

Guide to Developing a Request For Proposal (RFP) for Video Surveillance Systems for Schools

MTS Intelligent Surveillance Solutions, LLC

September 2006

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

1.0	Purpose of Document.....	3
2.0	Background.....	4
2.1	Why Schools need Video Surveillance.....	4
2.2	Video Surveillance Evolution – Technology changes and updates	6
2.3	Security Policy Role and Development	9
3.0	Request For Proposal (RFP) Recommendations.....	10
3.1	Organizing the RFP Process	10
3.2	Process Recommendations.....	11
3.2.1	Requirements Process	11
3.2.2	Specification Development Process.....	12
3.2.3	RFP Package Development Process	13
3.2.4	Solicitation	14
3.3	Example Scoring Techniques	15
4.0	Specifications	17
4.1	Digital Video Recorder/Network Video Recorder	17
4.1.1	DVR Hardware.	17
4.1.2	DVR Features/Functions.....	18
4.2	Cameras.....	20
4.3	Wiring/Cabling	21
4.4	Implementation	22
4.4.1	Project Management.	22
4.4.2	Installation Practices.	22
4.4.3	Scalability.	22
4.4.4	Head-end standards and best practices.	23
4.4.5	Lighting considerations.....	24
4.4.6	Lensing- the ability to use video for discipline and prosecution.	24
4.4.7	Documentation.	24
4.4.8	Training.....	25
4.4.9	Other - Integrator Specifications.....	25
4.5	Maintenance.....	26
4.6	Costs.....	26
5.0	Glossary	27

1.0 Purpose of Document

This document is targeted at providing assistance to the education community. It is intended for school administrators, security managers, procurement officials, or other municipal officials whose responsibilities include specifying or procuring security systems for schools. In the instance of new construction, this document may prove useful to architects and designers such that video surveillance systems can be incorporated into design specifications early-on in the design process.

There are three key objects of this document:

- To provide the education community with guidelines and tools to procure video surveillance systems
- To provide an example method to aid in the procurement process
- To provide a sample specification to use as a guideline in developing a procurement package for schools

This document is structured such that it specifically does not recommend any particular manufacturer name hardware or software and, as such, is intended to help develop an open procurement.

2.0 Background

It is important to understand the growing requirements that suggest video surveillance in the schools. It is also useful in understanding the rapid advances in technology pertinent to video surveillance. Finally, understanding the relationship to security policy ensures the final solution performs as intended and is optimized.

2.1 Why Schools need Video Surveillance

There is a need for increased safety and security within our public education community. Springfield, Oregon; Columbine, Colorado; Red Lake, Minnesota. These are the headline tragedies that have caught the nation's attention over the past few years. Agreeably, these are isolated incidents. However, 10% of the nation's schools reported one or more violent crimes in the 1996-1997 school year, including murder, suicide, rape, robbery and fights involving weapons. In 2002 alone there were 659,000 student victims of rape, robbery and aggravated assault. In 2003, 7% of students said they were bullied at school and twenty-one percent reported street gangs in their school. In 1999, 9% of teachers were threatened with injury by a student and 4% were physically attacked by a student.

According to the National Center for Education Statistics, 7.2% of girls in grades 9-12 reported engaging in a physical fight on school property. Boys reported 18%. According to the Centers for Disease Control, more than one out of every twenty high school students skipped school at least one day because of safety concerns in 2003. That number is up from 4.4% in 1993. This does not even consider the issues of narcotics trafficking and the unlawful presence of pedophiles within school grounds

According to *The New York Times*, nearly 1,000 new public schools opened in 2002 and 75% of them were equipped with surveillance cameras. This is not a question of whether or not video surveillance should in the schools, but a question of how and when.

Reality within the education institution

There is not a school system in this country that is not facing budget limitations and scrutiny on how the budget is being spent. Increased security, albeit a common desire by faculty, parents, and students, typically represents a cost that traditionally hasn't been fully accounted for. MTS believes there are ways to leverage other technology investments in schools to improve security through the careful design of the Digital Video Surveillance (DVS) architecture and the application of key technology.

Related to budget constraints are limitations within the administrative structure. Many schools do not have dedicated security personnel available to monitor schools via video surveillance technology full time. Even those schools that do have dedicated personnel typically are in large schools with thousands of children and multiple buildings. How can

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

we expect these individuals to watch everything, even with adequate surveillance camera coverage?

Many of these incidents are virtually undetectable. Schools face two forms of security threats – internal and external. Internal threats stem from within the school grounds, and from either students or faculty. Depending on the school grade, this can range from schoolyard fights to more violent acts for the older grades. External threats occur when individual(s) who are not permitted or authorized on school property transcend the perimeter and threaten our children and teachers. Typically, this can be threats from narcotics trafficking, pedophile assault, or violence from outside individuals. Finally, infrastructure security is both a growing concern and cost and ranges from vandalism to theft and destruction.

Possibly the most valuable element of video surveillance in schools is deterrence and reassurance. The mere presence of cameras and the understanding that wrongful acts will be punished may deter a significant number of events from happening. Likewise, knowing that something is being done about it creates a sense of reassurance in students, teachers, and parents alike.

Why Video?

The timely exchange of *current, relevant, and accurate* information is an essential component to safety and security. Historically, the more detailed and timely the information is the more informed security personnel, administrators, and law enforcement personnel responsible for the protection of people and infrastructure become. This enables a more effective prevention or response to a safety or security incident. Whether it's providing the police information to apprehend schoolyard drug deals or helping administrators discipline violent students, information is the key.

2.2 Video Surveillance Evolution – Technology changes and updates

There are several choices when considering surveillance technology. Foremost, we believe in establishing a surveillance architecture. An architecture serves as a blueprint from which school systems can build their surveillance systems. We fully recognize that video surveillance technology is rapidly changing – more capable systems at more affordable prices. It would be foolish to deploy a solution that is product-based and does not take into consideration the evolving technology within the surveillance industry. With an architecture, we can tie the requirements – including the threats and vulnerabilities associated with the schools – to the solution. Understanding the threats and vulnerabilities the schools face are only a part of the requirement process. Understanding the vision that communities may have in establishing an enterprise architecture, understanding the policing policies and finally, understanding how the organization would administer and manage such an architecture, are all critical components that need to be taken into consideration when developing that architecture.

