



## **SCIENTIFIC WORKING GROUP ON IMAGING TECHNOLOGY (SWGIT)**



### **RECOMMENDATIONS AND GUIDELINES FOR THE USE OF CCTV SECURITY SYSTEMS FOR COMMERCIAL INSTITUTIONS\***

**(\*such as banks, convenience stores, and other facilities)**

(Version 2.1 – July 22, 2004)

#### SECTION 1. Purpose of this document:

The purpose of this document is to provide recommendations and guidelines for the use of Closed Circuit Television (CCTV) security systems in commercial institutions such as banks, convenience stores, and other facilities. For the purpose of this document, we will primarily address stationary, unattended cameras and on-site recording devices. The basic principles and recommendations can, in most cases, be applied to any system utilizing closed circuit television cameras and video recorders. This document addresses both analog and digital video systems. The intent of these recommendations and guidelines is to optimize image quality to facilitate the identification of unknown individuals and objects depicted therein.

This document does not specifically address employee theft or other internal security issues, although some of the recommendations can be applied to those problems. Likewise, this document does not address live monitored surveillance systems. References that address such systems are included in Appendix A, CCTV References.

Furthermore, these guidelines are not intended to replace or take precedence over other regulatory requirements in the specific jurisdiction of the establishment to which these guidelines will be applied.

## SECTION 2 SWGIT POSITION ON CCTV SYSTEMS in Commercial Institutions<sup>1</sup>:

The use of closed circuit television systems and the recording of security images is an accepted practice in commercial institutions such as banks, convenience stores, and other facilities. In addition to deterring crime, this practice can often facilitate the apprehension and conviction of individuals involved in criminal activity. It is the position of the Scientific Working Group on Imaging Technology (SWGIT) that in order to optimize the use of these systems the following criteria should be met:

1. Recordings that depict criminal activity must be preserved in a manner that permits law enforcement officials to recover the original images with a documented chain of custody.<sup>2</sup>
2. The number, placement, and type of cameras should be sufficient to provide adequate coverage and detail in the monitored area.
3. Adequate, balanced lighting should be provided in the monitored area.
4. Institutions should establish and follow a program of regular maintenance for their systems.
5. Institutions should have documented procedures to ensure that employees know what to do in the event of a criminal incident.

### Section 3. Introduction

A CCTV security system may include a single camera or multiple cameras. Coverage can include checkout areas, walk-up or drive-up automated teller machines (ATMs), public service areas within an institution, entrance or exit doors for the premises, work areas, interior corridors or common building hallways, and exterior or interior parking areas.

---

<sup>1</sup> This document addresses electronic CCTV recording systems only. It does not address the use of film-based or digital still cameras. It should NOT be assumed that this document is intended to suggest the removal of film surveillance systems, or digital still cameras, from the affected establishments. Due to the fact that images recorded using film and digital still cameras are usually of higher quality than video images, the continued use of such systems, where existing, is strongly encouraged.

<sup>2</sup> CHAIN OF CUSTODY –The chronological documentation of the movement, location, and possession of evidence

A camera system may include cameras, a monitor on which to view the camera images, a recording device to capture selected images and software or a switching system to control the method of selecting and storing images. Depending on the location and situation, video camera systems may use an analog videocassette recorder (VCR), a digital video recorder (DVR), or a PC-based digital recording capture station to record images from the cameras. Finally, a means of retrieving and storing images must be incorporated into the system.

This document addresses closed circuit television (CCTV) systems in seven areas. These are:

- (1) System Design (Section 5)
- (2) Recording systems (Section 6)
- (3) Cameras (Section 7)
- (4) Media (Section 8)
- (5) System Maintenance (Section 9)
- (6) Retention of Recordings (Section 10)
- (7) Procedures for Evidence Handling/Preservation (Section 11)

#### Section 4. Functional Requirements


The purpose of these requirements is to increase the likelihood that images recovered from CCTV systems are sufficient to enable law enforcement officials to identify the people and objects of interest depicted therein.

In order to identify a person, one must be able to distinguish specific individual features on a person such as the detailed shape of the eyes, ears, nose, mouth, and chin. Identification is facilitated if one has the ability to distinguish smaller features such as moles, scars, tattoos, and freckle patterns, as well as the ability to derive measurements of these features.<sup>3</sup> Likewise, identification of a vehicle will require that one be capable of objectively reading the license plate numbers, or distinguishing other identifying characteristics.

---

<sup>3</sup> CCTV systems that were designed for automated facial recognition may not meet the minimum standards specified in this document.

In Figure 1, the images on the left are more likely to allow for personal identification than the images on the right. The lower part of the figure shows the head of the subject from each image after it has been enhanced.

	
<p style="text-align: center;">Figure 1(a)</p> <p>A CCTV image likely to be suitable for personal identification.</p>	<p style="text-align: center;">Figure 1(b)</p> <p>A CCTV image not likely to be suitable for personal identification.</p>
	
<p style="text-align: center;">Figure 1(c)</p> <p>Cropped, enlarged, and enhanced image processed from Figure 1(a) above.</p>	<p style="text-align: center;">Figure 1(d)</p> <p>Cropped, enlarged, and enhanced image processed from Figure 1(b) above.</p>

## Section 5 System Design

The ability of a CCTV system to record images that will be of greatest assistance to law enforcement depends on multiple factors including

the choice and placement of cameras and lenses, recorders, storage space, and compression schemes. These factors are not independent of one another, but must be coordinated with one another. As an example, adding cameras to an existing system may require adjustments to the amount of storage or the rate at which images from each camera are recorded.

A careful survey of the establishment in which the system will be installed must be completed and analyzed as an integral part of the total system design process. A site plan documenting the location and field of view of each camera in the establishment should be included as a part of this survey. Finally, upon installation, the system must be tested to confirm that images produced by the system as output (i.e., those that would be provided to law enforcement in the event of a criminal investigation) are of sufficient quality to maximize the likelihood of identifying individuals or objects depicted therein.

## Section 5.1 System Components

CCTV systems should include the following components, at a minimum: (1) a camera or cameras, moveable and/or fixed; (2) a monitor; and (3) a recording device, including the means by which the recording may be extracted from the device. Consideration should also be given to any need for recording audio with the video from one or more cameras, and any legal problems unique to audio recording. Guidelines for recording devices are addressed immediately below and in Section 6, while cameras are addressed immediately below and in Section 7.

### Section 5.1.1 Monitors

A monitor should be included with every CCTV system so that system operation may be checked on a daily basis (see Section 8). Monitors capable of operating in an underscan mode are strongly recommended since this capability permits the viewer to observe the entire field of view being recorded.

## Section 5.2 Number and Placement of Cameras

The number of cameras needed for any given institution will vary depending upon a variety of factors, including the specific security needs of the institution and the monitored area(s). Care should also be exercised to ensure that cameras are not located in places in which they may be subject to tampering or accidental adjustments. Camera disabling and tampering can be minimized by using components that feature concealed wiring and protection of the camera and lens assembly from weather and/or physical damage.

