrate the effectiveness of providing high-bandwidth data communications to/from the police mobile data computers
• Demonstrate the ability to expand the network coverage area by adding access points to implement a MESH network.”
PROJECT BACKGROUND

On July 1, 1991, Santa Cruz County, and the cities of Capitola, Santa Cruz, and Watsonville occupying over 435 square miles in the central coast area of California created a “Joint Powers Authority” consolidated emergency communications central 911 Dispatch center in Santa Cruz called the Santa Cruz Consolidated Emergency Communications Center (SCCECC). SCCECC serves four (4) major law enforcement agencies, ten (10) fire districts, and American Medical Response (AMR – local ambulance/paramedic services provider). In 1999, Watsonville, Santa Cruz, Scotts Valley, and Capitola Police Departments combined efforts in creating a wireless Mobile Data Computer (MDC) infrastructure using the 800 MHz radio spectrum. This group is still operating in a joint effort and is called the Santa Cruz Metro Records System (SCMRS). This initially provided the agencies with a 9.6 Kbps data network using three (3) radio base stations. This system gave the agencies the ability to share an MDC network that tied them together so that all four agencies could communicate to one another via a data system. In 2000, SCMRS executed a letter agreement with SCCECC to provide technical administration and services for the MDC infrastructure as well as the MDCs to the unit level.

Since that time, there has been an increasing need to implement a higher bandwidth solution that would give the officers in the field the ability to have the same access to the police computer systems as if they were on a computer at their police agency. Some common systems that require a high bandwidth data connection are email, real-time access to the Records Management System, mug-shots and streaming video, police intranets, and access to state systems.

In 2004, the benefits of using an agency operated MESH network to deliver increased data speeds to the MDCs was presented to the Santa Cruz County Emergency Management Council in an attempt to increase interoperability efforts in the county. The plan for a pilot project implementing a MESH network was proposed requesting that Homeland Security Grant Funding be allocated to SCMRS. This pilot project proposed items are included in the mission statement below:

“To plan, coordinate, and implement an agency operated Wireless MESH Network Pilot Project for Capitola, Santa Cruz, Scotts Valley, and Watsonville Police Departments to:

- Provide wireless access at each agency in and around their individual police departments
- Provide a cost-effective solution
- Demonstrate the effectiveness of providing high-bandwidth data communications to/from the police mobile data computers
- Demonstrate the ability to expand the network coverage area by adding MESH units to implement a multi-node MESH network.”
The last mission statement item can be accomplished by one of two methods:

- Adding portable MESH units that are easily mobilized for field deployment to remote locations for special events or circumstances, e.g. areas normally outside the coverage map such as fairgrounds, or to handle circumstances such as a natural disaster aftermath.

- Adding MESH units to fixed location(s) such as buildings or light poles scaling upward towards a fully implemented MESH network

Moreover, SCCECC’s role in this endeavor is that of project management, coordination, installation, and implementation for SCMRS.

A MESH network solution provider is sought, knowledgeable in this technology to provide SCMRS with the equipment necessary to execute such a pilot project.

Once the initial proof of concept is completed for this pilot project, the same technology will be used to expand coverage around the agencies interested in doing so. One of the agencies looking to immediately expand coverage after the pilot project is the City of Watsonville and its Police Department. Their expansion will be regarded as a test case for the surrounding cities should they decide to follow suit to further expand their own coverage areas.

Much of the funding for the expansion coverage will be provided by other city departments. Thus, it is logical to conclude that the public safety infrastructure developed within this pilot project be capable of expanding services beyond the Police Department to handle other city agency requirements. For example, the wireless network should also be flexible enough to handle future city agency needs such as VoIP telephones and radios; the use of mobile wireless finger-print scanners, Public works application of wireless utility meter reading-automatic meter readers, GIS, and support municipal employees in such endeavors as building and code enforcement, building inspection-licensing-permits. Ultimately, the public safety departments (police and fire) can be on its own network and the City municipal systems on another, all sharing the same wireless infrastructure funded by their respective cities.

The initial expectation for the City of Watsonville is to cover 2 square miles beyond the “in and around” test area defined within this RFP. As additional funds become available the eventual goal is to expand the wireless infrastructure to provide coverage across the entire city.

Thus the design presented by the solution provider must be flexible and scalable enough to accommodate the requirements of this pilot project but then to rapidly expand to handle each city’s/agency’s current and future requirements.