Future-proofing

With such a rapidly developing technology as Digital Video Surveillance, it is important to incorporate within your architecture the ability to adopt technological advances as they become more cost effective and more mission-critical. MTS understands where DVS technology is headed and, as such, we recommend including provisions for those advances within your architecture: Some high-level recommendations for future-proofing include:

- Using CAT5e/6 cabling for all new cameras. Internet Protocol (IP) cameras are not only available now but 75% of the R&D associated with cameras are focused on IP cameras and intelligent cameras. Regardless, at the time of this paper, the price points and technological edge still lie with analog (NTSC) cameras. However, by developing the infrastructure with CAT5e/6 cabling, schools can adopt IP cameras at any given time without any additional costs – cables can be easily converted to Ethernet and incorporate Ethernet switching.
- Solutions based on network video recorder technology (NVR) – not digital video recorder (DVR) technology. Although somewhat transparent to the end user, NVRs

represent a more open solution, utilizing standard computers and networks. Software can be hosted on any computer technology, can be easily upgraded, can scale both horizontally (adding servers) and vertically (upgrading servers), and does not include costly proprietary maintenance fees. DVRs are essentially computers, but the proprietary nature of them make them very costly and limited for any upgrades, scalability, and flexibility in configuration. Additionally, in the evolution of video surveillance, network video recorders represent where the technology is now and also where it is headed. DVRs, although still very popular, represent a technology phase that has already been surpassed. Due to the extremely profitable aspect of DVRs – both in installation and in maintenance – they are still recommended by many integrators. The diagram below illustrates the evolution of video surveillance. Moving from left to right, surveillance architectures have evolved from tape-based recording formats, to proprietary, closed DVR formats, to open architecture NVR formats, with multi-format cameras.

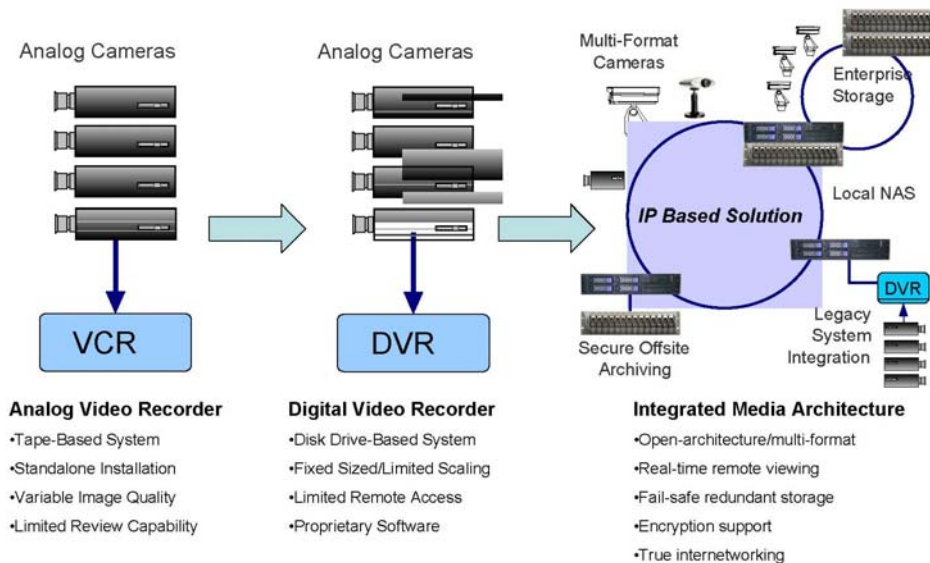


Figure 1 - Evolution of Video Surveillance

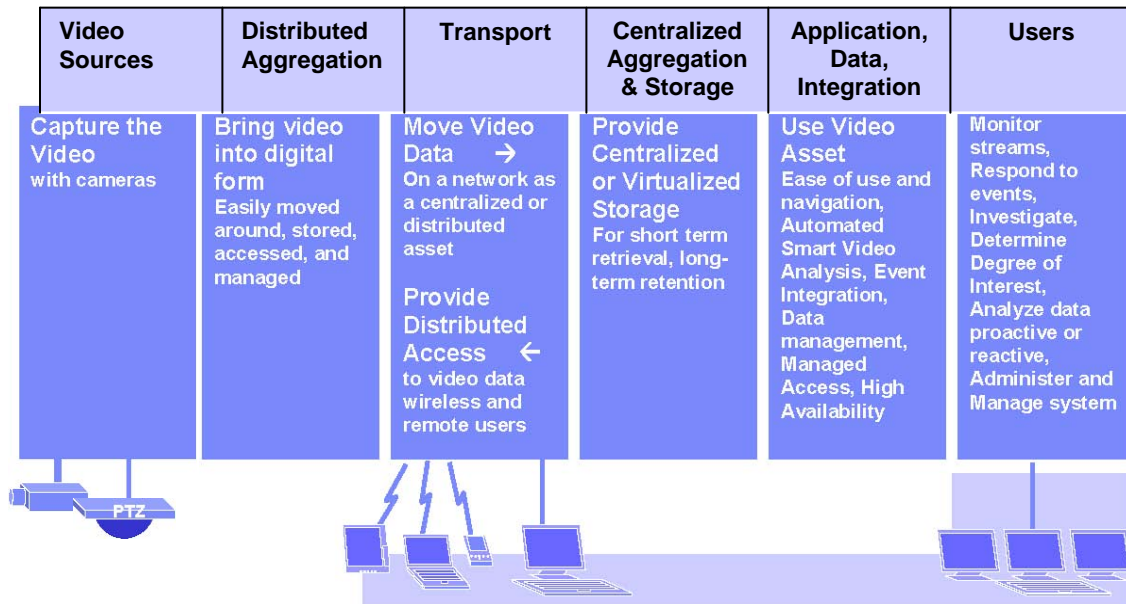
- Multi-format cameras, storage, and access solutions. We recommend server technology that supports both IP based cameras and NTSC cameras. These solutions allow for storage within the server, within the network or within any computer peripheral. We recommend solutions that include the ability to view and *manage* the system from anywhere within the architecture. Since software-based solutions are

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

based on Commercial Off The Shelf (COTS) computer systems, technology such as RAID, NAS, and refined processes for systems management can be easily and affordably applied. Similarly, upgrades (more storage) are trivial as these are not proprietary DVRs - they are computers. With the ability to currently support IP cameras, schools can easily add a camera location anywhere they have an Ethernet location, without any integration effort. This would be particularly useful for special functions such as graduations, assemblies, or sporting events.

- **Bandwidth Management.** Because many towns have multiple schools and the need to link police to schools, connections between schools, and between schools and other municipal entities is essential. These connections can be made over a varied means of ever-evolving communications. Internet connections (DSL, Cable modem, etc.), Intranet (township owned communications), WiFi (future), wireless broadband, etc. are all viable communication means for which the video or alarms will traverse. We recommend solutions that follow a loosely coupled architecture – i.e., each architectural component is somewhat independent of the next. The capture (cameras) is independent of the transport (network) which is independent of the processing (server/NVR) which is independent of the storage. As such, schools can adopt whatever network is feasible and available for any component of the solution. The diagram below illustrates the concept of uncoupling architecture components



- **Software-based solution.** We recommend solutions that are based on software and as such, several advantages can be realized. Upgrades are trivial and cost effective. Since the architecture is software based, upgrades typically do not include hardware upgrades and, as such, are much more cost effective. Also, with a software-based solution, costly, proprietary ‘black boxes’ are avoided, reducing overall maintenance fees. Schools would not be tied to any hardware and can add or upgrade independent of any one hardware solution. We recommend solutions with virtually unlimited scalability. Any number of cameras can be added – there is no limit. It is favorable

to have one unified solution, that is, it is one single system – distributed over as many servers (or schools) as it makes sense. However, all databases within each server should be synchronized to an overall enterprise architecture, which allows for any client to see any camera from any location. This is a single, structured management environment, and a single entity from which to build upon. We recommend server solutions that typically achieve a greater port density (number of cameras per unit) than DVRs and can take advantage of dual processor technology and higher order processor technology (64 Bit). As advances in servers and operating systems continue, each new server added to a school's growing architecture can take advantage of those advances, which typically reflect higher performance and lower cost. At the time of this writing, some popular, current DVRs on the market are still using Pentium 1 processor technology while dual-core Pentium 4 technology is the standard in desktop computing.