The cameras' fields of view should not be obstructed, nor should cameras be pointed directly at bright light sources such as picture windows, spot lights, etc. If bright areas cannot be avoided in a scene, cameras with backlight illumination or compensation adjustments are preferred to optimize the resulting image.

As a minimum, there **MUST** be at least one camera for every exit. These exit cameras should be aimed toward the interior of the facility, and each one should be located where it can obtain an unobstructed frontal view of the head and shoulders of every individual exiting the facility. The lenses on exit cameras should be configured to have a depth of field that extends from 3-feet to at least 10-feet from the camera in order to provide images of exiting individuals that are in focus. Exit cameras that have a depth of field extending from 3-feet to beyond 10-feet will have the added benefit of providing overviews of the interior and head-to-foot views of people as they enter and exit the facility.

Cameras should be placed where they can record images with unobstructed views at each point of customer transactions, such as teller windows (both walk-up and drive-through), cash registers, automated teller machines (ATMs), or customer service stations. There must be at least one camera at each point of customer transaction. Cameras should be adjusted to ensure that they are in focus at the location that a customer can be expected to stand. If a window or other security barrier is present, care must be taken to position the camera in a manner that minimizes reflection, glare, and

other obstructions that can interfere with a clear view of the persons or objects being recorded.

Figure 1(a) illustrates a head and shoulders image that is preferable for the exit and transaction cameras. The camera lenses needed to achieve the fields of view are discussed in Section 7.

Cameras that provide overviews of the interior and exterior portions of an establishment can be useful in an investigation, but cannot be relied upon to provide images suitable for identification purposes. Therefore, in these guidelines they are considered to be of reduced importance. However, if the combination of the exit and customer-transaction cameras does not provide complete coverage of the interior of the establishment, then it is recommended that additional cameras be included for this purpose.

If deemed necessary, exterior cameras intended to record images of vehicles should be placed to provide direct views of the vehicle, so that the license plate is clearly visible and legible. Additional exterior cameras covering wider fields of view can provide additional vehicle information.

Finally, in some instances, commercial institutions may find it useful to include monitored cameras as a part of their overall security strategy. The views from such cameras are not intended to be recorded, but provide employees with a means to view areas within a facility that would otherwise be out of employees' sight. Moveable dome and pan/tilt cameras can be used to provide additional room coverage through automatic alarm presetting and parking. Motion detection or door contact alarms can automatically initiate a camera preset providing a high-resolution view of the alarmed scene. This provides un-manned, additional target coverage. After a pre-determined time, the camera can return to a preset parked position or to a scanning pattern to cover site locations not viewed by the fixed devices.

If the system contains a matrix switch with a joystick controller, a guard or observer can manually track a suspect giving a tightly

zoomed, high resolution image of the suspect. Variable speed control and automatic focus are recommended to facilitate smooth target tracking. When in the parked position, the unit can serve as an additional fixed camera.

Specific information regarding camera types and lenses is provided in Section 7.

### Section 5.3      Lighting

Poor lighting is the most common factor that degrades the quality of video images. Adequate, balanced lighting should be provided in areas viewed by the cameras. Particular care must be taken to ensure that the dynamic range present in a scene does not exceed the capability of the camera to record it.

Strong backlighting or high contrast lighting may cause the face of a subject to be obscured in shadow, making identification of a suspect from the image difficult or impossible. Likewise, spotlights can create both shadows and highlights on faces, making it difficult to determine if observed tonal variations represent actual features, such as facial hair, or are merely a product of the lighting. The use of non-infrared, high dynamic range cameras and those capable of operating in low light conditions should be considered to help improve the image quality.

As an example, ceiling-mounted fluorescent lighting that is well distributed throughout interior spaces would be preferred to the use of track-mounted spotlights.

Finally, different light sources have different color temperatures that will affect the apparent color of objects within a scene. Tungsten lamps impart a reddish tint to objects in a scene, while fluorescent bulbs can impart a greenish tint. Likewise, sodium lamps can make objects appear more yellow than they actually are. Most color video cameras can be adjusted to compensate for this, and many perform this function automatically.

A color video camera is considered balanced for a particular reference white when a neutral white card is placed in the camera's field of view under normal illumination conditions and the red, green, and blue channels provide equal output levels. Therefore, interior color cameras should be balanced for white upon installation, and rebalanced if the type of lighting used is changed. Note, however, that since many commercial institutions will operate under conditions in which lighting is variable, white balance may not be possible at all times.

Infrared (IR) lighting can be used to provide improved low light performance for monochrome cameras. IR lighting is not supported by standard color cameras as they filter out the IR spectrum. If an IR sensitive video camera is used, law enforcement officers should be made aware of this because an IR sensitive video camera often reproduces clothing that appears to be dramatically differently when compared to images of the same clothing that were recorded with a video camera that is not sensitive to IR.

A more complete set of technical guidelines for lighting is provided in Appendix B.

#### Section 5.4 Electrical Power

CCTV systems must be provided with adequate power. Backup power sources and surge protection should be included in the system design to ensure that recordings are preserved in the event of a power loss. Systems that require electrical power to preserve their recordings should have backup power sources sufficient to last for at least thirty (30) minutes, until either the system power is restored or the system is shut down in a manner that preserves the recording. Video processors such as DVRs should also automatically restart in a preprogrammed operation mode upon power-up from extended power outages.

When a VCR or DVR with automatic restart is used, there must be an ON-OFF switch on the front of the recorder. This is to ensure that no data is lost following an incident that led to the recorder being purposely turned off to preserve the recording of the event.

CCTV systems should be placed on isolated circuits that are properly grounded to reduce interference and signal degradation. If the system is on a long power run, outdoors, or in an area prone to electrical storms, special protection devices to control power surges and nearby lighting strikes are strongly recommended.

## Section 5.5 Bandwidth

The bandwidth provided for the transmission of the video signal must be compatible with, and sufficient to meet, the resolution requirements listed below for the system's recording device. While bandwidth minimum standards do not guarantee acceptable video image quality, they do play an important part. To improve the likelihood of acceptable image acquisition, video cameras should have a signal bandwidth of at least 7MHz.

### Section 5.5.1 Signal to Noise Ratio

One major problem with picture clarity is noise. Electronic noise is present to some extent in all video signals. Noise manifests itself as "snow" or graininess over the whole picture on the monitor and subsequently on recordings. There are several sources of noise: poor circuit design, heat, over-amplification, external influences, automatic gain control, and transmission systems. Some video signal noise cannot be overcome in a reasonable manner. However, to improve the likelihood of acceptable image acquisition, video cameras should have a signal to noise ratio of at least 48 dB. Further, the line loss between each camera and the multiplexer or recorder that the camera is connected to shall not cause the signal to fall below 45 dB.

## Section 5.6 Recorder security

Steps must be taken to ensure the physical security and integrity of the system's recording device. Placement of the recording device in a restricted access location, such as a locked cabinet or room, is strongly recommended. Note that proper environmental controls must be implemented per manufacturer specifications. For example, VCRs require adequate airflow to prevent overheating.

