# In-Car Cameras

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>47</td>
</tr>
<tr>
<td>A Perspective</td>
<td>51</td>
</tr>
<tr>
<td>Benefits to the Community and Agency</td>
<td>53</td>
</tr>
<tr>
<td>How In-Car Cameras Work</td>
<td>55</td>
</tr>
<tr>
<td>Things to Consider</td>
<td>57</td>
</tr>
<tr>
<td>Challenges to Implementation</td>
<td>67</td>
</tr>
<tr>
<td>Estimating Costs</td>
<td>73</td>
</tr>
<tr>
<td>Purchasing Guidelines</td>
<td>75</td>
</tr>
<tr>
<td>Training</td>
<td>77</td>
</tr>
<tr>
<td>Sample Policy</td>
<td>81</td>
</tr>
<tr>
<td>Sample Press Release</td>
<td>89</td>
</tr>
<tr>
<td>Legal Issues</td>
<td>91</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>107</td>
</tr>
<tr>
<td>Glossary</td>
<td>109</td>
</tr>
</tbody>
</table>
Executive Summary
By Colonel Thomas (Tim) Hutchins, Secretary/Superintendent, Maryland Department of States Police

With all the technological advances of today, few have impacted law enforcement as significantly as the use of in-car cameras. The Supreme Court has referred to cameras as “the Silent Witness.” The in-car camera has become another valued tool in an officer’s arsenal that confirms and assures the high degree of professionalism they demonstrate daily in the performance of their duties. From the time the first in-car cameras were installed to document roadside DUI/DWI sobriety tests, the cameras have captured both intended and unintended video proving their value into investigations. The vast majority of the intended video recordings have resulted in convictions, serve as training videos for police academies around the world, and provide a means to expedite or resolve citizen complaints. Most video provides documentation of our officers doing their jobs and conducting themselves as professionals even under adverse and hazardous conditions. Occasionally, unintended video ends up on the evening news or as a humorous excerpt on television; however, the greatest single value of the in-car camera is that it is more and more frequently called upon to speak for the officer when they cannot speak for themselves.

For law enforcement executives, one of the most difficult obstacles to the acquisition of any new technology is the ability to obtain community support. Most new technologies come with a substantial cost and require legislative approval and funding. These approvals are often based on the community’s belief in the value of the program.

The 2004 IACP In-Car Camera Study demonstrated that 97 percent of the citizens polled across the U.S. support the use of in-car cameras for law enforcement. While law enforcement views the acquisition of camera technology as a means to demonstrate their professionalism and increase officer safety, the public views cameras as a means to guard against abuse. Despite the difference in opinions, both the public and the police support use of the technology making the acquisition and implementation of an in-car camera program a win/win proposition for all.

Planning
Prior to the acquisition of any new technology, police executives have an obligation to ensure that the equipment selected meets their agency business needs now and into the future. Establishing an agency’s business needs begins in the planning mode. Larger agencies may have the personnel and resources to assign this task, however, in the mid and smaller-sized agencies this responsibility usually falls solely with the top executive, the police chief, or the sheriff. Regardless of whether the task is delegated to subordinates or handled personally, in order to ensure an agency’s business needs are met, the executive should have a basic understanding of the technology to ensure successful acquisition and implementation.
Successful planning requires that all stakeholders be brought to the table to identify their individual needs. Possible stakeholders for consideration include the courts, the administration, the training division, forensic video examiners, supervisors, officers, and IT staff who all have an interest in the selected camera systems and will provide valuable input into the selection process. This gathering of stakeholders can also be of great help to develop a comprehensive strategic plan that encompasses the entire process from beginning to end.

**Purchasing**

Prior to the IACP becoming involved with in-car cameras in 2000, agencies had to depend on equipment vendors for guidance. Although there were many reputable manufacturers, the basic format was either VHS or Hi8 analog media. In the analog video environment, interoperability and sharing of video files were not a problem. Then came the digital revolution.

The promised benefits of pre- and post-event recording coupled with the streamlining of the video management process makes the use of digital video too appealing to ignore. Many of the manufacturers that jumped into the digital arena, often made promises that their technology could not support, and are no longer in existence. Consequently, their law enforcement customers have systems that cannot be maintained resulting in a significant financial loss to the agency and the citizens it serves.

Today there are over 60 in-car camera manufactures offering a wide range of digital recording formats. These vendors employ proprietary file encoding that require special viewing software to view the recordings. Exporting or converting these files can be difficult, even destructive. This situation leaves the executive with a major decision: Do I choose maximum recording time to save media and storage space or do I choose quality images that will provide the best evidentiary value?

**IACP Technical Assistance**

Navigating the complexities of digital video can be confusing for any police executive, but there is assistance available for law enforcement. The IACP, through grants from the U.S. Department of Justice, Office of Community Oriented Policing Services (COPS) and the National Institute of Justice (NIJ), have taken on these challenges and are providing free assistance to the law enforcement community.

The following In-Car Camera chapter contains information gleaned from the COPS/IACP National In-Car Camera Study, the COPS/IACP In-Car Camera Technical Assistance Program, and the NIJ/IACP Minimum Performance Specifications for Digital In-Car
Camera Systems. Whether you are just beginning your in-car camera program or are making the transition from analog to digital, this chapter is a must read before starting and is designed to assist the law enforcement executive in designing a system that meets your business needs now and into the future.

Developed for the IACP’s Technology Desk Reference, 2006 by Colonel Thomas (Tim) Hutchins, Secretary/Superintendent, Maryland Department of States Police
A Perspective

An officer was responding to a major incident requiring immediate police assistance. As he approached a busy intersection with lights and siren activated, he slowed to move around stopped traffic and then proceeded through the intersection. While in the intersection, he was struck by another vehicle. The officer reported that he had the green light and the right of way. No less than five independent witnesses to the accident stated that the officer ran a red light. The officer’s vehicle was not equipped with a camera; however, the secondary officer who was behind the involved officer did have his camera activated. The video evidence recovered from the secondary officer’s vehicle served as the unbiased witness and clearly proved that the involved officer’s vehicle entered the intersection on a green light and in fact proved that the citizen’s vehicle striking the officer’s vehicle had run the red light. The video evidence disputed the testimony of five eyewitnesses. A multi-million dollar lawsuit had been filed against the police agency, which was dismissed based on the video evidence. The agency recovered all the costs and financial restitution for the damages to the police vehicle, as well as medical costs for the officer.

Adapted from the IACP’s Report on In-Car Cameras, 2004.
http://www.iacpresearch.org
Benefits to the Community and Agency

The decision to install an in-car camera system should not be, “If you should do it” but, “when and how soon.” There is no other product in law enforcement today that can provide the benefits and return on investment like an in-car video system. In today’s litigious society it does not take long for a video system to prove its worth.

The modern in-car camera systems provide many benefits to officers and agencies, such as increased officer safety, training and education, decreased agency liability and as well as agency professionalism review, policy, procedure and protocol review. Many agencies and officers have been exonerated in unsubstantiated complaints against them by the mere fact that the incident was captured on in-car video. In addition, many agencies have benefited from improved community perception and support for officers actions as a result of the installation of in-car camera systems and review of camera recordings.

Chief Mike Burridge (ret.)
Farmington Police Department—New Mexico

In a recent IACP evaluation of in-car cameras, surveys were given to community members to gauge their support of the use cameras in patrol cars. 900 citizens from eighteen states completed and returned the surveys. 94 percent of responding community members stated that they support policies that include use of in-car cameras in their community. However, 71 percent suggested that they should be informed when they are being videotaped.

When asked if they would modify their behavior if they were aware that they were being recorded, 51 percent of the respondents said that their behavior would change. The citizens added that the presence of a camera would make them less likely to drive aggressively.

The participants were asked if the presence of an in-car camera would impact their decision to initiate a complaint against an officer. A significant percentage, 48 percent responded that the presence of the camera would make them less likely to file a complaint. At the opposite end of the spectrum, 34 percent reported that the knowledge of police use of cameras made them more likely to lodge a complaint. A small representation, two percent, replied that their likelihood to complain was contingent on the particular circumstances; 15 percent did not think cameras would affect their decision to complain.
In 12 of the 47 surveyed states, public forums were held to discuss the use of in-car cameras. In addition to the surveys, community perception was measured through citizen forums held to gauge the public opinion in the participating states. It was discovered that the public held several common misconceptions. The general belief was that all police vehicles are equipped with in-car cameras. There was also a perception that the camera was mobile and shadowed the officer, as on television and in the movies. Current technology limitations generally restrict camera use to a stationary wide view of the event. This misconception needs to be recognized not only by the police, who deal with the complaints regarding police practices, but also by the prosecutors’ who select jurors from the community at large. It also must be addressed in trial proceedings to ensure the jury does not have unreasonable expectations of what the video evidence can provide.

The single greatest value from the results of the public opinion survey and citizen forums is the fact that citizens support and even expect all police officers to be equipped with in-car cameras. The public recognizes that the camera systems not only help prevent the abuse of authority, but they also serve as a valuable tool to ensure the integrity of an agency.

How does an agency effectively negotiate with union representatives who may be concerned with negative aspects of the cameras use? The following facts may be useful:

| In 93% of the time a complaint is filed regarding police conduct and there is video evidence available, the officer is exonerated. |
| The officer is provided with a tool that can enhance their individual performance through self-critique. |
| The overwhelming majority of officers having used in-car camera systems do not wish to patrol without them. |
| In the worst-case scenario, the camera must speak for the officer who cannot speak for him/herself. |

When all the facts are taken into consideration, the rumors and fears begin to fade.

Adapted from IACP’s Report on In-Car Cameras, 2004.
http://www.iacpresearch.org
How In-Car Cameras Work

Source: IACP’s In-Car Camera Report

This section is included in the Technology Desk Reference (TDR) to offer chiefs a brief introduction to in-car cameras. It is designed to give executives a basic understanding of the technology system they are considering for purchase, and is not designed to be a comprehensive review of all technical considerations.

As law enforcement executives develop technology systems to meet the needs of their specific agencies, additional information on the benefits and considerations of future pieces should be sought. This section is written to help non-technical persons understand the basics of how systems work, the meaning of common terminology used, and the implications of choosing one technology over another.