2.3 Security Policy Role and Development

Video Surveillance should be viewed as a technology-based tool which automates and carries-out school security policy – it is not a replacement for security policy. Policy, including processes and procedures, needs to be somewhat independent from the technology used to automate and execute those policies. It is important to understand that policy must be independent of the organization of who is to carry out that policy and in turn independent of the technology used to automate that policy.

EXAMPLE: If the school security policy stipulates that no one is permitted in the school after 9:00 AM unless they check in with the front office, then the policy can be executed as follows:

1. *Access is controlled at 9:00 – **Policy***
2. *School Security Custodian locks the doors at 9:00 – **Organization***
3. *Door sensors or cameras signal an alert of when a controlled door is opened and that alert is sent to Security Custodian – **Technology***

It is vital to establish the policy and procedures prior to procuring the video surveillance system. Policy and procedural requirements may dictate system requirements from which the procurement is evaluated on. Assistance on developing security policy for schools can, in part, be found at: <http://www.ncjrs.gov/school/state.html>

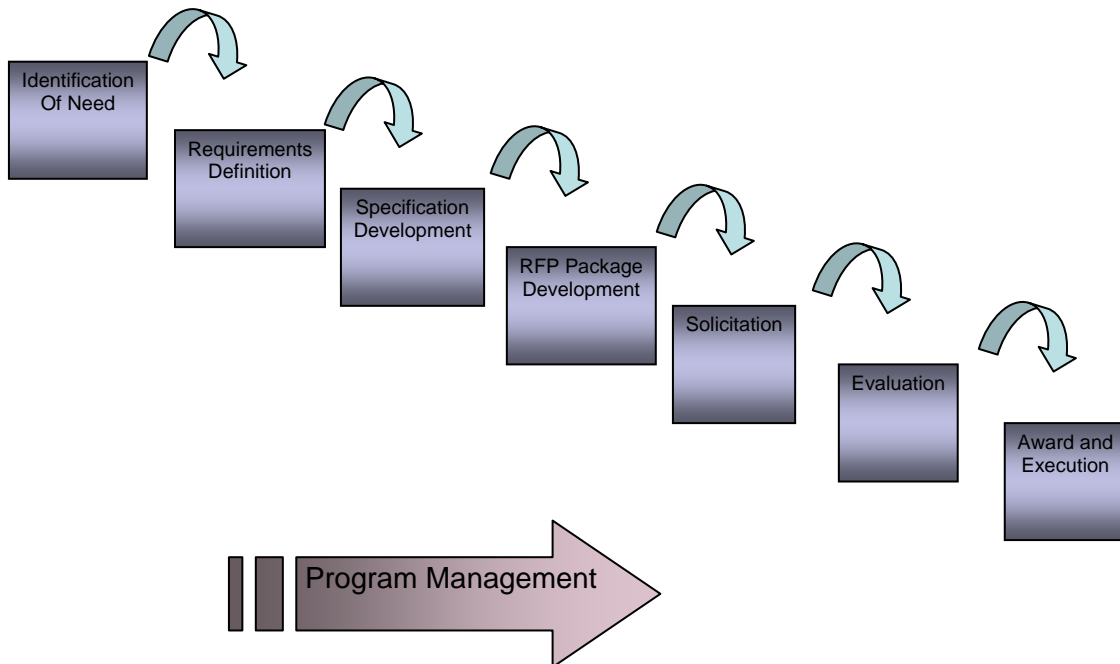
3.0 Request For Proposal (RFP) Recommendations

Each school facility/district has its own procurement policy and procedures. This document is not intended to conflict with or replace those procedures. This section is intended to suggest recommendations on how individuals in charge of evaluating and procuring a video surveillance system can differentiate between multiple proposals.

One important consideration in the procurement process is the source of funding. In many instances, grant programs can assist educators in offsetting costs associated with video surveillance solutions. Federal, State, and local/private grant programs may support the integration of video surveillance technology within the school system. As such, it is important to understand the procurement and policy guidelines and requirements of the corresponding grant to ensure proper procedure is followed and adhered to. Examples of applicable grant programs include NJ DCA SHARE (Sharing Available Resources Efficiently) program and the Department of Justice's COPS (Community Oriented Policing Services) program.

3.1 Organizing the RFP Process

Within the guidelines of your school's procurement policy, it would be beneficial to lay out the entire request for proposal process.