Policies should be in place to ensure that law enforcement can gain immediate access to the recorded images when necessary.

### Section 5.7 Recordings of Associated Text Information

Both analog and digital CCTV systems include the capability to associate text information, such as time, date, and camera ID, with the images recorded by the system. In some cases, transaction or personal information may also be recorded in association with image data. This is often accomplished by superimposing the text directly upon the images.

Time, date, and camera information is useful in investigations and should be preserved. However, text that obstructs the view of subjects' faces or vehicles' license plates may hinder investigations and should be placed to minimize its effect on image content. Test recordings should be performed to ensure that this requirement is being met and that the information being recorded is accurate.

SWGIT strongly recommends that digital CCTV systems be configured so that associated text information is unalterable and preserved as data records or files that are linked to the respective images. In such cases where time and date, transaction, or personal information is recorded in digital systems along with the image stream, it **MUST** be possible for law enforcement to recover the images separate from this information.

For analog CCTV systems, in which it is not possible to separate personal or transaction data from the images, systems **MUST** be configured to record this information for one (1) second or less for each instance (e.g., transaction) in which such data is required. If the text information is visible on the recorded video, then the text characters must be as small as possible while still being legible, and it must be possible to position the text anywhere on the screen to minimize the effect.

Each individual image and transaction data packet should have a time/date stamp associated with it. Whenever possible the time/date stamp should be generated as close to the image source as possible. For example, when a camera is directly wired to the digital recording device at the same site, then time synchronizing the recorder is sufficient. However, when the camera is located remotely (in another city) and connected to the recorder via a Wide Area Network (WAN), then the image may be delayed in transit. In those cases, it is highly desirable to associate the time stamp with the image at the source sensor (the camera) instead of at the recorder. A time-tag image file is then transferred over the WAN to the recorder. The trend toward using Internet Protocol (IP) cameras will facilitate this process where the IP camera is capable of accepting time synchronization input.

The industry accepted standard for time synchronizing computers and all digital data devices is the Network Time Protocol (NTP). It is an open standard sponsored by the Internet Engineering Task Force (IETF) and is defined by RFC 1305. This standard specifies an accuracy level of the time synchronizing device called the Stratum level. The Simple Network Time Protocol (SNTP) is another such standard. With the proliferation of Global Positioning Satellite (GPS) based timing equipment, these time references are readily available for low cost. The use of an industry standard time synchronization protocol is recommended.

## Section 6 Recording Systems

Recording systems used in CCTV systems should adhere to the following minimum standards:

### Section 6.1 Recording Resolution for Analog Recording Systems (VCRs):

Analog VCRs must record each image at a minimum line resolution of 240 visible lines. This resolution is typical of most VHS VCRs. The use of VCRs with higher line resolutions (e.g., S-VHS VCRs and tapes) is strongly encouraged, since this improves image quality.

## Section 6.2 Recording Resolution for Digital Video Recorders (DVRs):

The minimum resolution requirements for Digital Video Recorders will vary depending upon the media used to record the images. Some manufacturers quote digital resolution (pixels) in analog lines of resolution. For rough comparative purposes, a minimum digital resolution of 450 lines can be used for DVRs using digital video tape. DVRs using a hard disk or optical disk for storage must record each frame at a minimum resolution of 640 pixels in the horizontal direction and 480 pixels in the vertical direction<sup>4</sup>. If images are recorded in field mode, then each field must be recorded at a minimum resolution of 640 by 240.

SWGIT strongly encourages the use of higher resolutions than those described above whenever possible.

## Section 6.3 Compression:

Compression is a process in which the size of a digital file is reduced. Due to the large amount of information present in each second of video, most digital video systems use compression to reduce storage and transmission requirements.

Compression may be "lossless" or "lossy". In "lossless" compression information is not lost. In "lossy" compression, information is lost. If a file has only been saved using "lossy" compression, then it is not possible to recover all of the information in the original file.

In the event of an alarm-triggered mode (see Section 6.8), it is recommended that lossless compression be used to record the sequence of interest, if possible. If a system is incapable of lossless compression during the alarm mode (as well as at all other times), then in order to maximize the amount of information available to law

---

<sup>4</sup> Differences in the units used to describe these resolution recommendations are due to the differences in the industry standards used to describe these media.

enforcement, it is strongly recommended that the lowest possible amount of compression be used in recording files.

Some manufacturers utilize proprietary compression formats that require the use of proprietary software in order to view the video sequences or images. Use of such software can prevent or hinder law enforcement from viewing or otherwise accessing these images. If such software is utilized, then steps must be taken to ensure that law enforcement will be able to access them when needed. See Section 9, "Evidence Handling," for more guidance.

#### Section 6.4 Time Lapse Recordings

NTSC video records images at a rate of approximately 30 frames per second. Each frame consists of two fields or images, producing an actual rate of 60 images per second.

Analog videotapes are usually recorded in one of three speeds – SP (Standard Play), LP (Long Play), or EP/SLP (Extended Play/Super-Long Play). A T-120 tape recording at SP speed will record for a period of 2 hours, while a T-120 tape recording at LP speed will record for a period of 4 hours, and a T-120 tape recording at EP/SLP speed will record for a period of 6 hours. Changing the recording speed from SP to LP to EP/SLP does NOT change the rate at which images are recorded – it remains 60 images (fields) per second. Any recording made at a rate of 60 fields per second is commonly referred to as a “real-time” recording.

Time lapse recorders are capable of recording video at rates that are much lower than 60 images per second. This enables the recording of images over a longer period of time. For example, using T-120 tapes, a VCR set in SP mode will record 30 frames (60 images) per second for 2 hours. With a time-lapse setting of 24-hours, a T-120 tape will run for 12 times the normal two-hour tape length, and the VCR will record no more than 5 images per second. Table 1 provides the image recording rate for a variety of common time-lapse settings under normal recording conditions.

TABLE 1 – Typical image recording rate for different time lapse modes\*

Time Lapse Mode (in hours)	2	12	24	48	72	120	240
Number of fields (images) per second	60	10	5	2.5 (5 every 2 s)	1.67 (5 every 3 s)	1	0.5 (1 every 2 s)

\* Based on an approximate “real-time” rate of 60 fields per second.

Some analog time-lapse video recorders manufactured specifically for CCTV security applications are designed to record a higher number of fields per second in different time-lapse modes than those reported in Table 1. For example, some “High-Density” video recorders can achieve record rates of more than 20 fields per second in 24-hour time-lapse mode. Likewise, digital video recorders may also be capable of recording at higher rates.

In order to meet SWGIT guidelines, CCTV systems MUST capture and record at least one complete field per camera per second. Any rate lower than this may result in inadequate temporal coverage of events in the scene.

### Section 6.5 Switchers/Multiplexers

Establishments with more than one camera may choose to utilize a device that enables the recording of images from all of the cameras to a single recorder. The two most common devices used to do this are switchers and multiplexers.