Every effort has been made by the IACP’s Technology Technical Assistance Program (TTAP) to ensure that this section incorporates the general issues related to in-car camera technology. However, law enforcement administrators should be cautious that no primer can meet all the needs of any given law enforcement agency. Each agency needs to tailor its research to its unique technology needs.

An in-car camera system is, essentially, a closed-circuit television (CCTV) system designed specifically for use in motor vehicles. Some in-car systems are simply compact camera/recorders, much like consumer camcorders, that are mounted on the dashboard of a patrol vehicle. Because of the possibility of these cameras breaking loose in an accident, and because they are vulnerable to theft or damage by violators, the IACP does not recommend this type of device.

By far, the most common in-car video recorders consist of several components electronically linked to form a system within the vehicle. The usual configuration includes a front-facing camera, a wireless microphone worn by the officer, a control panel, a monitor, and a video recorder. Some agencies may elect to add a second camera and microphone that monitor suspects in the back seat of the vehicle. Typically, analog (VHS) recorders are housed in a climate-regulated, tamper-proof enclosure in the trunk of the vehicle. Newer digital recorders may be located under a seat, within the dashboard, or a number of other safe, convenient locations within the passenger compartment of the vehicle.
In addition to the in-car equipment, any agency implementing a mobile recording program must have the capability to view, copy, and store the video collected in its vehicles. A comprehensive policy covering the collection, storage, and dissemination of the recorded video is critical for the success of any in-car video program, but it is especially important for agencies with digital recording devices. Digital video can require vast amounts of storage space on a server, so it is very important to develop a strategy for managing these digital assets without damaging potential evidence through compression of video files. The transfer of digital video files from the vehicle to the onshore storage system must be secure and maintain the integrity of the original video recordings.

Both digital and analog systems require proper installation and maintenance, in accordance with the manufacturer’s recommendations. The IACP recommends that the system is tested at the beginning of each officer’s shift to ensure the proper operation of the equipment.

Adapted from IACP’s *Report on In-Car Cameras*, 2004.
http://www.iacpresearch.org
As the in-car video industry embraces the needs and demands of law enforcement, it becomes increasingly important to leverage the technology to meet specific needs. Agencies need to develop a strategic plan that incorporates the entire in-car video subsystem, from camera capture to secure transfer and storage. It is not enough to simply buy a product represented as the latest and greatest in technology. It doesn't matter how sophisticated any system is engineered. Depending on the size of the agency or program a well designed support system is needed to ensure success. Agency or department heads should be willing to devote the necessary resources, to include staffing, to support 'the system'.

A successful system implementation will include agency support at all levels. That may require time and careful oversight. The impact of having a successful system will require the support of local and state prosecutorial agencies as well as Justices of the Peace, Commissioners and Judges. Agency heads should consider the marketing of the system to local elected officials and community groups. The benefits of in-car cameras are many and any drawbacks are offset by enormous returns on any investment in time and/or public funds.

Lieutenant Jim Davis
Los Angeles County Sheriffs Department—California

When instituting an in-car video initiative, an agency must take into consideration how to collect, track, review, analyze, and store their recorded video. Police officers and supervisors must have equipment available to them in order to review and copy a video for training or evidentiary purposes.

In recent years, the proliferation of affordable video technology has resulted in a rapid increase in the use of surveillance systems in businesses, schools, government offices, even churches and private homes. Law enforcement has been challenged to manage vast amounts of video evidence from various sources. Many agencies have elected to maximize the value of their investments in in-car video by integrating video management and support functions into an enterprise-wide strategy for handling video evidence. This strategy supports investigative review and analysis of video from many sources, including in-car camera footage, recorded interviews, surveillance footage, video recovered from a crime scene, or incidental video that may provide evidence of a crime or investigative leads.
The following four levels of video support systems detail the benefits that can be achieved by in-car camera programs, and the varying requirements needed for each level.

**Level 1—Basic In-Car Video Support**

- This is the minimum level of support needed by agencies with an in-car camera program. The agency must be equipped with playback and recording equipment compatible with the in-car system in use. This will allow for the review and duplication of tapes or tape segments. A log of videotapes for archives and monitoring of tape use must be maintained. Depending on the size of the agency, there may be one log or, more likely, one at each patrol district. If advanced levels of video support are instituted, officers should have access to the equipment to afford the opportunity to review tapes for the purpose of report writing and case preparation.

**Level 2: Expanded Video Support**

- While primarily designed to support the in-car program, an agency may elect to offer expanded video services by adding additional playback formats for conversion, duplication, or capturing and printing still images. The services or access to the equipment (with proper training) would be made available to investigative divisions. Digitization of analog video could be supported to create CD, DVD, or streaming video conversions for distribution or archiving. A log would be maintained for tracking tapes and documenting caseload.

**Level 3: Agency-Wide Video Support, and Basic Forensic Video Analysis**

- This level includes the establishment of centrally located audio/video support for all investigations involving video processing within an agency. Additional specialized equipment can include de-multiplexers, time-lapse VCRs, time base correctors, or photo printers. A digital forensic audio/video analysis system should be considered and or included at this stage. Computerized case tracking and evidence management is recommended at this level, as cases may include digitally processed video as well as the original tape or video file. The video examinations at this level and above may be significantly more complex than simple contrast and brightness adjustments. Therefore, personnel should be required to receive comprehensive training in the specialized techniques and procedures, including courtroom testimony. Because of the time and effort required for this level of video support, basic support systems for quick review and copying of tapes should still be available to line officers, preferably located in patrol stations. Any video considered to be evidentiary should be forwarded to the central video support unit for examination, ensuring chain of custody procedures are followed.
Level 4: Advanced Forensic Video Analysis, Inter-Agency Support—The most advanced and extensive level of support, the forensic video analysis unit will provide full-service audio/video examination and support. It includes a digital forensic video analysis system, network connectivity, and secure wide area network access to stream video clips to investigators throughout the agency. A secure communication system with the District Attorney’s office and other agencies may be in place to foster information sharing. Digital asset management software should be utilized to maintain video files in a “virtual property room.” If possible, the agency should consider adding support for professional broadcast video formats, to facilitate analysis of news tapes and distribution of material to media outlets.

Note: Video examinations performed at Levels 3 and 4 may be subject to crime laboratory accreditation guidelines as set forth by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB). Agency managers should be familiar with ASCLD/LAB accreditation guidelines and local regulatory requirements when considering the establishment of a forensic video analysis unit. Specific training and/or certification of personnel may be required for accreditation.

Many agencies use audio, video, and imaging technology for a wide variety of tasks, from undercover surveillance to monitoring local newscasts. By identifying all these technical and human resources, an agency may be able to negotiate more cost-effective supply and maintenance contracts, build internal support and training infrastructure, and expand operational capabilities.

To best assess an agency’s needs for audio/visual support, the IACP has developed the Agency Video, Audio, and Imaging Inventory (in this chapter). This checklist, will help identify all the resources currently in use within the agency.

Managing Video Evidence
As Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA), standards stipulate, “The products of this technology could become an important piece of evidence in any type of case and should be maintained in a way to insure the integrity of contents. When tapes become evidence, they should be treated as any other evidentiary items…” Therefore, all recordings should be treated as potential evidence until it can be established that the contents are not required as evidence in either a criminal, civil, or administrative matter.

The issue of storage and management of audio/video recordings has become one of the largest obstacles agencies have had to overcome. The purchase, acquisition, duplication, and storage of recorded media requires personnel time, space, and resources. Planning for maintenance and protection of the integrity of recorded media is essential in developing an in-car camera management plan.
Once an audio/visual recording is admitted as evidence in a court of law, the test for admissibility becomes whether an officer can authenticate the audio/video recording as a true and accurate depiction of what transpired during the incident. However, to prevent incriminating evidence from being presented at trial, the defense may challenge the recording’s admissibility based on the chain of custody. Although prosecutors across the country are divided on whether video recordings fall into this category, the best policy, as with any physical evidence, is to always guard the integrity of the evidence and ensure policies and procedures maintain a strict chain of custody and are followed.

During IACP’s impact evaluation, discussions with the mid-level managers highlighted a common concern about the increased amount of time supervisors dedicate to reviewing and copying tapes along with the limited amount of space available for secure storage. As an in-car camera program expands this demand on valuable time will only increase. A mathematical example: Agency AAAA has 100 video enabled patrol vehicles and the average analog recording media is changed out or turned every 5 days. This means the agency goes through approximately 5,000 analog media (VHS or Hi8) per year. Supervisor B is assigned as the recorded media custodian at a district. Supervisor B’s salary is approximately $30.00 per hour. It takes supervisor B on the average 15 minutes to recover the recorded media from the patrol vehicle, log it in and place the media in a secured environment. Supervisor receives 30 requests per month to reproduce segments of the media for prosecuting attorneys or the defense attorneys. This process takes anywhere from 45 minutes to two hours depending on the length of the incident and the fact that the copies are made in real-time. Based on the aforementioned facts, the agency will spend approximately $59,100 in administrative labor costs per year. Underestimating workload and costs were common problems experienced by the majority of the agencies participating in IACP’s study.

**Acquisition and Storage of Recorded Media**

The majority of police and highway patrol agencies studied are currently using analog video as their recording media. Issuing, ordering, filing, retrieving, and copying videotapes, are all labor-intensive tasks. The most efficient way to deal with the majority of these tasks is through automation. Automated storage systems designed to manage recorded media are currently available. As in-car camera projects expand, automation will prove to provide long term cost savings. On a cautionary note, before investing in a media storage system, ensure that the system has an open architecture that will handle all your recorded media needs. A media storage system should be capable of handling analog and digital formats, as well as multiplex recordings. The open architecture should also allow for expansion and must be upgradeable as new technology becomes available. Purchasing an open system allows the agency to select or change recording equipment as needed without limiting the agency to a specific brand or model. Purchase of a proprietary system may handicap the agency’s ability to advance their technology.
Camera Deployment

The study found that in-car cameras have been primarily distributed to departments based on personnel and geographical regions. In some cases the camera systems were deployed equally or proportionately to all districts across the state; in other states, camera systems were provided to areas and assignments that would benefit the most from the new technology. For instance, counties with the highest average alcohol related crashes, largest number of D.U.I. arrests, areas that had the highest volume of traffic stops, or to specific areas where officer safety was of the greatest concern. Those agencies that selected personnel as their deployment criteria reported that they issued camera systems to many of their high activity personnel and personnel who would perform higher risk activities such as drug interdiction or D.U.I. task force members. Other state agencies equipped every new patrol vehicle with camera systems.