Procurement Process

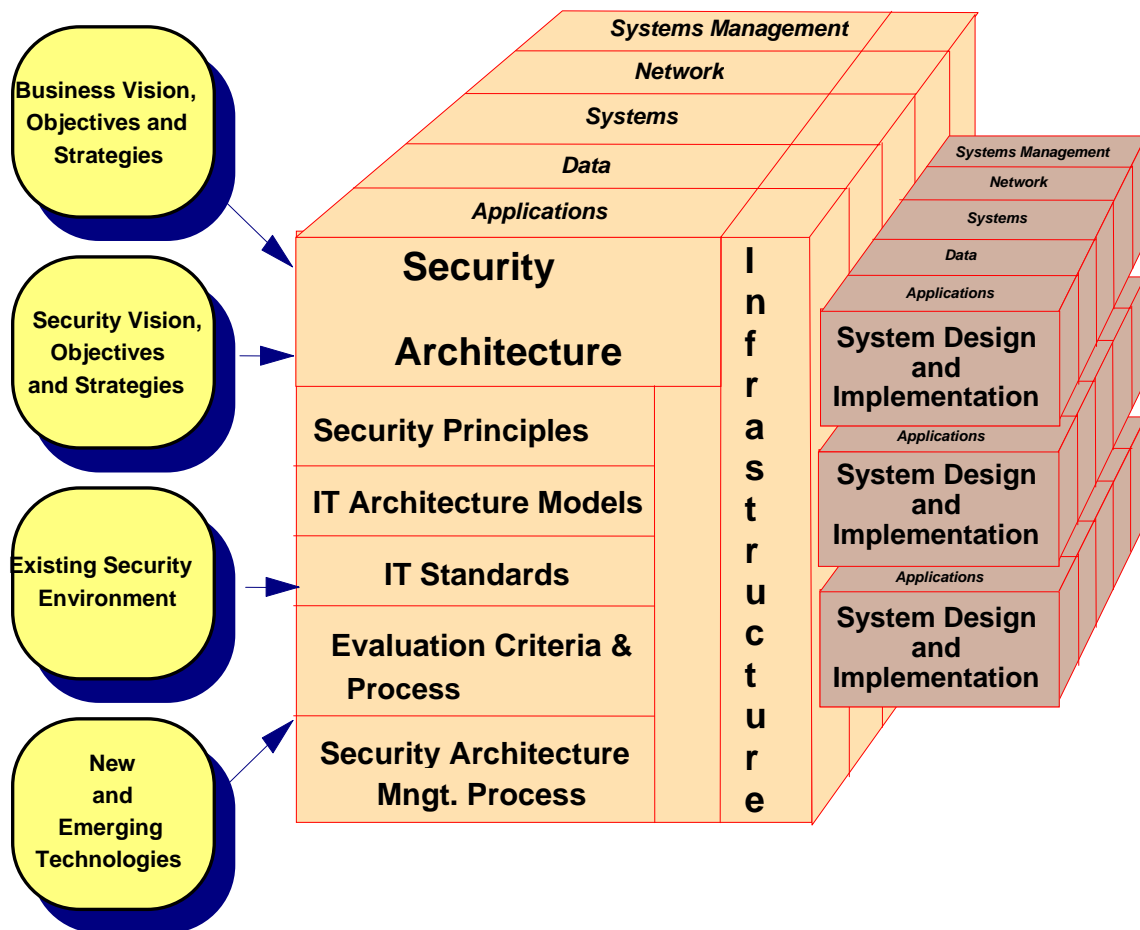
The steps most educators tend to need help in is the specification development through evaluation steps. This paper will focus on those areas.

3.2 Process Recommendations

In this section, we will choose several key processes and provide recommendations and examples on how to execute those processes.

3.2.1 Requirements Process

Since the solution being procured is actually part of an architecture, it is important to tie in the requirements to the architecture up front. This ensures the requirements are accounted for in the final solution selection. This process can be as formal or informal as feasible, based on knowledge, urgency/timeliness, and prior experience.



Examples of school surveillance requirements fall into multiple categories, including:

Threat and Vulnerabilities

- Internal threats
- External threats
- Infrastructure vulnerabilities
- Organization vulnerabilities
- Process vulnerabilities

Policy Enforcement – Functional Requirements

- Access Control – using surveillance to identify and log visitors to the school facility and/or students/teachers to the school
- Access Control enforcement – using surveillance to enforce access control policies such as door closure/locking, off limits areas, etc.
- Deterrence
- Identification of wrongful incident – bullying, fighting, stealing, assault, etc.
- Identification of individuals not permitted on school grounds
- Enforcement of parking policies
- Alerting and alarming of incidents
- Forensics of events for discipline and prosecution
- Assistance for resource officers
- Alerting police
- Crowd monitoring (e.g., stadium events)

Technical Requirements – System requirements

- Ability to identify individuals, not just incidents
- Ability to view/monitor from multiple locations
- Ability to provide evidence
- Ability to evaluate video post-event
- Ability to work within existing IT and security infrastructures

3.2.2 Specification Development Process

Video surveillance and associated technology is a rapidly developing technology. As such, it is important to allow for technology advances and improvements in system design. With that, educators should avoid specifying brand-specific technology, but rather indicate capability, performance, and feature requirements. Although this may appear to be more work up front, the end result is a more open and competitive procurement process and a system that is designed around school security policy and needs instead of security policy developed around system capabilities or short-comings. Section 4.0 of this document provides for an example of an open-system specification for a school surveillance system.

Of equal importance when developing the technical specifications of the system itself, educators need to take into consideration the following other specifications:

- Functional Specifications – how the system shall perform and what features it shall have
- Program Execution specifications – how the awarded integrator shall perform including, but not limited to:
 - Program Management
 - Program Reporting
 - Scheduling
 - Testing
 - Quality Assurance
 - System Turnover
 - Training
 - Calibration
 - Maintenance
- Integrator specifications – how the system integrator demonstrates an understanding of the entire requirements process – from threat and vulnerability to system management
- System Management specifications – how the system shall be administered

3.2.3 RFP Package Development Process

The majority of items within this process are governed by a school's existing and established procurement policy. However, this section will focus on one particular area – evaluation criteria. Since we recommend the specifications NOT to identify brand name equipment, it is important to establish a process to evaluate and rate individual proposals against stated specifications. We believe a simple yet disciplined procedure can be applied to help in evaluating proposals.

Creating a point system. Whether or not actual numerical value is assigned to a particular evaluation criteria is not important – it can be quantitative or subjective. What is important is understanding when a proposal is meeting, not fully meeting, or exceeding (adding value) to a specified criteria. Simply exceeding a technology criteria does not necessarily equate to adding value. Also, all criteria must be evaluated with respect to cost. An example would be in video storage time. If the specification requires 2 weeks recording time for all cameras (a reasonable requirement for schools), then an integrator who provides 30 days at no additional cost is considered providing value while an integrator who provides one year on-line for a 75% cost increase is not.

It is important that the RFP requirements request integrators to demonstrate meeting, exceeding, or not meeting a particular requirement. They should be required to stipulate HOW they meet/exceed/not meet a requirement in words (simply stating “meeting requirement” should not be sufficient). Also, when exceeding, the integrator should be

required to explain the ‘value to the school’ and when not meeting, the integrator should be required to explain the ‘impact to the school’ and, if any, what alternative approach or technology is proposed.

Finally, good organization of the specification helps in establishing an easier evaluation process.

EXAMPLE: Specification – Bandwidth Management

The system shall be capable of providing bandwidth management for remote viewing (40 points)

- a) The system shall provide for variable frame rate (fps) selection on selected viewing (10 points)*
- b) The system shall provide for variable compression selection on selected viewing (10 points)*
- c) The system shall provide for varied bandwidth management, depending on viewing priorities (10 points)*
- d) The system shall provide for varied bandwidth management, depending on a time schedule engine (10 points)*

3.2.4 Solicitation

One consideration regarding the solicitation is to possibly provide a pre-screening process to help lessen the unqualified bids received. An example could be soliciting a pre-bid acceptance criteria survey to help narrow down the field.

One important decision that must be made is site survey/walkthrough. There are two approaches that can be followed. One approach is to have all potential bidders visit a site survey to perform a walk-through of the facility and let them decide on the number of and placement of cameras for a facility. They should be required to identify the camera, what it is viewing, what it is protecting against (requirements), and the type of camera. The other approach is for the specification to identify a nominal number of cameras (based on a preliminary design by the school) and let each integrator bid on the same number of cameras, each within a specified camera group (hallways, perimeter, doorways, common areas, etc). This approach, although a little more effort is required up front, saves a lot of time in the evaluation process and helps to compare “apples to apples”. The reality is, it is not necessary for integrators to do a walkthrough of a facility if a preliminary design is included in the specification and a set of plans indicating distances and access is included. Final count and location can be agreed to post award.