Preliminary wireless coverage drawings will be supplied to “qualified” solution providers to assist in bidding for this pilot project. Once the pilot project proof of concept is
completed, coverage drawings will be supplied by the agency’s respective city to expand their coverage beyond the initial police department coverage areas. The RFP for this pilot project is issued and will be awarded by the Santa Cruz Consolidated Emergency Communications Center (SCCECC) on behalf of the SCMRS agencies represented.

**NETWORK TOPOLOGY**

In order for the solution provider to present a viable solution, the existing infrastructure must be taken into consideration. The SCMRS data network is built on a 100Mbps switched Ethernet backbone that connects to all SCMRS participant servers through T-1 connectivity in a single domain. The City of Santa Cruz hosts the primary domain controller and the data is replicated to each of the other agency’s back-up domain controllers.

The various agency networks are built on 100 MB switched Ethernet backbones that connect to the Santa Cruz County data network, California Department of Justice, Santa Cruz Metro Record’s System (SCMRS), and Santa Cruz County Consolidated Emergency Communications Center (SCCECC). Internet connectivity for each agency is through their respective department’s firewall through their City’s proxy server. The police department’s intranet system is hosted on a local server as part of the department’s data network.

Law enforcement currently accesses CAD and CLETS data through MDCs connected via 800 MHz to on-site antennas and base station radios. They are then transferred to SCCECC through T-1 connectivity. Desktop connectivity to Santa Cruz County data systems is routed via T-1 line.

![Figure 1. Generic overview of the Police data network.](image-url)
The wireless network will initially provide coverage locally in and around each of the Police Department agencies depicted in Figure 1. If a particular city decides to move forth and expand coverage across their city, like the City of Watsonville, the design and equipment should be flexible enough to accommodate not only public-safety traffic, but also other city departmental traffic while maintaining security, integrity, and segregation of each group’s data.

**SCOPE OF WORK**

SCMRS is seeking proposals from MESH Network Solution Providers with demonstrated experience in metropolitan scale wireless networks. Joint proposals will not be accepted. If a firm intends to have services provided by other solution providers, it will be mandatory for the firm submitting the proposal to act as the prime consultant for all service/equipment delivery as specified in this RFP. The proposing firm shall be considered the sole point of contact with regard to contractual stipulations.

SCMRS proposes to engage the selected Solution Provider to provide the equipment necessary to implement a wireless MESH network pilot project as set forth in this Scope of Work.

The MESH Network and Equipment should exhibit the following essential characteristics:

- **Affordable**: Affordably priced system components necessary to demonstrate the benefits of a MESH network near each police department’s headquarters, with the exception for the City of Watsonville looking to immediately expand beyond the initial test coverage area.

- **High Availability**: System reliability and fault tolerance shall be major objectives in the design of the system. The system shall offer high levels of reliability and deliver 99.99% network uptime within the coverage area. It shall provide automatic fail-over protection at multiple levels, including at the wireless link and the connection to the wired network. The system as proposed must provide protection against local environmental disrupters, including transient power, power failures, and resiliency to interference. This protection must operate automatically and not require manual intervention. To ensure optimal network performance, the network needs a comprehensive, up-to-date view of the RF environment and the ability to auto-configure to avoid this interference.

- **Scalable**: The system shall provide high bandwidth capacity to handle multiple applications. These applications would include application to write, submit, and print reports while in the field; viewing mug shots and live video, access to the records management system, ability to access the Web and other
portable wireless computing applications. The system shall offer fully redundant coverage over the proposed service area, i.e. anywhere that a car can navigate on the streets. Finally, the system shall offer an expansion path for increasing the service coverage area.

d) **Support Multiple Users:** Provides wireless services for the named governmental agencies using 802.11a/b/g protocols or equipment operating in the newly designated 4.9GHz range as well as provide for the ability to bring on non-public safety traffic, i.e. other city departments and NOT the general public, using the 802.11g/b protocols in the 2.4GHz range. Ideally, this would be thru the use of a system capable of supporting VLAN traffic to segregate client traffic onto their respective networks.