Although equity in the disbursement of equipment and new technology is understandable, this policy creates problems when managing, controlling, training and implementing new programs. Therefore, it is recommended that agencies implement in-car cameras incrementally (by district or barrack) to make the most of limited resources and allow for future program development. Incremental implementation allows for a smoother transition and new challenges to be met and addressed. Subsequent installation and implementation of in-car cameras in the remaining districts should then be seamless.

Determining Storage Requirements for Digital Video

Implementing a digital video program requires a significant investment in digital storage technology. Typically, a digital in-car system will require 500MB to 2.5 GB of storage for each hour of recorded video. To determine the storage requirements for an agency, you must first determine how much video is being recorded. When the recorder is activated and stopped will be determined by agency policy but the IACP and industry research have found that, on average, agencies generally record between 1.5 and 2.5 hours of video per officer per 8-hour shift.

Another important consideration when determining an agency’s storage needs is the retention period of digital video files. Every jurisdiction may have legal or policy requirements governing how long in-car video recordings must be maintained. Some agencies may keep them as long as two years, while others may be required to destroy the files after 30 days. (The IACP recommends storing the files at least one day longer than the statute of limitations for complaints filed against officers.) Major events, such as pursuits, felony arrests, officer accidents, etc., should be archived indefinitely.

The following equation can be used to determine storage needs:

\[ \text{Number of equipped vehicles} \times \text{number of shifts per vehicle} \times \text{hours of recording per shift} \times \text{retention period} \times \text{file size per hour of video} = \text{minimum storage required.} \]
Example – Agency A has 20 video-equipped vehicles, each of which is used by 3 shifts every day. On average, each shift records 2 hours of video at 1.5 GB per hour. All recordings are retained for 30 days.

\[
20 \text{ cars} \times 3 \text{ shifts} \times 2 \text{ hours} \times 30 \text{ days retention} \times 1.5 \text{ GB file size} = 5400 \text{ GB}
\]

In this case, a server with just under 3 terabytes would be required for 30 days of video, provided that one complete day of video is always deleted on its 31st day. To ensure adequate capacity, an additional allocation of storage—perhaps as much as 50 percent—should be considered. Any files maintained beyond 30 days will require additional permanent storage in a secure location, possibly on a separate server or permanent WORM (write once, read many) media, such as a DVD-R.

**Digital Video File Formats**

Possibly the most confusing aspect of digital video is understanding the differences among the various file formats. There are a number of industry-recognized file formats for digital video, each with its own technical advantages and limitations. MPEG, MPEG-2, MPEG-4, H.264, wavelet, and Motion-JPEG are some of the common terms used to describe the recording format of a digital video system. And though there are industry standards governing each of these formats, there are a wide range of variables within the format the software developer can use to customize the files to meet the needs of the manufacturer. To make matters worse, each manufacturer designs the recording process with proprietary programming that makes it nearly impossible to make a side-by-side comparison of performance specifications. As a result, agencies are faced with a bewildering list of technical details that provide little or no help when it comes time to select a system based on video quality.

Digital images contain vast amounts of information. Anyone who uses a digital still camera understands the storage requirements of 4 mega pixel or larger pictures. Video is essentially a series of still images, and the addition of motion in video recording increases the file size dramatically. Processing and storing files of that size would require a system that would far exceed the budget of any police agency.

Compression is a process that reduces the amount of data in a video file for faster image processing and smaller file size. Compression allows the practical recording and management of video. Unfortunately, it can also be very damaging to image files. Therefore, manufacturers have spent a great deal of time and resources on developing compression/decompression algorithms (codecs) that reduce file size while maintaining reasonable image quality. Frankly, some results have been more successful than others.

Because of the complexity of image compression and the proprietary design of each vendor’s codecs, it is not possible to identify one file format or codec as superior to another. Sometimes
and MPEG-2 file may look better than a MPEG-4, but requires significantly more storage space. A motion JPEG might capture movement and maintain detail better than another format of similar file size, or a wavelet format could be cleaner than either. It is left to the customer to weigh the advantages of reduced storage requirements against the quality of the images being recorded to determine which system is right for a particular agency. Because we consider officer safety as the primary reason to install in-car cameras, the IACP strongly encourages agencies to give image quality and reliability a high priority when selecting a vendor. The images and sounds recorded by these devices are evidence, and as such, should be handled with appropriate care.

Adapted from IACP’s Report on In-Car Cameras, 2004.  
http://www.iacpresearch.org
Agency Video, Audio, and Imaging Inventory

Use this form to identify units and personnel employing video, audio, or imaging technology within your agency. Identifying these resources may help your agency maximize their value through the sharing of knowledge and support. There may also be cost savings realized by centralized procurement of equipment and supplies. Check the box next to each application in use in your agency, and identify the division or command to which it is assigned. Check the box in the column marked D if digital technology is used, and the box in the column marked A if analog equipment is used. (In some applications, both analog and digital technology may be in use.) The blank lines can be used for applications not otherwise identified on this form.

### VIDEO

<table>
<thead>
<tr>
<th>Application</th>
<th>Division or Location</th>
<th>D</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Production Unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crime Scene Unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accident Investigation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tactical Units/SWAT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Covert/Surveillance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patrol Vehicles</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Robbery/Investigation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification Unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crime Laboratory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jail/Booking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interrogations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility Security (CCTV)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### PHOTOGRAPHY/IMAGING

<table>
<thead>
<tr>
<th>Application</th>
<th>Division or Location</th>
<th>D</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crime Scene Unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accident Investigation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tactical Units/SWAT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Latent Prints/ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crime Laboratory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forgery/Documents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sex Offender</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jail/Booking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### AUDIO

<table>
<thead>
<tr>
<th>Application</th>
<th>Division or Location</th>
<th>D</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tactical Units/SWAT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio Forensics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interrogations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Covert/Surveillance</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Challenges to Implementation

One of the first challenges in implementing an in-car camera program for a small police department is the budget. For some small departments the need is there but the funds are not; this may mean that the chief has to approach the city council or governing body for the additional funds. While the fact of the conveniences of having the in-car cameras sometimes are a hard selling point, a chief using the argument of officer safety is often successful.

Implementing a departmental policy and training the officers in that policy, is essential for the success of the program. Chiefs must make sure they develop a policy that will work for their department. The officers must know that the in-car camera is not something the chief installs in the car to catch them not doing their job, but as an important tool in the job. The benefits of recognizing and addressing these and other challenges leads to a more professional job accomplished by your officers, more convictions, fewer citizens complaints and another valuable technology asset for your agency.

Chief Montie Sims
Dardanelle Police Department—Arkansas

Prior to installing the first in-car camera, departmental policies and procedures regarding use, storage and handling of the video evidence must be in place. This approach ensures the future admissibility of video evidence in court. Users should be properly trained in the operation of the equipment as well as federal and local laws relating to the use of electronic capturing of audio and visual images. The IACP study revealed that training needs to go beyond the users to the executive levels. Executives must have a basic understanding of the technology to ensure its compatibility with the agency’s video evidence needs.

User perception is an additional factor that must be addressed when implementing an in-car camera program. If officers believe that the system is only being installed for disciplinary purposes, the program will falter and may fail. An agency can use the lessons learned through pioneer participants in this study to increase the chances for a successful in-car camera program.

Implementing an effective program requires more than simply purchasing and installing camera systems. A comprehensive video management plan must be in place. As we
enter the digital age, planning for a system should be developed from the back-end (storage, filing and retrieving images) to ensure that technology will support the system selected. In addition, the plan begins with a broad assessment of an agency’s video evidence needs and should bring together all parties with an interest in the success of the program. Prosecutors are integral to this process. Ultimately, they will have to defend the video medium selected in court. The video management plan must provide a means for proper installation and maintenance for the systems. Key considerations when selecting a system include the durability and reliability of the system; assurances of officer safety through the placement of the various components; and ease of operation.

Today’s in-car camera enjoys overwhelming public support and can enhance an agency’s image while ensuring integrity and accountability. Camera technology, if applied properly, will enhance officer safety and provide valuable insight on the effectiveness and application of departmental policies. When it comes to purchasing technology, police executives must avoid the temptation to settle for an off-the-shelf technology solution when that solution may not meet an agency’s needs. Technology designed for a city police department may not be suitable for a state agency. Police must be educated consumers of technology. This was illustrated by the industry’s reaction to IACP’s Line Officers Roundtable in January 2003, where the in-car camera users identified problems with their in-car camera technology and made specific recommendations for change. By the IACP Conference in October 2003, every major manufacturer of in-car camera systems encompassed the user requested changes.

The in-car camera is a multifaceted tool that assists police executives by ensuring integrity and accountability while enhancing public trust. In-car cameras allow officers to critique and enhance their performance and provide training material for new recruits and advanced officer training. With the proper education, video evidence can be of great value to prosecutors as well as police. Video evidence can be used to refresh an officer’s recollection of events while validating the officer’s testimony. In many cases when video evidence is present, both time and money can be saved if the defendant elects to plead guilty to the charges. In civil, criminal, and administrative cases, the presence of video evidence streamlines the investigative process and allows an agency to come to a timely conclusion. Even when revealing departmental violations, video evidence allows investigators, supervisors and executives to make sound assessments of the facts. With videos, mitigating circumstances that may impact the severity of discipline can be addressed.

This information is designed to help agencies create an organized plan of action that will serve as a blueprint for the successful acquisition and implementation of an in-car camera program. A comprehensive plan takes into account all of an agency’s video evidence needs and will assist in the assessment, design, selection, acquisition and implementation processes.
When purchasing, installing, or repairing in-car cameras, officer safety should always remain the number one priority:

- Overhead consoles with protruding corners should be avoided. In the event of a rollover accident, these sharp corners may cause serious head trauma to vehicle occupants.
- The camera casing should be mounted forward on the windshield and rest in front of the rearview mirror. This will minimize the peripheral obstruction of view and remove the camera from the passenger side airbag deployment zone.