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

Response time. We recommend making the required proposal response time fairly short. It should not take more than one or two weeks to respond to a properly prepared specification. Since you are not specifying brand, integrators should have existing (or readily available) price quotes on equipment they are familiar with and need not to wait for quotes. Also, keeping the response cycle short helps weed out prospective bidders who are not familiar with providing surveillance systems to the education community.

Q&A. It is recommended to allow for a question and answer process within the proposal response cycle. Integrators may think of questions overlooked by the specification development process that may be critical to the overall success of the program. The process should be simple, one time, timely, and of open format.

3.3 Example Scoring Techniques

EXAMPLE rating system that can be applied.

Not Meeting Requirements – a proposal does not include the capability/feature required OR does not indicate it provides the capability or feature. Also, an indication of by how much the proposal falls short of the requirement (if applicable) shall be made and an explanation of the ‘impact to the school’ shall be made. If applicable, any alternative technology or feature should be indicated.

Meeting Requirements – a proposal technically or functionally meets the requirement

Exceeding Requirements – a proposal technically or functionally exceeds the requirements, an indication of how much it exceeds the requirements by (if applicable) shall be made and an explanation of the ‘value to the school’ should be made

A point system can be assigned to this process, if deemed appropriate and then tallied for easy ranking. In some instances, procurement officials may assign a dollar value to each requirement, then when understanding the requirement relevant to cost, it can be easily matched.

EXAMPLE: Point System.

The desired requirement is for a surveillance system to send an audible alarm should there be motion detected after midnight inside a school. In

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

developing the specification, the education institution determines that this is a 'nice to have' feature, but not a 'must have' feature. As such, they assign a dollar value of \$1000 to this requirement. Proposals that include this feature (meet) are awarded the \$1000, proposals that do not (not meet) are assigned a \$0 value and proposals that can do this either via email, phone, SMS, page, or alarm to police dispatch are given a \$1500 award. In the end, when comparing pricing, the award pricing is compared to the actual pricing to determine best value.

4.0 Specifications

Technology Specifications

MTS recommends video surveillance systems that protect the education institution from:

- Proprietary, closed solutions
- Solutions with costly upgrades
- Limited scalability solutions
- Hardware-specific solutions

With those objectives in mind, this section of the document provides for a sample specification for a video surveillance system for public education.

General Guidelines. Integrators are required to respond to each stated requirement in the specification and indicate whether their solution meets, does not meet, or exceeds the requirement. Integrators are required to indicate as to what extent they meet the stated requirement, and, when exceeding the requirement, indicate what the value or benefit is to the school. When alternative approaches are being proposed, integrators are required to state such, and are also required to demonstrate how the alternate approach meets the stated requirement. Integrators are also encouraged to indicate additional capabilities, not stated in the requirements, which they deem of value to the school and must provide detail as to that stated value.

System Specification

4.1 Digital Video Recorder/Network Video Recorder

The digital video recorder (DVR) shall be based on a software-based solution. That is, it shall be software and/or hardware that can be hosted on a standard Information Technology (IT) Commercial Off-The-Shelf (COTS) computer. Integrator shall indicate portability to different manufacturer standard computers.

4.1.1 DVR Hardware.

Integrator shall indicate proposed computer specifications including:

- Processor speed and family
- System memory included and expandability
- System hard disk drive(s) included and expandability
- System graphics engine (card), including memory (if applicable)
- Systems optical drive capability and format
- Ability to support computer technologies such as:
 - RAID

- NAS
 - Hot-Swop drive technology
 - Systems Management (including SNMP)
- Indicate what, if any, upgrades are available to the proposed DVR system including:
 - Operating System
 - Application Version
 - Processor(s)
 - Memory
 - Storage
 - Other
- Ability to be hosted on an industry-recognized operating system (e.g. Windows or Linux) in native format
- Indicate networking support, including speed, format, and redundancy
- Port Density. The integrator shall indicate the DVR's port density. The integrator shall indicate the proposed number of cameras (channels) that the DVR supports and the limit of cameras/channels that the DVR can support. If more than one DVR is required/proposed, the integrator shall clearly indicate how the multiple DVRs communicate with each other, how they are viewed/monitored from a single application with a single logon/access, and how they are administered/managed from a single management point.

4.1.2 DVR Features/Functions

Access. Multiple DVRs that require multiple logons/access to view and/or manage are not acceptable. The integrator shall indicate how upgrades/modifications to the DVR(s) shall be made.

Alarm/Event Based. School security personnel are typically not in the mode of monitoring cameras. The video surveillance system should be configured to accommodate security policies and processes. As such, with the use of schedules, zones, and rules, alarm and alerts may be programmed into the system whenever possible to avoid 'monitoring' and increase 'alerting'. The integrator shall indicate how the DVR software can provide for alarming (such as motion detection) and how they alarm shall be transmitted. If applicable, the integrator shall indicate how the system can apply security rules to the alarming process.

Internetworking. The integrator shall indicate networking format, (e.g., TCP/IP standard networking) between cameras, servers, and clients. The integrator shall indicate what, if any, bandwidth management techniques are incorporated into the overall system. That shall include the ability to match the video stream to the appropriate available bandwidth. (some schools may have varying networking access and as such, appropriate adjustments shall be made to the method of access to the system).

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

Video Export. To aid in prosecution and discipline process, video recording software must be able to export video and still frame images to a industry standard format (such as AVI). The integrator shall indicate the format for creation of optical disks

Multi-format camera support. The integrator shall indicate the proposed DVR's ability to support the following camera formats: NTSC, PAL, and IP cameras (MPEG/MJPEG)

Control support. The integrator shall indicate proposed DVR's ability to support control signals (Pan/Tilt/Zoom) and shall indicate whether this is external (PTZ controller), internal (integrated within software/DVR), or both.