Switchers, as the name implies, alternate among multiple cameras so that the output of the switcher at any one time is the signal from a single camera. Systems in which the output of a switcher serves as the input to the recording device will record images from each camera in succession. The time that it takes for a switcher to return to the same camera is called the “camera interval.” The reciprocal of this interval is referred to as the “camera refresh rate.” Therefore, a

camera interval of ½-second would correspond to a camera refresh rate of 2-times-per-second.

A multiplexer takes the outputs from multiple cameras and adds an encoded signal that allows a picture from each camera to be viewed in succession (as with switchers) or simultaneously. The encoded signal is almost always vendor-proprietary, making it difficult to recover the recorded images without the proper hardware and software.

Switchers, multiplexers, and similar devices are frequently used to generate multi-image displays. Multi-image displays consist of a split screen that allows for the viewing of more than one camera image on the screen simultaneously. Recording images in this mode, however, significantly decreases the individual camera's image size and quality. Many brands of duplex multiplexers will allow the user to view multiple camera images simultaneously, while still recording full-size images from each camera.

In order to meet SWGIT guidelines, CCTV systems MUST NOT RECORD in multi-image modes.

Given the requirement in section 6.4 that recordings capture at least one complete field per camera per second, this will restrict the refresh rate for each camera in a system with one recorder. As a reference, Table 2 relates the number of images per second per camera for given time lapse recording modes.

Table 2 Note: The values reported in Table 2 assume a nominal real-time recording rate of 60 fields per second. As described in Section 6.4, some CCTV security system video recorders, designed specifically for time-lapse applications, are capable of exceeding the values reported in this table. Under such circumstances, it will be possible to record images from more cameras while still meeting the SWGIT requirement of one image per camera per second.

Table 2 – Images Recorded per Second by each camera in a switched system for different time lapse modes (see Table 2 Note)

<b>Images (Fields) Recorded Per Second by Each Camera</b>							
		<b>Time Lapse Recording Mode (in hours)</b>					
		2	12	24	48	72	120
<b># Cameras</b>	1	60	10	5	2.5	1.67	1*
	2	30	5	2.5	1.75	^	^
	4	15	2.5	1.25	^	^	^
	8	7.5	1.25	^	^	^	^
	16	3.75	^	^	^	^	^
	32	1.875	^	^	^	^	^
	60	1*	^	^	^	^	^

\* Indicates limits fixed by SWGIT requirement of one image per camera per second

^ Indicates this cannot meet SWGIT requirement of 1 image per camera per second

## Section 6.6 Triggers/Incident Recorders

In some situations, systems may include triggers that lead to the recording of images at a rate, or in a sequence, that differs from the normal operating mode. An example of this would be to change from time-lapse mode to real-time mode when triggered by an alarm button. Another example would be to include an otherwise inactive camera in the recorded sequence if motion was detected in the field of view of that camera.

If such a device is used, its use MUST NOT conflict with the recommendation provided above in Section 6.4 (i.e., one field per second from every camera in the system must continue to be recorded at a minimum).

Furthermore, test recordings should be made to ensure that activation of the trigger and subsequent operation of the incident recorder does not have a deleterious effect on the quality of the recorded images.

## Section 6.7 Remote Recording

Some CCTV systems transmit the system signal (images and other information) to a remote site for recording.

The images transmitted this way are usually compressed significantly in order to meet bandwidth restrictions. As noted in Section 6.3, excessive compression severely degrades image quality.

In those situations in which remote monitoring is practiced, SWGIT strongly recommends that recording devices also be installed at each monitored location, so that images may be stored with a minimum of image compression, when necessary.

In some cases, a remote facility recording video signals from multiple off-site locations may also have the capability to control recording devices installed at each off-site location. It is important to ensure that this capability be tested on a regularly scheduled basis. Procedures must be established that define the response by personnel at the remote facility in the event of an incident at one of the off-site locations. Steps should be taken to preserve the recorded video at both the remote facility, as well as the off-site facility.

#### Section 6.8 Alarm-Triggered Digital Buffers

In an alarm-activation event, law enforcement will seek to have the highest possible image quality. This includes recording images using lossless compression.

Therefore, in order to meet SWGIT guidelines, CCTV systems that record images using lossy compression MUST have an alarm-mode included in their system.

Furthermore, in the event of an alarm trigger, in order to meet SWGIT guidelines, the following system settings are required for the alarm sequence:

- (1) Lossless compression;
- (2) The recorder must have a buffer capable of retaining the five (5) minutes of data prior to the alarm-trigger using lossless compression;
- (3) The system record at a rate of 60 fields per second, while maintaining the same rate at which the system switches

- between cameras (i.e., more pictures per camera each second if time lapse mode is normally used);
- (4) Once triggered, the system should continue to record in a lossless manner until manually stopped by user intervention by an authorized agent, per the establishment's policies and procedures<sup>5</sup>. This period of time should extend for at least 5 minutes after the completion of the crime or event that led to the alarm. The recorder shall have sufficient storage to be capable of recording in this mode for a minimum of 30 minutes.
  - (5) All alarm data may be stored as black and white images.

Note: Currently installed systems that are incapable of lossless compression should be configured to record the alarm sequence at the lowest possible compression ratio.

## Section 6.9 Digital Recorder Output Devices

Digital recording systems that do not use removable media for day-to-day storage must be capable of exporting exact duplicates of their recordings to removable media in a standard commercial format. This is necessary so that law enforcement officials can obtain copies of the recorded digital files that are a bit-for-bit copy of the files stored on the system.

In order to meet SWGIT guidelines, CCTV systems using digital recorders must be configured to permit output to write-once storage devices including compact disk (CD-WORM)<sup>6</sup>. It is strongly recommended that systems also be configured to permit output to digital versatile disk (DVD). This latter recommendation is based on the observation that the recording of any alarm-triggered event will be over 10 minutes in length (5 minutes before the alarm, plus the duration of the event, plus 5 minutes after the event). The greater

---

<sup>5</sup> Systems should be configured to stop recording in the event that the recorder runs out of memory/storage space prior to user intervention, in order to retain the existing images.

<sup>6</sup> At the time of this document's preparation, compact disks represent the current industry standard for storage. As advances in storage take place, CDs are likely to be replaced by DVDs or other types of media. The goal of this recommendation is to ensure that evidence is provided to law enforcement using media that requires no special hardware, but represents an industry standard.

storage capability of DVDs will reduce the number of disks needed to store the recording on removable media. Systems designed to output to DVD should NOT utilize standard compression techniques used in the production of consumer DVDs (that is typically on the order of 5:1), but should be capable of making bit-for-bit copies of files recorded on the system hard drive(s).

#### Section 6.10 Output File Types

Digital recording systems must be capable of exporting exact duplicates of their digital image files to removable media. If a system utilizes a proprietary format to store images, then steps must be taken to ensure that law enforcement can extract an exact copy of each image in the recording in a lossless and open file format capable of fully supporting the recorded data. The current preferred file format for such applications is TIFF.