**Acquisition**

**Problems:**

- Experiencing delays in the delivery of the in-car camera systems
- Awaiting legislative approval for spending authority delayed bid process
- Changes in new computer technology delayed bid opening
- Vendors questioning the bid process delayed closing the bid

**Solution:**

Careful development and dissemination of a request for proposals (RFP) can help avoid many of these problems. The IACP publication, *In-Car Video Camera Systems Performance Specifications Framework: Digital Video Systems Module*, was designed for use as a model RFP that can be easily customized to an agency’s specific needs. Be sure all terms for delivery, installation, maintenance, and payment are clearly defined and understood by bidding vendors.

**Equipment**

**Problems:**

- The number one complaint was with the poor quality of the audio portion of the recording
- More specifically, the transmitters were providing poor reception, the microphones were too fragile and the life cycle of the batteries were insufficient
- Excessive vibration on dash mounted cameras caused excessive system failure
- Poor quality recording media is causing poor quality recordings

**Solution:**

New generation digital audio systems have addressed most of the problems associated with older analog equipment. Digital transmission is much more reliable than analog. Before purchasing a product, it is important to have each bidding vendor install one or more units in your vehicles so they can be tested under the actual conditions in which they will be deployed. Reviewing the recordings on a large monitor, as they would...
be presented to a jury, will allow an accurate assessment of the video quality before buying.

**Installation**

**Problem:**
Improper installation has caused multiple problems with the monitors and cameras. For instance, improper mounting can cause video recorder failure. One agency reported that 15 percent to 20 percent of units broke due to human errors.

**Solution:**
Installation must be completed in strict accordance with manufacturer’s specification. Terms for installation and maintenance must be clearly spelled out in the RFP. Optimally, the vendor or vendor trained and authorized personnel will perform all installations and maintenance. Be sure the warranty takes effect upon installation, not delivery. Remember that proper training of personnel who actually use the equipment is as important as the training of those who install it.

**Management/Administration**

**Problems:**
- The collection, storage and cataloguing of videotape evidence is becoming a tremendous burden, especially for agencies that do not employ full time technicians assigned to the task. In most police agencies available storage space is at a premium.
- The absence of policies and procedures that dictate the use and explain the operations of the in-car camera equipment.
- Officers are not provided with adequate training for the use and operation of the in-car camera.
- Lack of funding for service contracts after the warranties on the existing equipment expire.
- Not having factory trained representatives on-site for repairs.

**Solution:**
The IACP strongly recommends that any agency embarking on an in-car video program consider the storage and management of the recorded media before purchasing the in-car equipment itself. Especially with digital recordings, the storage and management system may be more costly in fiscal and human resources than the camera systems. In-Car Video Camera Systems Performance Specifications Framework: Digital Video Systems Module includes guidelines for handling the recorded materials, which should be treated with the same care and security as other physical evidence. The storage system will be, in fact, a digital property room, and access to the files should be restricted and tracked to maintain the chain of custody. Beware of compression of video files, as the process is very destructive and can seriously damage the recorded evidence. Use the formula (see Things to Consider–
Human Element

Problem:
Negative attitude directed towards the forced use of the in-car camera must be overcome. Agencies had to overcome the hurdle of officers being reluctant to use the in-car video systems, believing that the system purpose was to allow “big brother” to be watching, or destroying or disabling camera systems by officers that do not wish to participate. Now patrols that do not have systems are asking for them, after seeing all the positive effects they can have towards making their jobs easier, especially in the elimination of citizen/officer complaints.

Solution:
The best way to deal with the human element is to ensure officers using this equipment are properly trained in the use and operational functions of the equipment. Another preventative measure is to ensure a strong departmental policy is in effect prior to implementing an in-car camera program. A strong policy will set out conditions of use and officers responsibilities. (See Sample Policy section in this chapter) The best way to secure compliance is with the facts. The IACP study on in-car cameras found that the use of the devices exonerated the officer in 93 percent of complaints when the incident was recorded and officer safety was greatly improved.

Warning! If the officers’ believe that the cameras are being installed strictly for the purpose of disciplinary actions, the agency’s program will be plagued with broken equipment and little support from the rank and file.

Adapted from IACP’s Report on In-Car Cameras, 2004.
http://www.iacpresearch.org
Estimating Costs

Source: IACP’s Report on In-Car Camera

Planning and purchasing technology involves careful consideration of long term and short term budgeting. Technology costs are not limited to the initial expense of equipment purchase but include recurring expenses, ongoing training and infrastructure support. It is essential that law enforcement agencies carefully account for all related costs when preparing for a technology purchase.

This section lists some of the expenses that should be accounted for when planning a technology acquisition. This list should not be considered exclusive and to create a comprehensive cost estimate, departments should develop a full request for proposals. Additionally, consultants that specialize in communications systems may assist departments in determining projected costs.

Preparation for Purchase of In-Car Video Systems

Estimating the cost of purchasing and operating mobile video equipment can be difficult, especially with digital recording systems. It is important to keep in mind that the costs associated with in-car camera systems, like any technology, extend well beyond the price of the equipment alone. In fact, the necessary support infrastructure could be far more expensive than the equipment installed in vehicles. For this reason, the IACP urges agencies to develop a comprehensive policy first, to help determine the storage, management, and support requirements of the agency. After these steps are completed, the agency can then find the mobile video system that will best meet its business needs.

Storage and Management

Agency policy will determine how much video is recorded by establishing rules for use of the equipment. The IACP Sample Policy can help to identify circumstances under which the use of the video recorder should be mandated and when the recorder should be stopped. Research conducted for this report found that, on average, an officer would record approximately of 2.5 hours during an eight hour shift. At this rate, a T-120 tape operating in the 8-hour (SLP) mode would last about three days.

Digital recording, however, is much different. Every manufacturer of digital recording systems has its own proprietary recording system that compresses very large audio/video files to reduce the storage requirements. The compression process can be very damaging to the quality of the video image, so it should be kept to a minimum to preserve the recorded details. This, of course, results in larger file sizes and a greater storage requirement.
Hardware
Many vendors market their systems with proprietary storage systems that lock an agency into a long-term relationship. As an alternative, an open architecture, “off the shelf” storage system will likely save the agency money on initial hardware acquisition and provide greater flexibility and scalability in the future. Viewing stations where officers and supervisors can view recordings and, according to agency policy, make copies of video files should be included in cost estimates.

Estimate storage requirements based on agency policy governing the use of the in-car systems. Base storage estimates on uncompressed transfer of files from the vehicle to the storage medium. Agency policy should determine how long the files must be maintained at their highest quality, and if they can later be compressed for long term archiving. These calculations are important to determine storage capacity; an initial purchase of 50 percent more storage capacity than calculated is recommended. Service agreements and warranties must be considered for ongoing maintenance.

Software
Media management software is available from most digital video vendors, as well as commercial off-the-shelf products. Again, an open architecture is recommended for interoperability with existing systems and cost-effective management of the system. Software that allows the addition of metadata from numerous sources (reports, photos, warrants, etc.) will greatly enhance the value of the video management system. Service agreements must be included in the initial purchase and budgeted for maintenance of the system in the future.

Mobile Video System
In addition to the up-front cost of the in-car video hardware, it is important to identify any additional costs that may occur, such as modification of a vehicle to accommodate the recording system, installation and maintenance costs, service agreements, and expendables like batteries and portable recording media. If the system utilizes wireless technology for the transfer of recorded media from the vehicles to the storage system, the cost of the appropriate number of wireless receivers must be included.

Maintenance
Regular maintenance is critical. The manufacturer will provide a maintenance schedule.

Training
Officers should be thoroughly trained in the operation of the equipment, as well as policies and procedures with an emphasis on officer safety.

Adapted from IACP’s Report on In-Car Cameras, 2004.
http://www.iacpresearch.org
Purchasing Guidelines

Because of the rapidly changing nature of technology, it can be difficult to stay current on technology upgrades. Performance specifications and technology standards are the underlying “laws” that govern the development of local, national, and international services, networks and procedures. Telecommunications networks worldwide use formal telecommunications standards to physically interconnect their systems and ensure that they perform as expected. Without agreements and the standards that codify them, wide-area voice, data, and video communications would not be possible.

The IACP’s stated mission is to establish minimum performance specifications for digital recording systems to enhance 1) officer safety, and 2) the effectiveness of audio/video evidence by identifying the scientifically measured, minimum performance levels appropriate for use by law enforcement. The challenge facing the Advisory Panel is to develop answers to the following two questions:

- How can the performance of digital in-car video systems be objectively measured?
- What level of performance is necessary and appropriate to meet the needs of law enforcement?

The IACP continues to work with representatives from law enforcement, industry and its federal partners to develop comprehensive digital in-car video minimum performance specifications, together with a valid and reliable testing and certification program. The objectives of this collaborative effort are:

- To provide law enforcement with the minimum performance specifications needed to ensure and acquire safe and reliable digital in-car video operating systems
- To provide guidance for manufacturers on the minimum performance specifications their products need to perform in a law enforcement environment

These specifications will provide for consistent evidentiary use of recorded sounds and images during the operation of the systems.

Responding to direction and needs from the field, the IACP, in partnership with the National Institute of Justice, Office of Science and Technology, completed the first draft for public comment of the Digital In-Car Video Systems Specifications for Law Enforcement Framework in July 2006.
Objective measurement of the quality of video images presents formidable challenges, and at the release of this document no appropriate method for measurements has been identified. For that reason, the first draft of the document should be viewed as a framework, which lays the foundation for the establishment of measurable performance specifications. The IACP is actively working with the scientific community to develop a method to objectively quantify image quality, and will add them to this document as soon as they are available.

The final system specifications, as of the printing of the TDR, have not been officially approved. The anticipated approval will occur some time after the first of the year, 2007. It is strongly recommended that your agency check the IACP Web site frequently for a sample RFP and the final version of the specifications. This information will be available electronically on the IACP Web site at the following locations:

Cutting Edge of Technology Project
http://theiacp.org/research/RCDTechCuttingEdge.html

In Car Camera Technical Assistance Training
http://theiacp.org/research/RCDTechPoliceInCar.html
Training

Source: IACP’s In-Car Camera Report

In many departments, the use of in-car video in police vehicles has now become customary and/or required police equipment. Each day, more and more vehicles are being outfitted with this evidence collection system. Officers are beginning to accept and use this unbiased witness to their advantage, by reducing complaints, saving court appearances, and increasing their safety. Some officers and/or departments will place a vehicle out of service for the lack of a working video system.