Fault Tolerance. The integrator shall demonstrate the system's ability to recover from power outage automatically (application load on power reboot) and the ability to recover upon disk corruption (full backup on separate disk). Video, O/S, Backup, and Audio should not be stored on the same disk drive

Archiving. The integrator shall demonstrate the ability for the system to easily provide archive capability in either compressed or uncompressed format, preferably selectable by the operator on a per-camera or per time segment basis

Scheduling Capability. The integrator shall indicate the DVR's ability to create policies within the system to have the ability to operate under different rules during different times of the day, different days of the week. This is important in both bandwidth management, and alarming/alerting. This is also important when police are involved in monitoring (police may only monitor off hours vs. full time)

Upgrade Costs. The integrator shall provide for upgrade cost estimates that meet the following criteria:

- Number of Cameras/channels. Cost indications shall be made for future upgrades for 10%, 25%, and 50% growth in number of cameras and shall include line-item specific costs for:
 - Wiring
 - Camera cost/installation
 - DVR channel cost
 - Additional DVR costs, if applicable
 - Licensing costs, if applicable
 - Labor costs
- Number of clients. Cost indications shall be made for future upgrades for 10%, 25%, and 50% growth in number of viewing and administrator clients and shall include line-item specific costs for:
 - Software/Licensing costs, if applicable
 - Hardware costs, if applicable
 - Labor costs

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

- Number of remote viewing and/or management clients. Cost indications shall be made for future upgrades for 10%, 25%, and 50% growth in the number of remote viewing/management clients and shall include line-item specific costs for:
 - Software/Licensing costs, if applicable
 - Hardware costs, including networking devices, if applicable
 - Labor costs

Intelligent Features. The integrator shall indicate the proposed DVR's ability to accommodate any intelligent features and how this would be accomplished. If any development is required, then that shall be indicated. Examples of intelligent features include:

- Face Detection
- Face Recognition
- License Plate Recognition
- Object-left behind
- Fighting/Rioting
- Crowd Gathering

External messaging support The integrator shall indicate DVR's ability to support messaging/alarming to the following formats:

- Pager
- Cell phone
- Telephone
- SMS
- MMS

Image Enhancement. The integrator shall indicate the DVR's ability to support image enhancement techniques and to what extent (e.g., digital zoom, 10X). The following are examples of image enhancements:

- Digital Zoom
- Contrast adjustment
- Brightness adjustment
- Color adjustment
- Motion detection adjustment (if motion detection is built within the DVR software, then the integrator shall indicate if it is adjustable/tunable to be able to limit the size of the object detected and/or the amount of motion detected). If applicable, the integrator shall indicate if the ability to mask motion detection is present.)

4.2 Cameras

Camera and Lens selection

- Flexibility in selecting cameras to include PTZ and fixed, indoor and outdoor, vandal-proof, low-light, etc. This is also important to be able to use different (and

appropriate) lenses. Greater distances can be accommodated via larger telephoto lenses (such as 100mm) where wide areas may need wider viewing lenses (2.8mm) and aspherical lenses. This also includes Auto Iris lenses for outdoor, fixed and electronic shutter. Bottom line is all lenses are not for all applications.

- Cameras shall have the minimum capabilities, regardless of enclosure/housing selection:
 - Minimum 480 Horizontal Lines Resolution (HLR) color
 - Minimum 520 HLR black & white
 - Day/Night capability of auto switching to black & white under low light conditions
 - Auto Iris feature for outdoor or areas where there is a wide range of lighting
 - Backlight Compensation (BLC) settings available
 - Low light sensitivity for cameras that must operate in unlit or poorly lit areas (<.05 lux)
- Enclosures. Where vandal proof enclosures are desired, then they shall be such that they can absorb and withstand mechanical shock. All outdoor enclosures shall be weatherproof in accordance with IP67 standards. For extreme conditions, outdoor enclosures shall have heaters, blowers, and defrosters to maintain camera temperature and humidity. Where possible, consistency shall be made in enclosure selection.
- Camera selection. Integrators shall indicate whether they are proposing fixed or PTZ cameras. If PTZ cameras are proposed, then integrators must indicate how full coverage will be achieved and what is the rationale for using PTZ cameras vs. fixed. Integrators shall also indicate what type of enclosures and mounts are proposed in particular areas

4.3 Wiring/Cabling

The integrator shall utilize Video over Unshielded Twisted Pair (UTP). Baluns shall be used to match the cable resistance to 75 ohms. Separate leads for power should be utilized for excessive distances and/or outdoor enclosures. Integrator shall indicate when separate power leads are being used (at what distances) and what wire gage leads. Integrator shall indicate, what, if any, growth is accommodated in the wiring plan. Integrator shall indicate any wiring formats/guidelines followed, including, but not limited to:

- Labeling and labeling format
- Pull stress/strain
- Curve limitations
- Dressing. How the cable ends shall be dressed
- Stress relief
- Cable hooks, cable trays, or other cable passageway infrastructure proposed
- Maximum cable distances
- Termination type and method

4.4 Implementation

4.4.1 Project Management.

The integrator shall indicate what project management activities are included with their proposal. This shall include, but not be limited to:

- Project Plan
- On-site Project Manager
- Schedule
- Project Reporting
- Project Meetings
- Approval process
- Change process
- Acceptance Criteria
- Turnover process

4.4.2 Installation Practices.

The integrator shall indicate their installation practices and procedures, applicable to video surveillance. Integrators are encouraged to include adherence/conformance to any industry standards, demonstrate any knowledge in best practices for this installation, and provide any illustrations or pictures of previous installations or diagrams of proposed installations. This shall include, but not be limited to:

- Camera Mounting. This shall include working with masonry, metal, wood, and drop ceiling grids
- Cable installations. This shall include working with trays, raceways, hooks, plenum vs. non-plenum, labeling, and wire routing. This also shall include bends, pull force, and other industry-standard best practices
- Conduit work. This shall include indoor, outdoor, wire molding, and any other required conduit work.

4.4.3 Scalability.

Ability to grow without penalty. Integration should be designed such that the system can be built in multiple phases or all at once. The cost between the two should not be very different at all. The integrator must indicate how the system can be built in n phases evenly over 2 years and show the cost differences in doing this in n phases or all at once.

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

- Support for future – Expansion. Ability to add schools, cameras, clients, or features without any changes to the core enterprise architecture. The costs to add these features shall be determined within the context of this proposal, per section 4.1.2 Upgrade Costs. The integrator must indicate what are the limits in hardware, software, and licensing of the proposed system and what the process, hardware, software, licensing and costs would be to expand the system. This shall include additional schools, cameras, viewing clients, and any features.
- Technology changes/updates. The integrator shall indicate the ability to add/modify components of the architecture. This includes, but not limited to:
 - O/S updates
 - Application version updates
 - Server updates
 - Networking updates/additions (e.g. The addition of wireless)
 - Storage updates
 - Intelligent features
 - Video format changes
- New Features and capabilities. Integrator shall indicate the system's ability to grow in capability as these become desirable and affordable

4.4.4 Head-end standards and best practices.

Video surveillance is analogous to a data system in that it is a large investment and represents mission critical infrastructure. It is also vulnerability to the same system management issues as IT. Wiring, termination, labeling, cable management, system documentation, change management rules, etc are all important criteria for integration design and selection. Integrator shall indicate their approach and design for the head end components. Integrator shall show rack elevation diagrams and indicate what components constitute the head-end. At a minimum, the system shall have the following head-end characteristics and capabilities:

- Rack-mountable components (19" rack)
- Centralized, rack mountable power supplies with separate fuses
- Any patch panel components proposed
- Any UPS system(s) proposed
- Any backup/archive system/capability proposed
- Any server keyboard/monitor/mouse proposed
- Any PTZ control systems proposed
- Cable Stress management system proposed.
- Cable labeling for head end
- Conformance to any standards (e.g., EIA 568a)

4.4.5 Lighting considerations

Lighting is one of the most critical issues in camera/lens selection and camera placement. It is important that the integration design takes into consideration all hours of surveillance (especially outdoors) and all possible lighting conditions. Selection of which direction cameras are aimed, angles, and other integration criteria are all important factors in overcoming lighting issues. Low-light cameras, manual/electronic shutters, Auto-iris, Back Light Compensation (BLC), and filters are all effective tools that can and should be used to maximize the viewing capabilities of a camera. Integrator shall indicate their approach to compensate for varied lighting conditions either as a broad statement for a group of cameras, or for any specific cameras.