This wireless network is specified for public safety and will not function as a carrier mechanism for general public Internet access. Solutions intermingling general public traffic and public safety infrastructure, even thru VLANs, will not receive consideration.

e) **Cost Viable:** Must be economically viable to the System Owner.

f) **Upgradeable:** Progressive and forward-looking technology, taking into account new technologies and evolving SCMRS needs, e.g. support for 4.9 GHz public safety spectrum via software upgrade to 802.11a radios.

g) **Reliable and Simple:** Reliable and easy-to-use services.

h) **Roaming Support:** Transparent and seamless integration relative to service hand-offs and account settlements. The wireless network shall permit the MDC’s and portable wireless devices to roam across the entire area of coverage without requiring manual switching or changing of MDC/handheld configuration. Once authenticated, a connection shall be maintained while roaming across the coverage area, i.e. there must be no re-connection required when moving from access point to access point.

i) **Secure:** Support robust technologies and methodologies for ensuring secure access over the system.

j) **Ruggedized:** The equipment used outdoors must be weather-proof to withstand adverse weather conditions inherent to coastal areas. The MESH equipment must also be protected against power spikes and brown-out conditions.

k) **Bandwidth:** Bandwidth should be at least 2-5 Mbps whenever the client is within the coverage areas.
WIRELESS MESH NETWORK REQUEST FOR PROPOSAL

l) **Standards-Based:** The System will be built on standards-based technologies like IEEE 802.11 (Wi-Fi) and IEEE 802.16 (WiMAX).

m) **Encryption:** The encryption used over the radio portion of the network is to be no less than AES 128-bit.

n) **Traffic Management:** The system can support multiple users based on organizational requirements (VLANs) and if necessary prioritize traffic across the network (QoS) for specific types of users or traffic, i.e. VoIP, streaming video, public safety, etc.

o) **Aesthetically Acceptable:** All equipment (antennas, radios, base stations, etc.) that are mounted to outdoor structures (Ex. Buildings, street light poles, etc.) shall not impact negatively the appearance of such structures and whenever possible shall not be visible to the public.

**EQUIPMENT**

The equipment necessary to successfully demonstrate wireless access at each police agency are as follows:

a) A single MESH access point to be deployed at each police department:
   1. Capitola Police Department
   2. Santa Cruz Police Department
   3. Scotts Valley Police Department
   4. Watsonville Police Department

The access point should meet the following requirements:

- Operational temperature range from -10 to +50 degrees Celsius.
- Lightning protection to be provided on all antenna systems
- Antennas to be grounded per NEC and EIA standards
- Enclosures shall conform to UL579 and iEC6529 IP67 weather tight standards
- Survivable to winds of 165 mph, at this wind speed it shall exhibit wind loading of less than 320 Newtons
- Equipment shall comply with
  1. MIL-STD-810F 509.4 for salt, fog, and rust resistance
  2. Shock and vibration resistant to ETSI 300-19-2-4 spec T41.E class 4M3
- Equipment shall offer a variety of power input connectors, including the ability to tap street light NEMA photo-electric control at 110/208/240V AC, secondary power, and power over Ethernet
- Equipment shall contain an automatically rechargeable backup battery capable of powering the unit for a minimum of two hours in the event of a power failure.
• Mounting equipment shall provide a mount attachment separate from the unit itself such that the mount attachment can be mounted to the structure without the unit being attached and such that the unit can be removed from the mount attachment without the attachment being removed from the structure.

b) Wireless client access cards for each patrol vehicle (75 units) equipped with a Mobile Data Computer (MDC). Each vehicle will need an external antenna and it is desirable to use access cards that are ruggedized and use the CardBus card (Type II slot) standard to connect to the MDC.

Other solutions will be considered if they can minimally meet the external antenna requirement and are ruggedized to withstand the harsh operating environment of an automobile, e.g. shock and vibration stresses, and temperature extremes.

Minimally, the client access solution should meet the following requirements:

• Ruggedized for use within an automobile
• Capable of accepting an external antenna attachment (ruggedized)
• Visual means of indicating network connectivity and signal quality
• The preferable solution is a CardBus card (Type II slot) as not all MDCs are identically equipped with features and ports. The older MDCs only support USB 1.x ports and have no network port.

c) An additional MESH access point (for each agency) to be deployed demonstrating that the MESH network can be extended beyond the default wireless range of the police department. The unit can be affixed to fixed structures such as a light pole or a building, or it can be portable so it can be deployed ad hoc.

The same specification requirements for this AP apply as they did for the unit deployed at each of the agencies, (see above).

d) Authentication server and software to manage the security of the wireless network.

