

ATTACHMENT B GENERAL QUESTIONS

In preparation of its RFP the vendor shall provide answers to the following questions in regards to its SOW for a needs assessment and solutions based RFP:

General Solution Items:

- G-1 How often are major upgrades for the proposed software component of the surveillance system released? Minor upgrades?
- G-2 When was the last major upgrade to the proposed software component? Minor release?
- G-3 How many clients and sites are currently using the proposed version as their production system?
- G-4 Identify any scalability constraints within the proposed solution.
- G-5 What is the largest organization you support?
- G-6 Explain any plans for major technology or functionality changes in the proposed solution within the next 18 to 24 months.
- G-7 Describe the solution up time that can be expected from the proposed solution.
- G-8 Describe the documentation available for the proposed solution including the media on which it is available. One copy of the following documentation (either paper or CD) is to be included with your technical response:
- End user manual (including all operations, sample reports, screen illustrations, and instructions for software provided).
 - System administration.
 - Technical documentation and specifications.
 - New release, enhancement, and fix documentation.
- G-9 Describe any administrative remote access features in the proposed solution.
- G-10 Describe any electronic notification features within the proposed solution (problems, issues, performance, etc.).
- G-11 The Vendor understands that they will provide source code or will arrange for the source code to be placed in escrow on behalf of Clay County. One copy of your proposed escrow agreement must accompany your technical response.
- G-12 Describe the abilities within the proposed solution to archive, retrieve, and purge pre-recorded video.
- G-13 Provide a description of any failure notifications within the proposed solution.
- G-14 Describe error logging and reporting within the proposed solution.
- G-15 Describe the license structure available for the proposed solution (named user, concurrent user, enterprise, etc.)
- G-16 Vendor understands that the proposed solution may be installed on multiple environments (test, development, training, production, DR, etc.) Identify any concerns of the Vendor regarding this.

Security: - Indicate if the function is standard off the shelf or if customization would be required:

- S-1 Identify and describe the available levels of security (role, user, screen, module, table, column, update, view only, etc.)
- S-2 Describe any automatic functions including inactivity log off, etc. used in the solution.
- S-3 Identify administrator functions and the ability to lock out administrator from other functions (allow to: grant security access, modify inactivity timeout, password reset, accessing server console and management workstations, restrict from: performing database administration, backups, and recovery).
- S-4 Explain how the system can allow password reset by selected users without giving access to administrator functions.
- S-5 Provide a detailed description of the security model in the proposed solution. Explanation should include:
 - Security to protect against access to the system or its data by unauthorized users.
 - Encryption abilities – include Public Key Infrastructure (PKI) capabilities.
 - Lockout methods.
 - User passwords – include: maximum and minimum length configuration formats, (characters, numbers, blank etc.) limitations on password reuse, required reset periods and if a blank password is allowed
- S-6 Explain the authentication method employed (certificates etc.) – include discussion on invalid certificate processes.
- S-7 Provide detailed methods on how security is applied to protect the recorded video streams. Detail if users can access video without using the application interface, via ODBC connect or other means.

Camera Equipment:

- C-1 Vendor should provide supporting documentation (i.e., manufacturers' specifications) that all camera equipment recommended for the electronic surveillance and security control systems meets each of the following requirements:
 - Ability to transmit images wirelessly using industry standard wireless protocols and standards.
 - Digital Internet Protocol.
 - Pan Angle of 360 degrees.
 - Minimum Tilt Angle of 100 degrees.
 - Minimum optical zoom of 30X.
 - Automatic Iris Control.
 - Auto Focus.
 - High resolution color and black and white capability.
 - Ability to transmit viewable images in light levels of .008 lux or lower.
 - Ability to transmit a minimum of 30 frames per second.
 - IP based when functionally appropriate.
- C-2 Vendor should provide documentation that the recommended cameras are equipped with appropriate sensory devices that are capable of triggering recording only when motion is detected within its designated surveillance area.
- C-3 Vendor should describe the general power requirements and power maintenance requirements for cameras and enclosures.
- C-4 Vendor should provide documentation that camera enclosures are weatherproof, vandal resistant, UV resistant and non-ferrous (if metal only).
- C-5 Vendor should detail any internal temperature controls, sensors, heating elements, fans or other devices within the enclosures that are needed to maintain the proper operating temperature of the cameras.