Furthermore, in order to assist law enforcement in the expeditious dissemination of still images immediately after an event, digital recording systems must be capable of directly exporting still images at the highest quality setting in one of the following industry standard formats: TIFF, BMP, or JPG. The ability to export to an uncompressed non-proprietary AVI file and the native video file format, in addition to one of the previously mentioned still image formats, is desirable as well. All output formats must maintain accurate aspect ratios consistent with the original recording.

See Section 11 for further information regarding guidelines for output in the event of a criminal incident.

#### Section 7 Cameras

Cameras used in CCTV systems should adhere to the following recommendations:

##### Section 7.1 Black and White vs. Color Cameras

Although black and white video cameras may provide better image resolution than color cameras, the information available in color images may provide important investigative information. Therefore, the choice of cameras is left to the commercial institution, dependant upon the intended use of the recorded images.

### Section 7.2 Camera Detector Size

Video and digital cameras use detectors that come in a variety of sizes. Typical sizes are 1/4", 1/3", and 1/2". The size of the detector will have a direct impact on the focal length of the camera lens. See Section 7.5 for further information.

### Section 7.3 Camera Resolution

In order to meet SWGIT guidelines, analog video cameras MUST have an output resolution of at least 400 horizontal lines. Digital video cameras MUST have an output resolution of at least 480 horizontal lines. Cameras that have higher resolutions are strongly recommended.

### Section 7.4 Camera Infrared Characteristics

The detectors used in black and white video cameras may be sensitive to a part of the infrared spectrum that is outside of the normal range of human visual perception. This can improve the ability of the camera to record in low-light situations.

Due to the fact that images acquired by infrared-sensitive cameras can make some dark clothing and other objects appear to be lighter than they actually are, it is recommended that infrared-sensitive cameras not be used to record scenes that are well-illuminated. Many cameras are equipped with filters that can mitigate this effect. This does not apply to most color cameras that normally contain an infrared barrier filter to block infrared light.

The use of infrared-sensitive cameras should be noted within the system documentation (see Section 9.1).

## Section 7.5 Lens, Focal Length, and Field of View

The selection of lenses will be dictated by the field of view to be covered by each camera, as well as by the size of the camera's detector.

For cameras placed to record images at a point of customer transactions, such as a teller window (See Section 5.3), the area of interest (face, license plate, etc.) should cover approximately 15% or more of the camera's field of view (based upon the recommended minimum resolution found in Section 7.3). For an average human head that is 6-inches wide, a 3-foot-wide field of view will meet this guideline. For a license plate width of approximately 12-inches, a 6-foot-wide field of view is sufficient.

The focal length necessary to achieve an approximately 3-foot-wide field of view for a given detector size and camera-to-subject distance is provided below (see Table 3). The camera must be in focus at the position of this subject.

Table 3 – Approximate Focal Length (in mm) needed for 3-foot-wide field-of-view.<sup>7</sup>

	<b>Approximate Focal Length (in mm)</b>						
	Distance to Subject (in feet)	<b>2'</b>	<b>5'</b>	<b>10'</b>	<b>15'</b>	<b>20'</b>	<b>30'</b>
<b>Detector Size (inches)</b>	<b>1/4"</b>	<b>2.3</b>	<b>5.9</b>	<b>11.7</b>	<b>17.6</b>	<b>23.5</b>	<b>35.2</b>
	<b>1/3"</b>	<b>3.1</b>	<b>7.8</b>	<b>15.7</b>	<b>23.5</b>	<b>31.3</b>	<b>47.0</b>
	<b>1/2"</b>	<b>4</b>	<b>10.1</b>	<b>20.2</b>	<b>30.3</b>	<b>40.4</b>	<b>60.7</b>

Cameras that provide overviews of interior and exterior locations should have their focal lengths selected so as to meet the field-of-view requirements of the establishment. Note, however, that exit cameras should have sufficient depth of field to be in focus at distances of 3-feet and beyond to ensure that subjects exiting the facility will be in focus.

<sup>7</sup> Focal lengths determined using Panasonic Corporation calculator found at [www.panasonic.com](http://www.panasonic.com).

### Section 7.6 Exposure control

Cameras should be equipped with automatic mechanisms to ensure proper exposure under varying lighting conditions. Such mechanisms include, but are not limited to, automatic gain circuitry, day/night sensor switching, and lenses with automatic iris functions.

### Section 7.7 Camera Housings

Cameras may require coverings and environmental controls to protect them from the elements or tampering. Note that clear coverings placed in front of camera lenses will reduce image quality. Therefore, unless there are specific environmental or security concerns that require camera housings, it is recommended that they not be used.

## Section 8 Media

Media, including analog videotapes, compact discs, digital video tapes, and DVDs, should be of high quality and meet equipment manufacturers' specifications. Low quality media can result in damaged equipment and poor images.

## Section 9 System Maintenance

CCTV systems should be maintained in a manner that ensures their proper function over their entire lifetime. Therefore, the following recommendations should be followed:

### Section 9.1 Documentation of System

Institutions should maintain documentation regarding their CCTV systems that include the following information:

- (1) Make and model of all system components, including recorders, cameras, lenses, and multiplexer/switcher, etc. For digital systems, this information should include software and hardware information, including software

version. If infrared-sensitive cameras are in use, their location should be documented. An example of a system information sheet is included in Appendix C. If possible, a photocopy of the maintenance record should be included.

- (2) Adequate system documentation should be included at the site. This includes instructions for downloading and outputting recordings.
- (3) Point of contact information for system installer and/or system maintenance organization, to include at least two names and telephone numbers.
- (4) Site plan showing all equipment placement (including recorders), as well as field of view for each camera. Appendix C includes an example of a site plan.

This information should be verified monthly and made available to responding law enforcement officials upon their arrival at the scene.

## Section 9.2 System Validation and Maintenance

Prior to use, systems must be validated to meet the requirements of Section 4 – to wit, they must be capable of acquiring, recording, and producing output images that are of sufficient quality to enable law enforcement officials to identify the people and objects depicted therein. Revalidation of these requirements must occur every time the system is altered.

A variety of system checks and maintenance are necessary at different times. If system errors are found, steps to correct them should be implemented.

A maintenance log must be maintained to document all system validation activities, checks and maintenance activities.

Table 4 provides a calendar for these checks and maintenance items that should be recorded on a maintenance log.