The supplied equipment should be fully certified for operation under the adverse weather/power conditions stated above. Furthermore, the equipment should be accompanied by a minimum 1 year manufacturer’s warranty against any defects.

The MESH access points must be configured to be within the power output requirements to be in compliance with FCC rules and regulations according to the wireless standard.
SECURITY

SCMRS understands that access over wireless networks involves security risks and expects the Solution Provider to recommend viable solutions and advisories that will assist SCMRS with a multilayer security approach. The system shall exhibit the following features/characteristics:

- **Encryption**: Support for secure data transmission over the System is critical for government users. This should minimally be addressed in the following three primary areas.
  - The communications channel between the managing device(s) and APs should be encrypted to mask transmission of configuration data and parameters. In addition, there should be a mechanism to prevent rogue devices from joining the WLAN (Wireless LAN).
  - The backhaul layer must minimally support AES 128-bit encryption but AES 256-bit encryption is preferred.
  - The client to AP communications layer must support 802.11i authentication, encryption, and data integrity standards, (see below).

- **Support for security standards**:  
  - **802.11i**: The System shall support the IEEE security standard known as 802.11i, which offers advanced features in authentication, encryption, data integrity and digital certificates.

- **Support against Denial of Service (DOS) attacks, viruses, and other threats**: The System should exhibit the following ideal characteristics to combat these security risks:
  - Intrusion Protection/Detection Systems: Ability to protect and detect against intrusion and DoS attacks.
    - Ideally, there should be a central system that monitors intrusion. There should also be intrusion monitoring capabilities at the device level.
  - Ability to shut down and/or allow an AP to isolate a specific user based on:
    - User account.
    - Individual client device level (MAC, IP address, certificate, etc.).
  - Mechanisms to protect against other known security threats, such as:
    - Rogue access points.
    - Simultaneous identical MAC or IP addresses on the System.
    - Repetitive login attempts.
    - Attempts to access or block access to others.

- **Non-Broadcast (Hidden) SSID(s)**: Support for Multiple SSIDs, both broadcasted and non-broadcasted

- **Client isolation**: Architectures supporting client isolation via VLANs or VPN tunnels will be favored over those that allow all users to see all other users on the same access point.
• **Identity based networking**: The wireless LAN must have the ability to limit user privileges or access based upon user’s security privileges by the system and the network.

• **Audit mechanism**: The System must support an audit trail that includes tracking users that connect to the wireless network (See Network Management Requirements).

• **VPN Support**: The System must be able to seamlessly pass VPN (IPsec) traffic from multiple users to the same remote concentrator even if users are accessing the System from the same access point. More importantly, session handoffs while roaming between APs should be transparent to the end user and not require the user to manually reconnect.

**RELIABILITY**

One of the most important factors for the success of the System will be its reliability. The successful Solution Provider is expected to provide a solution with high levels of reliability and redundancy in mind. Although the system will not have much of a coverage area to serve initially, it is important that such a system expansion in the future will provide for the following:

• Uptime: Guaranteed System availability of at least 99.99%.

• Fault Tolerance: Mechanisms to mitigate and/or eliminate single points of failure for all key components of the System, wired and wireless. The system shall self-heal in the event of a unit or link failure or wireless link degradation. This shall not require manual intervention of personnel.

• RF Interference Detection: Support for detecting RF interference and automatically reconfiguring itself to utilize other possible interference-free channels.

• Units must be able to recover automatically from any loss of power.

**NETWORK MONITORING AND MANAGEMENT**

The System proposed by the vendor should be manageable from a centralized platform. The management platform should minimally include the following features and capabilities broken into the following categories:

Configuration of WLAN equipment

• All over-the-air network management traffic must be over secure links

• The network management application shall enable batch configuration and remote storage of configuration profiles

• The network management system shall provide the capability for scheduled downloading of software and configuration changes

• The network management system shall provide the ability to download software to WLAN equipment deployed in the field, both individually and in bulk

• The network management system must be able to discover, load and bring into the network new devices that are installed in the field upon receipt of their IP address
• The network management system shall offer the capability to pre-load WLAN equipment with software and configuration before they are deployed to the field as a last resort mechanism. However, it is not an absolute requirement.

User Management
• The network management system shall provide for definition of user IDs, the authentication mechanism to be used, and the assignment of corresponding network privileges and access control.

If additional resources such as RADIUS servers, etc. are required by the solutions provider, please enumerate and briefly describe in the submitted proposal its functionality and operation within the overall solution. Also, describe if these solutions can be components of existing server systems or if they must serve as standalone equipment.