4.4.6 Lensing- the ability to use video for discipline and prosecution.

Many video surveillance integrations are focused on area of coverage per camera rather than specific coverage within an area.. For schools, one of the primary functions required of the video surveillance system is to aid in the analysis of events and provide evidence that can be used to discipline or prosecute individuals who perpetrate those events. With that, there are several very important factors to achieve this. The integrator shall indicate the proposed system's ability to perform the following:

- The ability to recognize the individuals (surveillance that provide face identification)
- The ability to rapidly search multiple cameras for common criteria
- The ability to provide the video in an easy to read (e.g., CD) and open format (e.g. AVI), such that others who need to view the video do not have to have proprietary systems
- Design such that the recording of the video can be adjusted to capture pre and post motion detection

4.4.7 Documentation.

Design documentation should be provided prior to agreement/commencement of integration. The integrator shall indicate their approach and ability to provide all required documentation. The design documentation shall detail all the features/functions of the system, identify the threats and vulnerabilities that the system is intended to counter, and identify specific standards, camera placement/type, cabling considerations, etc. This should form the basis for the design document/agreement. After installation, 'as built' documents should be provided that cover:

- Physical layer installation (cable, cable labeling scheme, rack-level diagrams, and physical plant layout (camera locations, numbering))

- Logical layer installation (addressing, VPN associations (if applicable), host naming conventions)
- Software layer installation (configuration of servers, clients, etc)
- Training Documentation
- User and Administrator manuals

4.4.8 Training

The integrator shall outline their proposed training program for the installed system. This should include descriptions of hands-on training, training materials, indication of number of students, and different types of training (user vs. administrator). Any additional help features should be described at this point. The integrator must describe the timeframes for training relevant to system turnover.

4.4.9 Other - Integrator Specifications

The integrator shall demonstrate, in writing, the following understandings. Where possible, integrator shall indicate such as it relates to this installation and indicate what, if any, experience they have in the specific understanding areas:

- **Understands Security Policy.** The DVS system is to help enforce security policy. Integrator should possess and demonstrate an understanding of security policy development, administration, and execution
- **Understands security model.** The integrator should demonstrate an understanding of how the school might administer their security policy, how security personnel fit within this policy and how they would use the security system. This includes demonstration of how administrative rights would be configured in the surveillance solution. Integrator shall provide an example scenario.
- **Threat and Vulnerability understanding.** The integrator should demonstrate an understanding of the differences between a threat-based system and a vulnerability-based system and should indicate example generic threats and vulnerabilities of school environments including the differences between the different grade levels and geographic variants applicable to the school(s)
- **Value of deterrence and re-assurance.** The integrator should demonstrate an understanding of the value of deterrence as applicable in a school system and shall indicate what activities can be used to increase the effectiveness of deterrence.
- **Understands policing policy.** This helps with any law enforcement relationships. Video surveillance is a key component in policing at schools and it is important that the integrator demonstrate an understanding of how police use surveillance to help in prosecution of offenders, command and control response to incidents, and in the provision of evidence. Integrator shall demonstrate this understanding by including an example scenario for police involvement in this proposal.

4.5 Maintenance.

The integrator shall warrant the system for one year after installation. This shall include parts and labor. The integrator shall propose maintenance options for the out years and provide options for hardware, software, and labor.

4.6 Costs.

The integrator shall provide the cost for this proposal all inclusive. The integrator shall provide an equipment list of all items being provided under this proposal, with brand and model number (where applicable), and quantity. Major hardware and software items shall have a cost breakdown in the following format. It is important that all components needed to make a line item operational, be included. For example, if the DVR is composed of DVR, Monitor, keyboard, mouse, and operating system, then all those items shall be included in the price for the DVR line item. Integrator shall indicate how long pricing is valid for.

Item	Inclusive	Manufacturer	Model	Quantity	Cost
DVR	Monitor, keyboard, mouse, o/s	XYZ	123	1	\$5,000
Outdoor Camera	Camera, lens, housing	XYZ	123	1	\$500
19" Rack	Locking doors, hardware, casters	XYZ	123	1	\$500
Video Cable	Terminations, handing hooks, labels	XYZ	123	<i>N</i> feet (estimate)	\$600

5.0 Glossary

Here are some terms as they are related to video surveillance.

Alerting – In a video surveillance application, this would be creating alarms or alerts to events as opposed to monitoring video. It is much more effective to be notified upon an event then to watch for it.

Auto Iris – This refers to features in both cameras and lenses where a motorized iris is controlled by logic based on the amount of available light and conditions where varying light require an adjustment to the iris. Most typically used in outdoor settings and day/night environments.

AVI – Abbreviation for Audio Video Interleave – it is an industry standard that incorporates both audio and video formats, synchronized as one. Can be viewed/listened to with Windows standard media players, eliminating the need for proprietary media players to view video.

Back Light Compensation (BLC) – The ability for a camera to adjust the lighting by applying logic. Typically, most cameras have centered BLC where the center of the view is the subject and the surrounding area has excessive light. The BLC logic normalizes the light input such that all viewing areas achieve a consistency in light.

Baluns – A device, used in pairs, to change the resistance of an UTP cable from 100 ohms to 75ohms, which is optimized for video. There are passive baluns and active baluns and these are basic transceiver/receiver functions that allow for the use of video over UTP.

Bandwidth – In a video surveillance application, this would be relevant to the amount of network capacity or bandwidth that either the video stream from camera to DVR/NVR needs or the amount of network capacity that the video stream from DVR/NVR to viewing client would need. This is a key factor in complex systems with remote viewing, especially those that use common network medians such as the internet. In a digitized network, this can be measured in bits per second (bps) and can be bursty or steady-state.

Calibration – In a video surveillance application, this would relate to the adjustments needed for cameras, which include zoom/wide settings, iris, shutter speed, BLC, focus, and aiming. For the NVR/DVR, this could include frame rate settings, image acquisition settings, bandwidth settings, etc. In general, these are the adjustments needed to make a video surveillance solution optimized. Systems may need some level of recalibration throughout their lifecycle, but typically, any changes are a result of changing requirements or encountering different environmental settings (varying light conditions)

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

CAT5e/ CAT6 – Category 5e or Category 6 data cabling. It's application in a video surveillance application would be with the application of video over unshielded twisted pair.