With any new piece of equipment, a certain amount of training is needed to insure its successful implementation. In the case of the in-car video system, a need for training is compounded by the broad range of incidents that a patrol officer will record. Also, in departments where the use of the camera is required, training must be mandated for disciplinary purposes and regular inspections/repairs documented.

The bottom line is that video from a police vehicle is evidence, just like a shell casing or a suspect’s written confession. In some cases, this will be the only evidence. For this reason, the camera operator (officer), the repair technician, the evidence or records custodian and anyone else who uses or services the unit, must be trained and certified for the system. This includes the copying or transmission of video and its storage. Training should address all issues that withstand a reasonable court challenge. Reputable camera system vendors will provide instruction/certification for train-the-trainer and use training. Vendors must also certify technicians and be willing to testify as to reliability and accuracy of their systems.

The scene that should run through our mind is one of the officer down and the suspect driving away. When this happens, it is too late to discover that the officer did not know how to focus the camera, the microphone wasn't on, or that the tape ran out last week. Planning, training and documenting will go a long way in the acceptance, reliability and future of your in-car video system.

Captain Robert Liberati
Prince George’s County Police Department—Maryland
The value of the in-car camera for the purposes of training cannot be overlooked. Not only are officers using the cameras as an effective tool for self-critique, they have found them to be an invaluable resource for training new officers. New officers can review their actions with their training officers through the objective eye of the camera immediately after an event occurs. It is important to remember that recordings from the field that depict either positive or negative police behavior are an asset to the training division of any agency; however, care must be taken to present the material in a way that will not embarrass an officer or undermine morale.

A successful in-car camera program requires that the users, managers, and judicial recipients have a clear understanding of how the equipment operates, its limitations, and the potential drawbacks of the equipment. An effective program requires an understanding of the technology and unique issues involved in in-car video recording throughout the chain of command.

The following course of action is recommended:

- Implement a course of instruction that incorporates pertinent laws, Federal Rules of Evidence, departmental policies and procedures, and use and operation of the audio/video equipment
- Implement an introductory in-car camera course designed specifically for new recruits
- Implement a refresher course for advanced officer training

As with any new technology, failure to properly train officers in the use, operation, and legal implications of improper use can result in disaster.

**Agency Policies, Procedures, and Protocols**

A valuable lesson learned from IACP’s Impact Evaluation was the need for any agency implementing an in-car camera program to have a strong and clearly defined policy in place prior to system implementation. In 2001, CALEA issued standard 41.3.8, regarding agencies that use in-car audio/video recording systems. The standard requires that any policy and/or procedure must address situations for use, tape security and access, and tape storage and retention schedule.

The in-car camera documents the actions and demeanor of both the violator and the officer. A police chief may regard the in-car camera as a method of ensuring honesty, integrity and accountability. However, the officer may regard the same equipment as a disciplinary tool. This difference in philosophy must be taken into account when implementing or measuring the effectiveness of an in-car camera program.

The value of an in-car camera program hinges, to a great extent, upon the willingness of officers to record their daily actions and subject themselves to periodic scrutiny. The agencies studied have made excellent inroads with this difficult task. Almost all of in-car camera
policies reviewed for IACP’s study mandate that all traffic stops, police pursuits and citizen contacts be recorded in their entirety. The policies of many agencies have also highlighted the value of in-car cameras by demonstrating that officers are performing professionally.

**Supervisory Review**

Many agencies have developed a policy for reviewing videotapes to ensure integrity and accountability. This process is a valuable supervisory and management tool, yet a degree of caution should be exercised. If officers feel they are singled out and disciplined for minor infractions (i.e. not wearing a hat or tie) following a review of their tapes, this could have a detrimental impact on the program and an effect the morale of the officers and the program itself. Instead, these minor policy violations should be addressed through training or informal counseling.

Therefore, to ensure understanding and to promote trust with the in-car camera user, the agency may consider using the following or similar statements in their general order and/or policies and procedures:

- Minor infractions (not criminal in nature) discovered during routine review of the recorded material should be viewed as training opportunities and not as routine disciplinary actions. Should the behavior or action be repetitive after being informally addressed, the appropriate disciplinary or corrective action shall be pursued.
- Another important training consideration is the need for communication between management and the rank and file. The majority of the agencies evaluated displayed exceptional communication at all levels throughout the chain of command. In some cases, officers using in-car cameras have different interpretations of when policy requires the use of the cameras. Some officers and supervisors may be unsure of policies regarding the retention of tapes, resulting in problems with the storage of the media and subsequent chain of custody issues.
- Line officers need a clear understanding of what is expected of them. Mid-level managers and executives need to be cognizant of all problems the officers are facing and become actively involved in problem solving, while also engaging line officers in the decision making and problem solving process.

**Agency Leadership**

The in-car camera is an unbiased witness to events to ensure the accountability and the integrity of their officers. Although the “virtual ride-along” can never, nor should it ever, take the place of the personal contact between supervisor and subordinate, periodic review of the officers' recordings by the supervisor cannot be overvalued. Issues of officer safety, demeanor and professionalism can be diagnosed and addressed accordingly. The recordings, along with other supervisor observations, may serve as an early warning of an officer experiencing problems that should be addressed. The normally professional officer, who suddenly becomes easily agitated or short with the public, may alert the supervisor that the officer in question is under additional stress. The camera, in effect, can provide another level of supervision while providing additional protection for the agency against liability.
In addition, by streamlining the investigative process the agency can save hundreds of supervisory hours required to conduct a thorough investigation. The video evidence provides tangible, unbiased proof of officers’ actions. The study proved that in the majority of cases, complaints are either withdrawn or brought to a speedy conclusion when there is video evidence available to the investigating supervisor or commander.

Proper management of an in-car camera program is essential to its success. Executives must have a thorough understanding of the entire scope of needs before the instituting an in-car camera program. By utilizing the video assessment profile provided in the Challenges to Implementation section of this document, and ensuring that all parties with a vested interest are provided input into structuring of the program, police executives will be able to maximize the effectiveness of their program and ensure all needs are met.

On a cautionary note, once the agency commits to the use of the in-car cameras, the use of the systems will become the norm and not the exception. Community leaders, the courts, and investigators will expect video evidence in all cases. This became apparent during one IACP’s site visit where it was reported by officers that local prosecutors would not try a driving while intoxicated case without video evidence.

Many officers that use in-car cameras do not wish to patrol without them. Building a successful in-car camera program requires much more than the simple purchase and installation of the systems. There must be appropriate policies, guidelines, and training in place to ensure that while citizens are being protected, their personal privacy is not being violated. Agency executives and community leaders must ensure adequate resources for the proper management, storage, and retrieval mechanisms in hardware, software, and personnel are provided.

The value of this technology is self-evident. Public safety and citizen support for law enforcement will benefit from having in-car video cameras available for all police officers. All of these objectives can be accomplished through the efforts of law enforcement and our partners–the public.

Adapted from IACP’s Report on In–Car Cameras, 2004.
http://www.iacpresearch.org
Sample Policy
Source: IACP National Law Enforcement Policy Center

This policy is included in the Technology Desk Reference (TDR) as an example of procedural guidance for records and communications efforts. As law enforcement executives tailor this policy to their specific agencies, the policy will need to be redrafted in the context of existing local ordinances, provisions of union contracts and all other state and federal laws. Departments must ensure that all other related policies are updated to be consistent with the provisions of this new policy.

Every effort has been made by the IACP Research Center Directorate and the Technology Technical Assistance Program (TTAP) to ensure that this policy incorporates the most current information and contemporary professional judgment on the issue. However, law enforcement administrators should be cautious that no “model” policy can meet the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decision, and collective bargaining agreements, and each agency needs to tailor its policies to ensure compliance with all laws, regulations and agreements.

IACP National Law Enforcement Policy Center
Mobile Video Recording Equipment | Model Policy March 2005

A. Purpose
The purpose of this policy is to provide law enforcement agencies with guidelines for the use, management, storage, and retrieval of audio-visual media recorded by in-car video systems.

B. Definitions
1. Recorded Media—Refers to audio-video signals recorded on any of several storage devices, including analog tape (VHS, SVHS, Hi 8mm), digital tape (DV), or other portable digital storage devices (CD, DVD, hard drive, etc).
2. In-Car Camera System and Mobile Video Recorder (MVR)—These are synonymous terms and refer to any system that captures audio and video signals capable of installation in a vehicle, and that includes at minimum, a camera, microphone, recorder, and monitor.
3. Supervisor—Sworn personnel officially appointed responsibility for a departmental component.
4. **MVR Technician**—Personnel trained in the operational use and repair of MVRs, duplicating methods, storage and retrieval methods and procedures, and who possess a working knowledge of video forensics and evidentiary procedures. (Dependant on the size and needs of the agency, the role of the MVR Technician may be delegated to the supervisor.)

5. **Degaussing**—Electronic cleansing of analog recording media returns the media to its original state and when it is ready for the imprinting of new images.

C. **Policy**

The use of an MVR system provides persuasive documentary evidence and helps defend against civil litigation and allegations of officer misconduct. Officers assigned the use of these devices shall adhere to the operational objectives and protocols outlined herein so as to maximize the effectiveness and utility of the MVR and the integrity of evidence and related video documentation.

D. **Procedures**

1. **Program Objectives**

   The agency has adopted the use of MVRs to accomplish the following objectives:
   a. To enhance officer safety
   b. To accurately capture statements and events during the course of an incident
   c. To enhance the officer’s ability to document and review statements and actions for both internal reporting requirements and for courtroom preparation/presentation
   d. To provide an impartial measurement for self-critique and field evaluation during recruitment and new officer training
   e. To capture visual and audio information for use in current and future investigations.