Performance and Health Monitoring
• The network management application shall offer a real-time display of network status and connectivity in a graphical display
• The network management application shall report network statistics with minimal delay, including link quality and throughput
• The network management application shall offer a system event log and alarm management
• The network management application shall offer standard system and user definable performance analysis reports
• The network management application shall assist in root cause analysis
• The network management system shall store performance statistics and event logs in a user-exportable format (such as a relational database)
• The network management system must be able to send alarms to monitoring personnel utilizing a means such as SMTP.

System Requirements
• The network management system shall allow for up to 15 simultaneous users to access and maintain the system.
• The network management system must run on off the shelf Windows based hardware
• The network management system must be able to manage 1,000 WLAN devices on a single Windows based server (Handhelds, MDCs, VoIP devices, laptops, etc.)

OPERATIONS, MAINTENANCE AND SUPPORT

The Solution Provider is expected to have plans offering how it will operate, maintain and support the System and its users, or how it will train and support city or police IT personnel to operate, maintain, and support the System and its users.

For either scenario the Solution Provider should address the following aspects:
• **Customer Support Structure:** Overview of the customer support structure and procedures. Include the process from the viewpoint of the on-site end-user support personnel.
  - **Customer Assistance:** Customer helpdesk support availability (during normal business hours of the Solution/Hardware Provider).
  - **Onsite Maintenance and Support:** Options available and responsiveness in terms of time (i.e. 24/7, 4-hr windows, next business day, etc.).
  - **Escalation Process**
  - **Service Level Agreement**

• **Warranty:** Expected warranties on equipment. The vendor will indicate the warranty period for both system hardware and software components. The vendor will also describe the different maintenance/support plans available after the warranty period. Please provide cost details on included and extended warranty/maintenance plans. Ensure that all appropriate costs are included in the Price Proposal specifically on-going maintenance costs.

• **System Failures:** Process for dealing with System failures related to faulty access units in the field and System maintenance. Plans should include a list of what equipment will be required to access the components located on SCMRS agency assets (such as street light poles and traffic light poles), and the expected specialized skills required for component replacement.

• **Training:** A training plan identifying the minimum number of training hours that will be provided. The plan will identify the actual training hours and describe the size and assumed skill levels of each group. The courses should indicate whether the location will be on-site or off-site training. The Solution Provider will provide cost information for additional training that is available.

• **Documentation:** During Implementation the vendor will provide a full set of documentation required to operate and maintain the proposed system including hardware, software, computer operations, and training and operations users and reference guides. The vendor will provide one electronic and paper master copy from which the participating agencies may make in-house copies.

**SYSTEM ACCEPTANCE**

System acceptance will occur in three phases:

• Hardware and Software Certification
• Network Certification
• Final System Acceptance

After installing the system hardware and software and performing appropriate diagnostic tests, the Solution Provider will certify that hardware and software is functioning correctly. SCCECC may request specific demonstrations of the hardware-software readiness.
Upon completion of field installation of the network and training of personnel, the Solution Provider will certify that the network is ready for acceptance. The Solution Provider will be required to demonstrate all system functions to SCCECC’s satisfaction. The Solution Provider will immediately correct any problems found during this demonstration. SCCECC will verify the corrections have been made and accept the system.

The Solution Provider will then perform final system testing. Upon completion of the final system testing, the Solution Provider will certify that the network has passed the final system test criteria. Final minimal system test criteria include performance, functionality and reliability test such as:

- End-to-end throughput testing from spot locations within the coverage area. Should be at least 2-5 Mbps.
- Verification of security and VPN functionality
- Test the connectivity between the MDC and the police department network using the wireless network configuration proposed by the vendor.
  a. View a record in the police record’s management system
  b. Upload a mug shot photograph
  c. Connect to the police intranet system
  d. Connect to the wireless Metro Mobile Traffic Reporting and Citation System database hosted on the police department’s server.
- Ability to seamlessly transfer a wireless session from one AP coverage area to an adjacent coverage area without manual reconnection or authentication.
- Two-week reliability test for the pilot test and an extended reliability test period of fifteen to thirty days for the larger coverage area in Watsonville.
- Validation of link and network fail-over mechanisms

Additional system test criteria should be listed by Solution Provider in the submitted proposal.