Table 4 – System Checks and Maintenance Schedule

		Check/Activity	Procedure
Frequency	Daily	Is the system operating?	Play back 30 seconds of recorded video and confirm that all cameras are being recorded.
		Are the cameras aimed properly, in focus, and not obstructed?	Review live images from each camera to ensure this.
		Are the time and date correct?	How one does this will depend upon the system design.
		Is the removable recording media (i.e., tape) properly installed and in the record mode?	Check that the record indicator is active and that the tape counter is advancing.
		Is the system secured?	Check physical locks on cabinet and/or doors.
	Monthly	Clean lenses and camera housings. (Care must be taken to avoid damage and misalignment.) More frequent cleaning may be necessary depending upon environmental conditions.	Follow manufacturer's specifications.
		For systems using removable media (i.e., tape) recording mechanisms should be cleaned.	Follow manufacturer's specifications.
		Check environmental controls (temperature and humidity) to ensure that they meet manufacturer's specifications for all system components.	Follow manufacturer's specifications.
	Annually	Complete system preventative maintenance check.	A qualified CCTV technician should perform this check.
		For digital systems using hard drives for storage, a check for bad clusters and other disk errors should be performed.	Refer to manufacturer instructions and specifications.
		Ensure written policies and procedures regarding system operation are up to date.	Review existing policies and procedures and revise as needed.
		Ensure employee competence in system operations, including alarm-mode response.	Conduct operator training.
		Ensure system output to compact disk meets law enforcement needs.	Write sample images from system to removable media and review images on separate computer system.
		Ensure that reusable media is replaced.	To be performed by system operator

### Section 9.3 Maintenance of recording media

Institutional requirements will dictate the length of time for which recorded images must be archived.

All recording media has an expected usable life span. Based on that life span, policies should be developed to ensure that media is replaced before this period expires.

As an example, it is recommended that VHS video tapes be reused no more than 12 times and that they be replaced on an annual basis. Note that use of extended time-lapse mode may drastically shorten the life span.

For digital recording devices, manufacturer's recommendations for maintenance and the device service life replacement schedule should be observed. A regular ongoing (automated) inspection of hard drives should be conducted to ensure that the disk(s) is/are functioning properly and that there are no bad sectors or other hardware errors that could result in a loss of data. Other reusable media must be re-certified no less frequently than the manufacturer's guaranteed period.

Institutions should establish policies regarding the marking of removable media so that the most recent date of recording will be documented.

#### Section 10 Retention of Recordings

The purpose of this section is to provide guidelines regarding the retention of recorded media.

It is recommended that analog videotapes be retained for a minimum of thirty-one (31) days before being reused. This coincides with the twelve-time use recommendation. For ease of retrieval, each videotape should be sequentially numbered and the dates and times recorded on each tape should be written on a label on the videotape.

Due to the nature of digital recordings, the SWGIT recommends that recordings be retained for the longest time possible (minimum of 10 days) with the least amount of compression available within the system's capabilities. Storage capacity to meet these needs must be considered.

## Section 11 Evidence Handling Procedures

This section addresses procedures to follow when law enforcement response is necessary. This may be in response to a robbery, or it may be related to other criminal investigation.

### Section 11.1 Documentation for Law Enforcement

The system documentation, as described in Section 9.1, including equipment information, site plan, contact information, and maintenance log should be made available to responding law enforcement officials. Any additional pertinent information regarding the recording or the incident itself should be noted, such as incident time, record mode, discrepancies between actual time and recorder time. Appendix C includes an example of this type of documentation.

### Section 11.2 Handling of Evidentiary Recordings

Following an incident involving immediate law enforcement response, it is necessary to ensure that the recorded images are secured. Unless the possibility exists that the images may be over-recorded or overwritten, the recording should not be stopped until the arrival of law enforcement officials.

#### Section 11.2.1 Video Cassette Tape Systems

Upon termination of recording, the tape should be removed from the recording device and the recording tab immediately removed or shifted to the record disabled setting. The tape should not be played again prior to the arrival of law enforcement officials. The name of the institution and identity of the individual performing this function should be marked on the exterior of the cassette housing, along with the time and date of removal.

Prior to transfer to law enforcement officials, steps must be taken to ensure that the tape is not mishandled or damaged. This includes keeping the tape away from magnetic fields, such as those generated by televisions, radios, and speakers. Steps should also be taken to

keep the tape at room temperature and out of direct sunlight. Tapes should not be stored in vehicles for an extended period of time.

Personnel qualified to assist law enforcement in the recovery of images from the tape should be identified and made available prior to the arrival of law enforcement officials.

### Section 11.2.2 Digital Video Systems

The following steps should be followed:

- 1.** Upon termination of recording, personnel qualified to assist law enforcement in the recovery of images from the CCTV system should be identified and made available to offer technical assistance. This representative shall be available either in person or via telephone.
- 2.** Law enforcement officials will coordinate with appropriate personnel to view and retrieve the best image(s) prior to the officials' departure from the crime scene. When immediate transmission of images is necessary to expedite distribution from the crime scene, they should be transmitted via network, E-mail, compact disk, or other available means. Images shall be provided to law enforcement in the TIFF, BMP, or JPEG format. If the establishment utilizes a remote location for the storage of recorded images, then the establishment will provide the images to an address designated by the law enforcement officials.
- 3.** The establishment's security personnel will produce at least two copies of the relevant images and video on CD or DVD (non-rewritable) in the non-proprietary formats as well as the original native format.
- 4.** In the event of alarm-trigger incidents as described in Section 6.8, law enforcement would like all video and relevant data that were recorded five minutes before the alarm-trigger, the entire incident, and five minutes after the incident. This is barring any outside circumstances when it is required to save a longer period of time, i.e., a casing of the bank, etc.

5. If additional retrieval of video recording is warranted, law enforcement officials will notify the establishment's security personnel to secure the hard drive or retrieve additional video and data. The establishment will be required to maintain all recorded video and data on a rolling ten day period from the event of a crime. This would mean that at the date of the crime, law enforcement officials would be able to review all video for ten days prior to the crime. As an example, two days after the crime, law enforcement officials would be able to review all video for eight days prior to the crime and so on.
  
6. Once the relevant video, images, and data have been copied, each shall be labeled with the name of the institution and identity of the individual performing this function, along with the time and date of removal. This information should not be written directly on the media, but preferably onto a label that is affixed to a protective container (such as a jewel case, sleeve, or clamshell enclosure).

## APPENDIX A – CCTV References

USDOJ, Office of Justice Programs (OJP), National Institute of Justice (NIJ)  
[www.ojp.usdoj.gov/nij](http://www.ojp.usdoj.gov/nij)

The Appropriate and Effective Use of Security Technologies in U.S. Schools, *A Guide for Practical School Security Applications* by Mary W. Green, September, 1999  
<http://www.ojp.usdoj.gov/nij/pubs-sum/178265.htm>

Law Enforcement and Corrections Standards and Testing Program, Video Surveillance Equipment Selection and Application Guide, NIJ Guide 201-99 by D.J. Atkinson, V.J. Pietrasiewicz, and K.E. Junker, February 2000  
<http://www.ojp.usdoj.gov/nij/pubs-sum/179545.htm>

Police Scientific Development Branch, UK Home Office  
Digital Imaging Procedure Version 1.0  
 © CROWN COPYRIGHT 1998 FIRST PUBLISHED 2002 PSDB Publication number 02/2002  
<http://www.homeoffice.gov.uk/pcrg/psdb/publications/digimpro.pdf>

Assessment of the ADVIS, IMPRESS, VIEW Video Enhancement System  
 for the UK Police Service  
 J Rason, T Kent, I Sall, P Gugenheim, S Walker  
 © CROWN COPYRIGHT 2000 FIRST PUBLISHED 2000 PSDB Publication number 1/2000