2. **General Procedures**

   It shall be the responsibility of this department to ensure that the audio-video recording equipment is properly installed according to the manufacturer’s recommendations
   a. MVR equipment shall automatically activate when emergency equipment (lights) or a wireless transmitter is operating. The system may also be activated manually from the control panel affixed to the interior of the vehicle
   b. Placement and operation of system components within the vehicle shall be based on officer safety requirements
   c. All officers shall successfully complete this department’s approved course of instruction prior to being deployed with MVR systems in operational settings

3. **Officers’ Responsibilities**

   a. Inspection and general maintenance of MVR equipment installed in departmental vehicles shall be the responsibility of the officer assigned to the vehicle
   1. MVR equipment shall be operated in accordance with the manufacturer’s recommended guidelines and departmental training and policies
2. Prior to beginning each shift, the assigned officer shall perform an inspection to ensure that the MVR is performing in accordance with the manufacturer’s recommendations covering the following matters:
   • Remote audio transmitter functional
     o Adequate power source
     o Connected to the recording equipment
     o Remote activation of system via transmitter
   • Camera Lens
     o Windshield and camera lens free of debris
     o Camera facing intended direction
     o Recording mechanism capturing both audio and video information.
     System plays back both audio and video tracks
   b. Malfunctions, damage or theft of in-car camera equipment shall be reported to the immediate supervisor prior to placing the unit into service

1. A subsequent written report shall include information on the suspected cause(s) of equipment failure, as available, and any recommendations for corrective action. The supervisor shall determine if the unit shall be placed in service. If the vehicle is placed in service without an operating MVR, the emergency communications center (e.g., dispatch) shall be so informed.

4. Mandatory Recordation
   a. Traffic stops (to include, but not limited to traffic violations, stranded motorist assistance and all crime interdiction stops)
   b. Priority responses
   c. Vehicle pursuits
   d. Prisoner transports
   e. Crimes in progress
   f. Any situation or incident that the officer, through training and experience, believes should be audibly and visually recorded

The following applies to those states and jurisdictions that require two-party consent in which a person must be advised of the audio recording.

In addition to the aforementioned incidents, officers may record with the audio portion disabled anytime the officer believes such recording has a legitimate law enforcement purpose. Officers may audibly and visually record any incident in which all involved parties consent. At the beginning of any public contact or traffic stop, the officer shall notify the citizen that the events are being audibly and visually recorded. This notification does not apply to crimes in progress or similar situations where notification is impractical.

g. When the MVR is activated, officers shall ensure that the audio portion is also activated so all events are properly documented. Officers are encouraged to narrate events using the audio recording, so as to provide the best documentation for pretrial and courtroom presentation.
5. Operational Protocols

a. To prevent bleed over and/or noise from other MVRs in systems using low band transmitters (analog), only the primary officer initiating the contact shall activate his or her audio recorder.

b. Officers using the 900Mhz digital transmitters that are individually synchronized to their individual MVR shall activate both audio and video recordings when responding in a support capacity in order to obtain additional perspectives of the incident scene.

c. Officers shall review the recordings when preparing written reports of events to help ensure accuracy and consistency of accounts.

d. With the exception of police radios, officers shall ensure that the volume from other electronic devices within the police vehicle does not interfere with MVR recordings.

e. Officers shall not erase, alter, reuse, modify or tamper with MVR recordings. Only a supervisor or MVR technician may erase and reissue previously recorded recordings and may only do so pursuant to the provisions of this policy.

f. To prevent damage, original recordings shall not be viewed in any equipment other than the equipment issued or authorized by the MVR technician.

g. MVR recordings shall be marked as containing evidence and submitted to the property custodian or MVR technician to be held and/or duplicated for criminal prosecution when they record any of the following:
   1. Arrest Assaults
   2. Physical or verbal confrontations, vehicle pursuits
   3. Vehicle searches in which contraband is recovered
   4. Driving while intoxicated or under the influence arrests
   5. All prisoner transports

h. When the MVR is activated to document an event, it shall not be deactivated until the event has been concluded unless:
   1. The incident or event is of such duration that the MVR may be deactivated to conserve recording times.
   2. The officer does not reasonably believe that deactivation will result in the loss of critical documentary information.
   3. The intention to stop the tape has been noted by the officer either verbally or in a written notation.

i. The recording media shall be replaced when the recording time remaining is less than 1 hour, for long playing media lasting 6-8 hours, or 30 minutes for Hi8 analog or digital media with recording time of 5 hours or less.

6. Supervisors’ Responsibilities

a. Supervisors shall issue unrecorded media and when possible prior to issuance, shall assign and affix an identification number to the exterior of the media.

   1. The numbered media is then recorded in the chain of custody log.
2. Should the media be a computer hard drive, a computer generated file number shall be generated internally

b. The chain of custody log shall include, but need not be limited to:
   1. Tracking number of media
   2. Date issued
   3. Officer or vehicle issued
   4. Date submitted
   5. Officer submitting the media
   6. Hold for evidence indication
      (In the event an officer works at a remote location and reports in only periodically, multiple recording media may be issued.)

c. When an incident arises that requires the immediate retrieval of the recorded media (e.g., serious crime scenes, departmental shootings, departmental accidents), a supervisor shall respond to the scene and ensure that the appropriate MVR technician or crime scene investigator removes the recorded media. The technician or investigator shall then:
   - Place the media into evidence and provide copies to authorized investigative personnel
   - Ensure the appropriate notation is made in the chain of custody log

d. The supervisor shall periodically review the chain of custody log to ensure that issued media is surrendered in a timely manner. The supervisor is responsible for determining causes for such problems (e.g., unreported problems with the MVR equipment or equipment not being used in accordance with departmental policy).

e. Supervisors who are informed or otherwise become aware of malfunctioning equipment shall ensure that authorized personnel make repairs in a timely manner.

f. Supervisors shall conduct periodic reviews of officer assigned media in order to periodically:
   1. Assess officer performance
   2. Assure proper functioning of MVR equipment
   3. Determine if MVR equipment is being operated properly
   4. Identify recordings that may be appropriate for training

g. Supervisors shall conduct bi-weekly reviews of personnel who are newly assigned MVR equipment in order to ensure compliance with departmental policy. Supervisors shall thereafter conduct quarterly reviews.

h. Minor infractions (not criminal in nature) discovered during the routine review of recorded material should be viewed as training opportunities and not as routine disciplinary actions. Should the behavior or action become habitual after being informally addressed, the appropriate disciplinary or corrective action shall be taken.

i. Supervisor shall ensure that adequate recording media is on hand and available for issuance.
7. Technicians’ Responsibilities
   a. A designated officer or other employee (MVR technician) shall be responsible for the ordering, issuance, retrieval, storage, cleansing (degaussing), and duplication of all recorded media.
   b. The MVR technician shall be responsible for collecting all completed media. Once the media is surrendered, the technician shall:
      1. Ensure it is placed in a secured location with authorized controlled access; and
      2. Make appropriate entries in the chain of custody log.
   c. Recorded media may only be degaussed/erased:
      1. Pursuant to a court order
      2. In accordance with established retention guidelines
   d. For the purpose of accountability, all media will be assigned an identification number prior to issuance to the field. The MVR technician will maintain a record database of issued media.
   e. The MVR technician shall coordinate with field supervisors to ensure that an adequate supply of recorded media is available.
   f. The MVR technician shall be responsible for the following:
      1. Long-term storage of media deemed to be of evidentiary value consistent with the department’s evidence storage protocols and retention schedule
      2. The cleansing (degaussing) and re-issuance of all other media deemed to be of no evidentiary value consistent with the department’s document retention requirements.

8. Media Duplication
   a. All recording media, recorded images and audio recordings are the property of this department. Dissemination outside of the agency is strictly prohibited without specific written authorization of the agency’s chief executive or his or her designee.
   b. To prevent damage to, or alteration of, the original recorded media, it shall not be copied, viewed or otherwise inserted into any device not approved by the departmental MVR technician or forensic media staff.
   c. When possible and practical, a copy of the original media shall be used for viewing by investigators, staff, training personnel, and the courts (unless otherwise directed by the courts) to preserve the original media in pristine condition.
   d. At the conclusion of the trial proceedings or as otherwise authorized by the prosecutor’s office for which the media was required, all copies shall be submitted to the MVR technician for further storage.

© Copyright 2005. Departments are encouraged to use this policy to establish one customized to their agency and jurisdiction. However, copyright is held by the International Association of Chiefs of Police, Alexandria, Virginia U.S.A. All rights reserved under both international and Pan-American copyright conventions. Further dissemination of this material is prohibited without prior written consent of the copyright holder.
This project was supported by Grant No. 2000-DD-VX-0020 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices and bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice or the International Association of Chiefs of Police.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this model policy incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no “model” policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities, among other factors.
Sample Press Release

This press release is included in the Technology Desk Reference (TDR) as an example for communicating with the media about a new technology project. As law enforcement executives tailor this press release to their specific agencies, it will need to be redrafted in the context of local collaborations, project status and timelines. Departments must ensure that all information in the press release is accurate.

This media contact may be the only opportunity that agencies have to introduce the public to a department’s technology efforts, and follow-up reports of malfunctioning technology may be difficult to manager. Thus, prior to releasing a statement to the media about a new technology deployment, it is essential that the in-car cameras technology be tested repeatedly for usability.

Every effort has been made by the IACP Research Center Directorate and the Technology Technical Assistance Program (TTAP) to ensure that this press release incorporates the general issues related to in-car cameras. However, law enforcement administrators should be cautious that no “sample” press release can meet the needs of any given law enforcement agency. Each agency must tailor its media relations to ensure compliance with all laws, regulations and agreements.

NEWS FOR IMMEDIATE RELEASE | January 1, 2010

Governor Doe announces $150,000 grant to install video cameras in Anytown Police Department squad cars; 30 additional squad cars will receive video cameras as a part of pilot program.

Anytown – At the House of Hope on Anytown’s Southside, Governor John H. Doe today announced a $150,000 grant that will help the Anytown Police Department (APD) expand a pilot program to install video cameras in police squad cars. The state grant, in addition to a matching $50,000 grant from the City of Anytown, will allow APD to purchase and install 30 video cameras in squad cars. The video cameras are an important step to help to strengthen public safety and promote accountability and trust between law enforcement and the community it serves.
“Putting video cameras inside police cars protects drivers stopped by the police and it protects police officers. It’s good public policy and I’m glad we were able to help the City of Anytown do it,” said Governor Doe.