Network and Connectivity:

- N-1 Describe the types of networks the proposed solution can run on or over. Include topology and required speeds where appropriate. (IP-only, LAN, WAN using frame relay T1, etc).
- N-2 Describe how the cameras will transmit from themselves, wirelessly to the digital video management PC or DVR, specifying the open architecture and components that can be deployed elsewhere.
- N-3 Vendor shall specify the size of the video streams from real-time or captured video
- N-4 Describe how the proposed solution will minimize network bandwidth while still transmitting a minimum 30 frames per second. Include any bandwidth requirements or recommendations for each site to accomplish this throughput.
- N-5 Specify the security and encryption techniques that will be employed to secure the wireless transmissions within the proposed solution.
- N-6 Identify the browsers (including versions and service packs) with which the proposed solution has been tested.
- N-7 Does the proposed solution run over a Virtual Private Network (VPN)? Identify the broadband methods utilized (i.e. cable modems, DSL, NAT, etc.).
- N-8 Has the proposed solution been tested and implemented using Citrix? Citrix Secure Gateway? What are the requirements for software on Citrix to support the application?

Intelligent Video Analytics: – Provide detailed information regarding the Intelligent Video Analytics:

- VA-1 Describe the general parameters of the video analytics software and its specific features and capabilities related to remote monitoring of public facilities.
- VA-2 Describe the type of alert sent when the analytics detect an event. Include format, message size and how the receiver will access the live video feed directly from the alert message.
- VA-3 Describe how the analytics are able to distinguish between a non-threat (i.e., a deer) and a potential threat (i.e., a human) before an alert is sent.
- VA-4 Vendor should provide the proposed configuration of the video analytics, including:
- Scalability for an unlimited amount of cameras
 - Whether management of the analytical system is centralized or distributed or both
 - Number of items or events that can be recognized
 - Recommended placement of analytics within the network that will optimize network bandwidth
 - Any additional server or network hardware required to support the analytics
 - Ability to transmit an alert only when a specific event occurs during pre-defined hours
 - Describe how the end user can configure and manage the analytic parameters. What settings, parameters and tolerances are end user manageable?
- VA-5 Vendor must specify if the proposed solution is capable of triggering lights and an audible annunciation upon detection of a threat, and then waiting for a user specified duration before sending an alert.

Support:

- SP-1 What is the ratio of support staff to client?
- SP-2 Vendor will describe the methods that will be implemented to provide support for the proposed solution on a 24 X 7 X 365 basis including holidays.
- SP-3 Vendor will describe the technical team that would be implemented to support the County for implementation and on-going support (account representative / manager, project manager, technical team leader, etc.).
- SP-4 Describe the Vendors technical support procedures (include escalation processes, hours and methods for receiving support).
- SP-5 Describe any upgrade notification and / or proactive automated electronic notifications processes that the Vendor utilizes.
- SP-6 Describe how the Vendor will fulfill the County's Incident Response Standards as outlined herein. See the Incident Response Standards as defined in this document.

Training:

- T-1 Describe in detail the training methods (instructor led, train the trainer, on site at County, via ebex or Internet, on site at Vendor) available through your company.
- T-2 Identify the levels of training available to the County (end user, system administrator, power user, etc.)
- T-3 Identify any training restrictions (class sizes, etc.).
- T-4 Describe training length and times available from your company (different time intervals, spread out over longer periods of time, during non-standard work hours).
- T-5 Define, in detail, the environment required for training (delivery method, hardware requirements, OS/NOS requirements, client hardware requirements, etc.).
- T-6 Describe the training course materials available and identify who is responsible for providing student copies of the course materials. One copy of the standard course materials (either paper or CD) is to be included with your technical response.
- T-7 Identify the methods used to customize training materials for any County modifications or business processes.

Services:

- SV-1 Identify any/all services available through your company (i.e., project management, installation, electrical work, etc.).
- SV2 Describe your company's services staff including the ratio of services staff to client.

Hardware:

- H-1 Provide information regarding solution failover capability – including identification of compatible failover software.