CCTV: Making it Work. Guidance on Recruitment and Selection Practice for CCTV  
 E Wallace, C Diffley  
 © CROWN COPYRIGHT 1998 FIRST PUBLISHED 1998 PSDB Publication number 8/98

CCTV: Making it Work. Training Practices for CCTV Operators  
 C Diffley, E Wallace  
 © CROWN COPYRIGHT (1998) ISBN: 1 84082 045 4 PSDB No: 9/98  
[http://www.homeoffice.gov.uk/pcrg/psdb/publications/cctv-9\\_98.pdf](http://www.homeoffice.gov.uk/pcrg/psdb/publications/cctv-9_98.pdf)

CCTV: Making It Work. Time and Date Displays  
 A Griffiths  
 © CROWN COPYRIGHT 1998 FIRST PUBLISHED 1998 PSDB Publication number 13/98

CCTV: Making it Work. CCTV Control Room Ergonomics  
 E Wallace, C Diffley  
 © CROWN COPYRIGHT 1998 FIRST PUBLISHED 1998 PSDB Publication number 14/98

Guidelines for the Handling of Video Tape  
 P Mather  
 © CROWN COPYRIGHT 1998 FIRST PUBLISHED 1998 PSDB Publication number 21/98

Performance Testing CCTV Perimeter Surveillance Systems

J Aldridge, C Gilbert

© CROWN COPYRIGHT 1995 FIRST PUBLISHED 1995 PSDB Publication number 14/95

CCTV Operational Requirements Manual Version 3.0

J Aldridge

© CROWN COPYRIGHT 1994 FIRST PUBLISHED 1994 PSDB Publication number 17/94

ISBN 1 85893 335 8

[http://www.homeoffice.gov.uk/pcrg/psdb/publications/or\\_manual.pdf](http://www.homeoffice.gov.uk/pcrg/psdb/publications/or_manual.pdf)

UK Home Office Crime Reduction Programme

<http://www.crimereduction.gov.uk/cctvminisite4.htm>

**Crime Reduction: Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness**

Closed Circuit Television In Public Places: Its Acceptability And Perceived Effectiveness reports on results of an examination of public attitudes to CCTV issues.

<http://www.crimereduction.gov.uk/cctv3.htm>

19/7/2001

**Crime Reduction: Understanding Public Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities**

Police Research Group – Crime Prevention Unit Series Paper No. 42 (1993) by Nick Tilley

<http://www.crimereduction.gov.uk/cctv2.htm>

19/7/2001

**Crime Reduction: Closed Circuit Television in Town Centres: Three Case Studies**

Police Research Group - Crime Detection and Prevention Series Paper 68 (1995) by Ben Brown

<http://www.crimereduction.gov.uk/cctv1.htm>

19/7/001

**Crime Reduction: Transmission Guidance**

Guidance issued by the Home Office on the transmission of CCTV image data.

<http://www.crimereduction.gov.uk/cctv25.htm>

15/6/2001

**Crime Reduction: A Consistent Approach to Gathering Evidence**

Guidelines on how police may interact tactfully with CCTV operators when gathering CCTV tapes for evidence of criminal activity.

<http://www.crimereduction.gov.uk/cctv24.htm>

9/7/2001

**Crime Reduction: CCTV Initiative: Round Two Schemes that intend to use Digital Recording**

Information on the operational requirements and best value for using digital recording.

**<http://www.crimereduction.gov.uk/cctv23.htm>**

16/5/2001

**Crime Reduction: CCTV and the Human Rights Act**

The implications for the use of public space surveillance of the European Convention on Human Rights

**<http://www.crimereduction.gov.uk/cctv13.htm>**

19/7/2001

**Crime Reduction: Digital Images as Evidence**

Information and advice on the use of digital images as evidence.

**<http://www.crimereduction.gov.uk/cctv27.htm>**

15/6/2001

International Association of Chiefs of Police (IACP)

[www.theiacp.org](http://www.theiacp.org)

**Use of CCTV/Video Cameras in Law Enforcement**

**<http://www.theiacp.org/documents/pdfs/Publications/UseofCCTV.pdf>**

Uses and interests of over 200 responding law enforcement agencies using CCTV today. It also highlights some of the practical considerations and policy issues police executives must consider when employing this technology.

**Police In-Car Video Camera Evaluation**

<http://www.theiacp.org/research/index.htm>

The IACP will be conducting a comprehensive evaluation on the installation, use and impact of police in-car video cameras in 47 state police and highway patrol agencies. This 18-month project, commencing in June 2002, will examine and ascertain the impact of in-car cameras in four critical areas: police officer safety, agency liability, community perceptions of police, and police professionalism.

Security Industry Association (SIA)

[www.siaonline.org](http://www.siaonline.org)

**SIA CCTV Surveys**

**Survey on Evidence of Digital Images**

**[http://www.siaonline.org/page.asp?c=ig\\_cctv\\_srvy\\_intro](http://www.siaonline.org/page.asp?c=ig_cctv_srvy_intro)**

Recently, the SIA CCTV Industry Advisory Board formed a sub-committee to investigate the issues around digital evidence and the impact it has on the court systems both here in the United States and globally.

**The Focus - CCTV Newsletter**

[http://www.siaonline.org/page.asp?c=ig\\_cctv\\_news](http://www.siaonline.org/page.asp?c=ig_cctv_news)

The CCTV Industry Group quarterly newsletter, *Focus*.

**2001 Closed Circuit TV Market Report**

[http://www.siaonline.org/page.asp?c=storeproduct\\_19](http://www.siaonline.org/page.asp?c=storeproduct_19)

**MR-CCTV-2001** "Cameras everywhere" may well be the best motto for this growth industry. It is becoming a favorite tool in law enforcement, municipal infrastructure, education, retailing, medicine, commercial monitoring, residential monitoring, and a host of other market applications now made possible by video and communications technology.

**1998-1999 CCTV for Public Safety Report**

[http://www.siaonline.org/page.asp?c=storeproduct\\_59](http://www.siaonline.org/page.asp?c=storeproduct_59)

**PSR-CCTV-1998** This third in a three volume series details CCTV for public safety application in an additional 37 U.S. cities. The 1998 report, designed to assist law enforcement and public safety officials in understanding how CCTV technology is being used and defined in the public sector, is designed to offer real-world examples of CCTV application successes and failures. Each example outlines why a program succeeded or was sent back to the drawing board. The 1998 report also provides and summarizes examples of how state and federal legislation is defining the public sector use of CCTV technology. (355 pages) The 1998 report comes with a Privacy Supplement that details the legal and civil-rights issues associated with CCTV application in the public sector. This comprehensive resource document not only details CCTV privacy issues in the U.S., but also around the world. (75 pages)

## APPENDIX B - Technical Guidelines for Lighting

In this document, illuminance is measured in Lux. Some older documents and references may refer to the measurement in foot candles. 1 foot candle ~ 11 Lux.

To provide good quality camera images, a minimum of 275 – 333 Lux of illumination should be provided in the customer areas, office areas, hallways, stairways and exits where camera coverage is provided.