A 2004 study by the International Association of Chiefs of Police (IACP) looked at the impact of police in-car camera systems on state police and highway agencies. The study reported an increase in officer safety, a reduction in the number of citizen complaints lodged against officers, officers conducting themselves more professionally, and an increase in the number of convictions and guilty pleas prior to going to trial.

“The in-car camera technology not only protects citizens and police officers, but it serves as a reliable tool to gather evidence for investigative purposes,” said Anytown Police Superintendent Paul Smith. “It’s a common sense measure that police officers nationwide are embracing, and the Anytown Police Department will continue to seek state and federal funding to expand the Program,” he added.

Having video cameras installed in squad cars during a traffic stop will not only make it easier to obtain accurate information as well as make it more safe for the law enforcement officer but also the cameras may be a powerful tool in helping to eliminate racial disparities by providing a record of all patrol activity and traffic stops.

With the use of in-car video cameras, officer indiscretions can immediately be verified or discredited. This capability allows agencies to quickly rebut false claims against officers or swiftly take sanctions against officers who step out of line. The IACP has found that the use of video cameras has the affect of increasing the public’s understanding and trust of law enforcement by allowing private citizens to imagine they are riding along with the police.

“Having video cameras in Anytown police cars is the right thing to do and the responsible thing to do to help protect both drivers and police officers during traffic stops. This grant is an important step toward one day putting cameras in all of Anytown Police Department’s cars,” said Senator Banker. Through various grants and DUI funds, the SP has 1293 cameras in their law enforcement vehicles. Up to 1999, 119 cameras were donated to SP from various organizations and foundations, such as MADD and the Meadows Foundation. PD’s pilot program is an important first step to help them transition to an entire fleet equipped with video cameras.

The State Department of Justice charged with administering grants and conducting audits of the state’s criminal history records will be the source of funding for the grant, which is derived from federal monies.

A press release courtesy of the IACP Technology Technical Assistance Program—October 2006
Legal Issues

Source: *Forensic Video Analysis and the Law* by Jonathan W. Hak

During the research stage that led to the IACP’s 2004 report on *The Impact of Video Evidence on Modern Policing*, it was noted that the majority of agencies and departments were not treating captured video as evidence. Chain of custody issues abounded, VHS tapes (pre-digital) were not secured, and retention periods were inconsistent with state law parameters regarding civil litigation. As we move into the “digital world” it is absolutely essential that law enforcement optimizes the capabilities of in-car video technology, to include helping agencies with risk management. Agency or department heads should work closely with their local and state regulatory agencies to adopt sound management policies that conform to statute-of-limitations issues with regards to civil litigation. Retention policies should meet or exceed those thresholds to help indemnify the agency from adverse judgments.

As all of law enforcement moves to treat captured data as evidence, modern day technology is moving quickly to leverage the technology to meet those demands and assist in securely managing the potentially tremendous amounts of stored data for presentation in a court of law. Agencies and departments should use their greatest resources; experienced field officers, deputies, or troopers coupled with information technology (IT) specialists to develop the plan best suited to support their agency’s mission.

Advances in digital technology have led to the use of various scientific techniques in the analysis and presentation of video evidence to the courts. In some cases, this has allowed the courts to gain more valuable information from video evidence than would otherwise have been evident. In other cases, it makes the difference between admitting video evidence and excluding it.

It is important to understand the background of videotape evidence in our courts, how the law deals with the advent of new technology and how to effectively present such evidence in court. We will also examine the critical aspect of becoming qualified as an expert witness in court.

Lieutenant Jim Davis
Los Angeles County Sheriff’s Department—California
During a high profile murder trial, the prosecution's star witness takes the witness stand and is asked by the prosecutor “Can you identify the man you saw running from the 7-11 store?” The witness scans the courtroom, points at the defendant and says “That’s him right there.” From the jurors’ perspective, the witness must be correct—after all, he was there.

Eyewitness evidence, though often powerful, is plagued by the frailties that accompany honest but mistaken witnesses. There are countless cases where honest witnesses have erred in their evidence, sometimes by saying “that’s the man” only to be later proven wrong. Equally, there are many cases where witnesses cannot identify the perpetrator even though he is actually in the line-up or the prisoner’s dock. Stress, sensory impairment, time and circumstance impact upon a witness’ ability to accurately identify perpetrators of offences.

It is a fundamental tenet of our criminal justice system that we should prosecute criminal offences with vigor and ensure that only the guilty are convicted. Video evidence can be of significant value in identifying those who committed offences and those who did not. Video evidence is not subject to the same frailties that face humans. As noted by the Supreme Court of Canada in *R. v. Nikolovski*:

> The video camera on the other hand is never subject to stress. Through tumultuous events it continues to record accurately and dispassionately all that comes before it. Although silent, it remains a constant, unbiased witness with instant and total recall of all that it observed.

…So long as the videotape is of good quality and gives a clear picture of events and the perpetrator, it may provide the best evidence of the identity of the perpetrator. It is relevant and admissible evidence that can by itself be cogent and convincing evidence on the issue of identity. Indeed it may be the only evidence available.

For example, in the course of a robbery, every eyewitness may be killed yet the video camera will steadfastly continue to impassively record the robbery and the actions of the robbers.

Both the United States and Canada are common law jurisdictions. As such, we have much to learn from each country in our examination of forensic video analysis. We will examine relevant case law from both the United States and Canada in order to gain a proper grounding of the law. We will also review relevant provisions in the United States Federal Rules of Evidence and the Canada Evidence Act.

### I. Types of Videotape Evidence in Criminal Prosecutions

Video evidence, as used in the criminal justice system, falls into one of three categories:

a. **Illustrative Video**

   These are videos that show or illustrate certain things to the court that it would not otherwise be able to readily see. For example:
• Crime scene video
• Demonstrating that a weapon caused a certain injury where an in court demonstration is not practical
• Demonstrating that a firearm is capable of modification to fully automatic firing where firing the weapon in court is not an option
• Demonstrating the explosive force of a replication bomb

b. Staged Video
These are videos that record events that are about to occur for the record such as the interview of a suspect or witness.

c. Surveillance Video
Surveillance video is becoming pervasive in our society as a method of both preventing and detecting crime. It is estimated that in cities, we are captured on surveillance video many times per day. In downtown London, pedestrians are observed on surveillance video at all times.

2. Admissibility of Videotape Evidence
Videos are classified as a form of photographic evidence under Federal Rule of Evidence 1001 and parallel provisions in most states. In Canada, video evidence is classified as real evidence.

a. Theories of Admissibility
   i. Illustrative evidence theory ("pictoral communication")
      The traditional view of photographs and video evidence is that they have no independent significance as they merely illustrate facts testified to by a witness. This is referred to as the "graphic portrayal of real evidence". Under this theory, photographs or video evidence become admissible once a witness testifies that the photographs or video accurately depicts what was observed by the witness.

   ii. Silent Witness Theory
      Once the videotape has been authenticated, the tape speaks for itself. No witness needs to have viewed what the camera recorded. In R. v. Taylor, the Court admitted videotape evidence without eyewitness verification, stating:

      At issue is whether these tapes are capable of being real and demonstrative evidence to prove the scenes they depict as distinct from evidence that merely illustrates the testimony of a sworn witness…If the tape is relevant, material, and reliable it has actual probative value.

      The evidence is admissible upon proving the reliability of the process that produced the video.

b. Relevance
Admissibility is contingent, in part, upon the court being satisfied as to the relevance of the video evidence. There is no magic legal test for relevance. Relevance is determined on a case-by-case basis and depends on the issues raised in the prosecution in question.
The relevancy test applies to the video evidence as a whole. If irrelevant images appear on the video, which is typically the case in a surveillance context, that does not render the entire video recording inadmissible. It is the images of interest that must be relevant. The test for relevance is a practical one. If an eyewitness would be permitted to describe what is depicted on the video recording, then the relevancy requirement is met.\(^5\)

c. Authentication

In *State v. Molasky*,\(^6\) in admitting videotape evidence, the Court based its decision on the evidence of an expert who said that videotape “could not be undetectably altered by any known editing method”. While that may have been true in 1983, it is unlikely true today.

In order for the court to rule videotape evidence admissible and in order for the trier of fact to rely upon it, it must be established that the videotape evidence is reliable. This authentication requirement provides that the party tendering the videotape must establish that the video accurately depicts the scene and that it has not been altered or changed.\(^7\)

Authentication focuses on these elements:
- Location
- Date
- Time
- Alteration of the image in whole or in part

Proving the location of the captured images is generally not difficult. In the monitored surveillance context, this will require the operator of the camera or someone present during the recording process to verify the location shown. In the static surveillance context, such as a store or other commercial establishment, this would typically be done by someone familiar with the camera location and field of view, such as the store owner, employee or security officer. In the case of a bank, either a bank employee or a representative from the company who installed and services the surveillance equipment will suffice.\(^8\)

After proving location, the date and time of the images in question must be proven. Most surveillance cameras show the date and time and provided such information is accurate, this requirement will be easily met. Where the date and time shown are incorrect, such as failing to account for daylight savings time or failing to set the accurate time at all, the actual date and time must be proven. My practice is to call the person who is responsible for ensuring that the date and time code is correct, if there is such a person. Where no such witness exists, the date and time can usually be proven by establishing the known time other events on the video occurred, such as the arrival of the police. The bottom line is that in order for the videotape evidence to be admissible, it must be shown that what is depicted is the event in question.
In *R. v. Leaney and Rawlinson*,9 Harradence, J., in dissent (though not on this point), noted the following regarding authentication:

The party seeking the admission of the video must prove that it is accurate and fair through the verification evidence of a witness or witnesses under oath. In most situations this will be easily done. An eyewitness can testify that the video accurately represents the event that took place. Where there is no such eyewitness, accuracy and fairness will need to be verified by more technical evidence. The United States Court of Appeals examined the possible components of such evidence in *United States v. Taylor*, 530 F.2d 639 (1976) (at pp. 641-2):

In the case before us it was, of course, impossible for any of the tellers to testify that the film accurately depicted the events as witnessed by them, since the camera was activated only after the bank personnel were locked in the vault. The only testimony offered as foundation for the introduction of the photographs was by government witnesses who were not present during the actual robbery. These witnesses, however, testified as to the manner in which the film was installed in the camera, how the camera was activated, the fact that the film was removed immediately after the robbery, the chain of its possession, and the fact that it was properly developed and contact prints made from it. Under the circumstances of this case, we find that such testimony furnished sufficient authentication for the admission of the contact prints into evidence. Admission of this type of photographic evidence is a matter largely within the discretion of the court, *Moore v. Louisville & Nashville R.R. Co.*, 223 F.2d 214, 216 (5th Cir. 1955), and it is clear that the district court did not abuse its discretion here.