Compression – This pertains to techniques used to compress recorded video real time to help reduce the bandwidth and storage requirements for a system. Although there are emerging industry standards for some type of video, there really isn't solid standards agreed to for surveillance systems. This also depends on video format selection. What is important is to choose systems that allow user selection of compression settings, such that the system can be optimized. Typically compression includes: wavelet, delta wavelet, MPEG, etc

COTS – Commercial Off The Shelf – this refers to equipment that can be purchases from multiple sources. In the context of this document, it refers to desktop or servers computers that can be purchased from virtually anywhere and that run standard operating systems (e.g., Windows or Linux)

Digital Video Recorder – A proprietary device that encodes analog video, digitizes it, and stores it in a database. Typically, this is a self contained device with disk storage, operating system, and a finite set of features. The DVR is the replacement for the VCR, which was an analog tape based system.

Digital Video Surveillance – In general terms, this pertains to the technology or business of using digital technology to accomplish video surveillance. It is the replacement for the CCTV or closed circuit television term.

Digital Zoom – The ability, through software algorithms, to increase the zoom on a video stream (or still image), without the use of changing optics. The limitations typically are in what is called pixilation, where the multitude of little squares that comprise a picture, which are normally not visible to the human eye, become larger and more visible. Different developers use different techniques for digital zoom and there are varying quality differences between them.

Ethernet – Industry standard data networking technology, as described by the standards in IEEE 802.n series.

Frame Per Second – This refers to the frame rate (fps) of video. As applicable here, it can refer to the actual viewed/recorded rate of a particular camera. Full motion video is defined as 30 fps, however, typically video surveillance applications can use frame rates as low as 5-10 fps without much loss. This can also refer to the aggregate capability of a DVR/NVR, whereas the unit has a total frame rate available, that gets distributed over n cameras.

Information Technology (IT) – General context of any information technology system used to process digital data.

Integrated Media Architecture – In general, this refers to the ability to capture, process, store, and distribute data, video, and audio in a common format with common indexing.

Internet Protocol (IP) – As part of the protocol suite, TCP/IP, this is referred to in this document relevant to a generation of cameras where the encoding is performed in the camera, then the digitized video stream is transmitted over a standard IP network, such as Ethernet or the Internet.

Lensing - In a video surveillance application, this would relate to the adjustments needed for cameras, which include zoom/wide settings, iris, shutter speed, BLC, focus, and aiming.

Monitoring – In the context of this paper, this refers to the activities associated with monitoring or watching video real-time.

Motion Detection – The ability for a camera or camera system to detect motion. This is typically accomplished with changes in contrast or, once digitized, changes in pixels. What is of value is the ability to make adjustments (during calibration) to motion detection settings. This is important to eliminate nature motion (small animals or blowing leaves on a tree) from setting off cameras which can either set off alarms or waste hard disk space. Also of value is the ability to mask certain areas from motion detection. This is typically useful in outdoor cameras (or through windows) where adjacent roadways have significant traffic and the camera picks up the motion.

NAS – Network Attached Storage – this refers to network appliances used to supplement storage of servers (or DVRs). These typically are low cost and can be part of an overall IT data system, but used to centrally store digital media, such as video.

Network Video Recorder – The NVR supersedes the DVR in that it has come out of the proprietary box and now is hosted on standard, COTS computers. Typically what you are buying is software and/or an encoder card. The advantages are plentiful but include lower costs, lower upgrade costs, greater port density, and easier to maintain.

NTSC – National Television Standards Committee – in this paper, this refers to the analog video format produced by the cameras, before encoding. – wide spread use in North America

PAL- Phase Alternating Line – in this paper, this refers to the analog video format produced by the cameras, before encoding.- wide spread use in Europe and South America

Port Density – As applied to video surveillance, this refers to the maximum number of cameras/channels that can be attached to a single DVR or NVR. Typically, this is in groups of 8 (8, 16, 32) and typically, NVR achieve a much greater port density than DVRs. It is important to understand the upper limit of the device you are purchasing so you can understand what scalability is built into the acquisition.

PTZ – Pan/Tilt/Zoom – this refers to the capabilities of the camera to have a motorized panning capability (horizontal plane), tilting capability (vertical plane), and zoom (object enlargement). This also refers to the control mechanism and infrastructure associated with controlling the cameras from a remote area. The PTZ controls require additional cabling (in a non-IP environment), and, for some DVRs, require a separate controller. In many NVRs and some DVRs, the control functions and features are included within the software and a separate controller is not needed.

RAID – Redundant Array of Independent Disks – this is a standard IT term, relevant in data environments for storage, and talks to the ability of redundancy and performance. There are multiple RAID levels (0,1,2,3,4,5) and have levels of performance (striping) redundancy, (mirroring), and fault tolerance. What is relevant here is if NVRs are used, then the digital media (video) can be stored in a standard RAID environment, along with other data.

Scalability – This refers to the ability for the system to grow. In this context, this is talking about the DVR/NVR. There is horizontal scalability (adding more servers or DVRs) and vertical scalability (adding more capability to the DVR/NVR). Typically, DVRs are limited to horizontal scalability, although many have external add on features like port expanders and external hard drives. For this context, vertical scalability refers to actual internal expansion, not through the use of external devices.

Security Policy – This refers to a paper policy, that describes what the ‘rules’ are for school security. This typically will define such items as visitor access control, door lockdown, parking, off-limit areas, etc. This can be informal or formal, but forms the basis for which security systems such as video surveillance are implemented. There is a lot available both within the Department of Education and Department of Justice to help administrators with developing formalized security policy.

SNMP – Simple Network Management Protocol – this is the industry standard IT management scheme to help centrally manage IT devices such as network devices, computers, and servers. Devices that are SNMP-manageable would require SNMP MIBs (management information base) resident on that device. If the school has a good IT department and uses SNMP to manage their computers now, it would be beneficial to manage the DVR or NVRs with the same tools.

TCP/IP – Transmission Control Protocol/Internet Protocol – this is the transmission/access protocol widely adopted virtually everywhere and represents a standard for network transmission (commonly found in Ethernet, internet, and other networks). It is relevant here to ensure that the NVR/DVR has TCP/IP support to enable it to connect over standard Ethernet.

Threat and Vulnerability – Threats talk to what is typically facing a school institution – drug dealers, bullies, pedophiles – whereas vulnerabilities talk to a facility’s weaknesses – no fencing, alleyways, etc. In the context of this paper, we talk to threat and vulnerabilities which form the basis for the requirements for a video surveillance system.

MTS Intelligent Surveillance Solutions

Managing the intersection of IT and Security

Unshielded Twisted Pair – This refers to the type of cabling typically used for data transmission and is a series of 4 pair of 23 or 22 gauge wire, twisted in pairs, without a data shield. For this paper, we talk to UTP as it relates to Video over UTP, which has future-proofing and greater performance over traditional coaxial cable.