Exterior self-service facilities, such as ATM vestibules or drive up lanes, should have a minimum of 110 Lux of illumination 24 hours per day to ensure good image quality.

Exterior areas such as sidewalks, entrances, night depository areas, etc. that are provided with camera coverage should be provided with a minimum of 55 Lux of illumination.

Parking lots provided with camera coverage should have a minimum of 11 Lux of illumination at ground level.

Supplementary surface lighting may be necessary to provide adequate illumination for the face of anyone using an ATM or other self-service resource.

## APPENDIX C – SYSTEM DOCUMENTATION AND SITE PLAN EXAMPLES

### SYSTEM EQUIPMENT INFORMATION:

Recorder Make and Model \_\_\_\_\_

Multiplexer Make and Model \_\_\_\_\_

Camera/s Make and Model \_\_\_\_\_

Are any cameras infrared-sensitive, and if so identify them \_\_\_\_\_

Video Format (circle) VHS SVHS DVR (Digital Video Recorder) PC  
OTHER \_\_\_\_\_

If Digital Video Recorder or PC-based:

Hardware Manufacturer \_\_\_\_\_

Software Name and Version \_\_\_\_\_

Is a copy of the most current maintenance/service log attached? (circle) YES NO

Does the system record multiple cameras? (circle) YES NO

If yes, how many? \_\_\_\_\_

### Contact Information:

Point of contact for recording system:

Name \_\_\_\_\_ Phone: \_\_\_\_\_

Point of contact for institution:

Name \_\_\_\_\_ Phone: \_\_\_\_\_

IF SYSTEM RECORDS MULTIPLE CAMERAS, NOTE CAMERA LOCATION AND ANGLE VIEW (EXAMPLE DIAGRAMS ON FOLLOWING PAGES)

### ADDITIONAL INFORMATION TO INCLUDE IN THE EVENT OF LAW ENFORCEMENT RESPONSE:

What record mode was the system in? (circle) 2HR 6HR 12HR 24HR 48 HR 72 HR  
OTHER \_\_\_\_\_ UNKNOWN

Does the recorded date/time accurately represent the time of day? (circle) YES NO

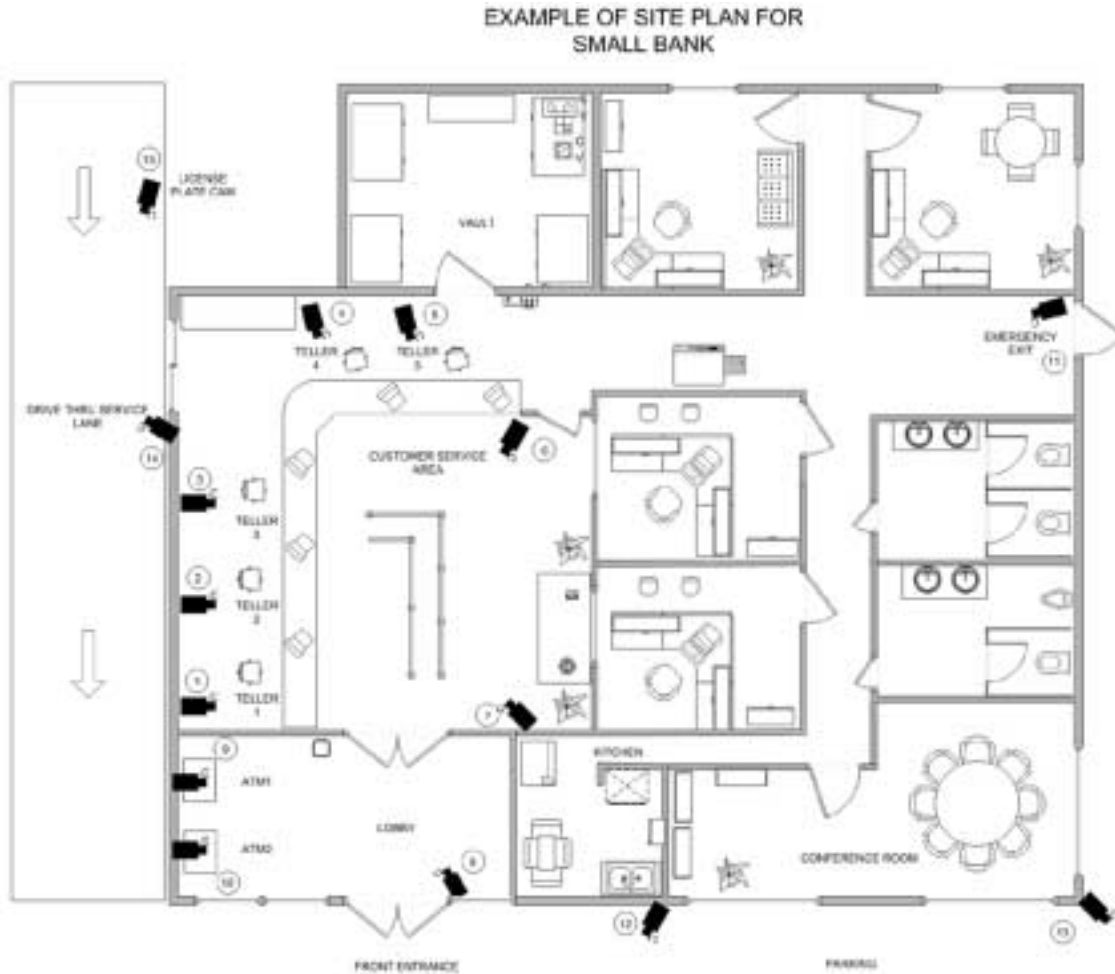
Note date/time of incident \_\_\_\_\_

Note date/time of incident on tape \_\_\_\_\_

Note date/time recording removed from equipment \_\_\_\_\_

Other Information: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_



- CAMERA 1 : Teller One Facing East
- CAMERA 2: Teller Two Facing East
- CAMERA 3: Teller Three Facing East
- CAMERA 4: Teller Four Facing South
- CAMERA 5: Teller Five Facing South
- CAMERA 6: Customer Service Area Facing SW
- CAMERA 7: Customer Service Area Facing NW
- CAMERA 8: Lobby Facing SW
- CAMERA 9: Lobby ATM 1
- CAMERA 10: Lobby ATM 2
- CAMERA 11: Emergency Exit Facing West
- CAMERA 12: Parking Lot Southside of Building
- CAMERA 13: Parking Lot South East Corner of Building
- CAMERA 14: Drive Thru Service Lane Facing West
- CAMERA 15: Drive Thru Service Lane Facing South

EXAMPLE OF SITE PLAN FOR  
CONVENIENCE STORE



- CAMERA 1 : Clerk/Check Out Area Facing East
- CAMERA 2: Front Door Entrance Facing North
- CAMERA 3: Outside of Office Facing South
- CAMERA 4: Freezer Area Facing South
- CAMERA 5: Emergency Exit Facing South
- CAMERA 6: ATM Facing West
- CAMERA 7: Parking Lot Facing SE