**QUALIFICATIONS, EXPERIENCE, AND SELECTION CRITERIA**

Proposals will be considered and Solution Providers will be evaluated based upon any one or all of the following general criteria:

a) General experience of the Solution Provider.

b) Record of the Solution Provider in successfully accomplishing a metro-scale MESH network using 802.11a/b/g technology, the newly allocated 4.9 GHz wireless spectrum, or other similar wireless technologies.
c) Understanding of the Wireless MESH Network Pilot Project.

d) Qualifications and years of experience of the proposed equipment providers.

e) Cost of equipment/software/support and maintenance

f) Compliance and responsiveness to the conditions and needs expressed in the RFP.

g) Documented proof of successful implementation in technically related projects.

h) Sample timelines based on prior project experience.

PROPOSAL SUBMITTAL

Firms having the qualifications and experience to perform the necessary services may submit proposals to Michael J. McDougall, General Manager, Santa Cruz Consolidated Emergency Communications Center, 495 Upper Park Road, Santa Cruz, CA 95065 (Phone # 831-471-1000). Proposals may also be submitted (in person only) to Scotty A. Douglass, Systems Manager located at the same address no later than 3 P.M. Pacific Standard Time on May 19, 2006. Failure to meet the deadline shall result in disqualification of the proposal without review. Submittals shall include five sets of the following:

a) Brief and concise statements of general background, staffing, and capabilities of the Solution Provider.

b) Detailed documentation of recent experience on implementing an 802.11a/b/g or newly allocated 4.9 GHz wireless spectrum Wi-Fi MESH network solution. Include a list of references for completed projects including names, addresses, and phone numbers of client representatives. If other wireless technologies are substituted into the design solution, supply a detailed explanation comparing and contrasting the use of such technologies, along with a numerical analysis demonstrating cost effectiveness or comparability, (see below).

If a 4.9 GHz solution is proposed, it is understood that SCCECC would be responsible for obtaining and maintaining the FCC license for the licensed spectrum required for the implementation. The solution provider will specify the channel allocations required for their design.

c) A detailed statement of any innovative approaches in which your firm has worked on or developed for other clients. Explain your approach and the results of the efforts.
d) The name of the person within the Solution Provider assigned to work on this project, a statement of that person’s availability, and a list of other members who may also become involved on the project.

e) A fee schedule outlining the basis upon which your firm will be compensated for services and equipment.

It is suggested that proposals be limited to the information requested herein, and be as concise as possible. A cover letter and brochures may be submitted in addition to the proposal.

**SELECTION PROCESS**

The SCMRS Executive Group in consultation with their Technical Committee will consider all written proposals at their May 2006 regular meeting. After consideration of the written proposals, the SCMRS Executive Group will either select the top firm (based upon the criteria as stated in the RFP) and authorize the General Manager to enter into contract negotiations with that firm OR invite the firms to make a presentation to the SCMRS Executive Group and/or their Technical Committee as part of the final selection process. Upon completion of successful negotiations, the professional services contract will be recommended for approval to the SCCECC Board of Directors.

Additionally, the criteria upon which the evaluation of the proposals will be based include, but are not limited to, the following:

a) Total costs

b) Completeness of the proposal

c) Quality and depth of references

d) Vendor compliance with state and federal legislative mandates and standards established by the California Department of Justice for public safety wireless networks. Upward compatibility for future growth.

e) Level of service and responsiveness that the Solution Provider commits to providing SCMRS

f) Financial stability and resources of the consultant

g) Experience and technical expertise of firm’s staff

h) Economic feasibility and justification of all costs

i) Solution Provider’s willingness and ability to negotiate a contract acceptable to the Authority
j) Quality and extent of Solution Provider’s documentation provided

EXAMINATION OF DOCUMENTS

Solution Providers shall examine carefully all documents and data provided. No pleas of ignorance of the requirements or of the documents will be accepted as a basis for any claim whatsoever for extra compensation.

COST OF PREPARATION OF PROPOSAL

The Authority shall not pay costs incurred in the proposal preparation, printing, demonstration, or negotiating process. All costs shall be borne by the proposing supplier.

CONTACT WITH AUTHORITY OR AGENCY EMPLOYEES

In order to ensure fair and objective evaluation, all questions related to this RFP should be addressed directly to Scotty A. Douglass at the address listed earlier in this document. Contact with Authority, its employees, or its consultants is expressly forbidden without prior written consent.