These are the kinds of matters the trial judge may wish to consider in determining the accuracy and fairness of a video tape sought to be admitted into evidence where no eyewitness verification is possible.

For analog videotape, authentication can usually be accomplished by proving chain of custody of the original videotape. The same approach is required for digital video evidence, though some argue that chain of custody is not enough.

As Erik Berg noted:10

Until a digital image is either printed or displayed on a computer screen, it has no visual form. It is completely dependent upon a host computer for its existence as a visual record. The potential for alteration or corruption of a digital image is much greater than one might think. Electrical power surges can scramble the binary bits that define the image. Hardware failure can destroy the very media upon which the image is recorded. Computer viruses can seek out and destroy the image. Anyone with access to the computer can be a very serious threat to digital images and, thus, to authentication at trial. One or two errant commands can be enough to destroy precious image data.
Controlling access to the computer is, therefore, important. So too, is tracking and preserving the images. The original image should be preserved intact. Any “enhancement” applied to an image must take place on a copy of the original. If the original image is enhanced, there will be no way to reproduce the results. The original image serves the function of control, much the same as any control used in scientific analysis. Without effective controls, any conclusions drawn from the evidence will be suspect.

Digital video is simply binary data recorded on tape or other media. As such, it is inherently susceptible to accidental or malicious tampering. That fact, coupled with the widespread availability of low cost digital video editing hardware and software, leaves digital evidence vulnerable to suppression on the grounds that it could have been modified.\(^1\)

Technical experts have been trying to create a method whereby image alteration can be detected and conversely shown not to have occurred. One method has been the use of watermarking which modifies the digital video content by superimposition of the watermark. A number of papers have shown that this is not a foolproof method of image authentication.\(^2\)

Another method that is being studied is a method whereby digital signatures are generated in an authentication system and stored on a media separate from the digital video evidence that theoretically would provide a means of proving digital video authenticity and simultaneously preserving the digital video in an unaltered state.\(^3\) The need for such authentication is predicated on the argument that something untoward may have occurred to the evidence between the time of collection and the time of presentation in court. For a digital signature system to be most effective, the signatures would need to be created in real time as the digital video is recorded.

Another method involves the use of encryption to scramble the image information making it impossible to view the image without the encryption key. This might prevent image tampering but the encryption process itself alters the original image. In order to view the encrypted image, it must be reconstructed. Once encrypted, the original image is not retained. This alone poses authentication problems.\(^4\)

There is another method of establishing the authentication of analog and digital video evidence—the integrity and reputation of the expert. This more basic method may not always carry the day, hence the desire to prove authentication objectively. Indeed, where the credibility of the authentication witnesses is suspect, such a finding will impact upon an missibility ruling.\(^5\)

**Original v. Copy**

In the analog video world, the determination of what is an original and what is a copy is straightforward. The original videotape can be readily seen and identified as such. In the
digital world, given the ethereal nature of digital images, the determination of what is an original is defined more by law than science. Some jurisdictions have commented on the difference (or lack thereof) between originals and copies of digital media. There are a number of legislative provisions that deal, directly or indirectly, with authentication related issues.

United States
Federal Rule of Evidence 1001(2) states that the original of a writing, recording or photograph is required to prove the content of the writing, recording or photograph. FRE 1002 defines “photograph” as including still photographs, x-ray films, videotapes and motion pictures.

FRE 1001(3) provides in part that:
If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is a ‘original’.

Thus, in respect of digital images, there is no single original as defined in the Federal Rules of Evidence. Provided the “original” data is shown by the computer, it does not matter whether the computer showing the data is the computer that originally captured the images.

A “duplicate” is defined in FRE 1001(4) as being:
A “duplicate” is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements or miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.

According to FRE 1003:
A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

To a large extent, this is simply an application of the best evidence rule. This is more fully reflected in Rule 1004 which provides as follows:

Rule 1004. Admissibility of Other Evidence of Contents
The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if:

1. Originals Lost or Destroyed—All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or
2. Original Not Obtainable—No original can be obtained by any available judicial process or procedure; or
3. Original in Possession of Opponent—At a time when an original was under the
control of the party against whom offered, that party was put on notice, by the pleadings or otherwise, that the contents would be subject of proof at the hearing, and that party does not produce the original at the hearing; or

4. **Collateral Matters**—The writing, recording, or photograph is not closely related to a controlling issue.

**Canada**

In Canada, there is no legislation that specifically deals with the issue of originals v. copies.

**United Kingdom**

The House of Lords Select Committee on Science and Technology Report (Fifth Report) preferred the following definition in relation to digital images—the original is the data first recorded in memory. Therefore, any image created from this data is a copy. Using this definition, digital recording technology is unable to produce an original that can be produced in evidence. All that is available for use as evidence is a copy of the first recording. The weight of this evidence will be dependent, amongst other things, on proper authentication.

**Authentication Legislation**

**United States**

The Federal Rules of Evidence do not specifically address the authenticity of digital video evidence yet the rules do offer some guidance in this regard. The relevant provisions are as follows:

**Rule 901. Requirement of Authentication or Identification**

**(a) General provision**

The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

**(b) Illustrations**

By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:

- **Testimony of witness with knowledge**—Testimony that a matter is what it is claimed to be
- **Comparison by trier or expert witness**—Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated
- **Distinctive characteristics and the like**—Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances
- **Process or system**—Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result
Canada
The Canadian Parliament has been progressive in dealing with the issue of authentication of electronic evidence. The Canada Evidence Act was amended in 2000 to deal with the reality of “electronic documents.” The amendments provide as follows:

31.1 Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.

31.2 (1) The best evidence rule in respect of an electronic document is satisfied
(a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or
(b) if an evidentiary presumption established under section 31.4 applies.

(2) Despite subsection (1), in the absence of evidence to the contrary, an electronic document in the form of a printout satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout.

31.3 For the purposes of subsection 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven:
* by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;
* if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or if it is established that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it.

31.4 The Governor in Council may make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures, including regulations respecting:
(a) the association of secure electronic signatures with persons; and
(b) the integrity of information contained in electronic documents signed with secure electronic signatures.

31.5 For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.
31.7 Sections 31.1 to 31.4 do not affect any rule of law relating to the admissibility of evidence, except the rules relating to authentication and best evidence.

31.8 The definitions in this section apply in sections 31.1 to 31.6.

1. “computer system” means a device that, or a group of interconnected or related devices one or more of which:
   (a) contains computer programs or other data; and
   (b) pursuant to computer programs, performs logic and control, and may perform any other function.

2. “data” means representations of information or of concepts, in any form “electronic document” means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.

3. “electronic documents system” includes a computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic documents.

4. “secure electronic signature” means a secure electronic signature as defined in subsection 31(1) of the Personal Information Protection and Electronic Documents Act.

By virtue of the definition of “electronic document” and “data,” these amendments apply to video images that are recorded or stored on any medium in or by a computer or other similar device. Practically, this would include the following:

- Images recorded by a digital CCTV system
- Images recorded by a digital video camera
- Digital video that is downloaded onto a computer system
- Analog video that has been digitized for use in court

These amendments do not change what the common law already required. Section 31.7 makes it clear that these amendments do not affect any existing rule of law relating to the admissibility of evidence. Rather, they accentuate the present rules relating to authentication and best evidence.

It remains the obligation of the party introducing an “electronic document” to authenticate the images contained within that document. Translated, digital images must be proven to be authentic, accurate representations of what was originally recorded. Parliament has specifically required under s. 31.2(1)(a) that the best evidence rule in respect of “electronic documents” requires proof of the integrity of the “electronic documents system” that recorded or stored the “electronic document.” Thus, in the context of forensic video analysis, the competency of the analyst is not the only issue. The competency and integrity of the computer system used by the analyst is also at issue. Section 31.3(a) requires evidence that proves proper operation of the computer system in question.
These provisions do not mandate the use of “secure electronic signatures” as part of an authentication scheme. Section 31.4 allows the Governor in Council to make regulations establishing evidentiary presumptions in respect of such an authentication scheme. Such regulations, entitled the Secure Electronic Signature Regulations were enacted on February 1, 2005. Section 2 of the Regulations provides that in order to constitute a “secure electronic signature” such a signature must be a digital signature that results from the completion of a series of listed consecutive operations. These operations include the following:

1. The application of a hash function to the data to generate a message digest
2. The application of a private key to encrypt the message digest
3. The encrypted message digest must be incorporated in, attached to, or associated with the electronic document
4. The electronic document and encrypted message digest must be transmitted with a digital signature certificate or a means of access to the certificate
5. After receipt of the electronic document, the encrypted message digest and the digital signature certificate or the means of access to the certificate, the public key contained in the digital signature certificate must be applied to decrypt the encrypted message digest
6. A hash function must then be applied to the data contained in the electronic document to generate a new message digest
7. There must be verification that the original message digest is identical to the decrypted message digest
8. The digital signature certificate must be verified as valid

Section 3 specifies what is required to validate a digital signature certificate.

The only relevant reported decision thus far regarding the amendments to the Canada Evidence Act is R. v. Morgan. This case dealt with fishing licenses that existed in a computer database.

In discussing these amendments, Flynn, J. said:

These sections must work in conjunction with either some common law general rule of admissibility of documents or some other statutory provision. These sections themselves do not authorize the admissibility of the documentary evidence it describes. Rather, what the sections do is to clothe electronically stored and produced documents with the status of “best evidence” provided they meet certain criteria for their admissibility. For example, the documents in this case must first be proven to be business documents or official or public documents which are admissible of themselves as documentary evidence and as exceptions to the hearsay rule. If they are admissible under these other criteria, then Sections 31.1 and 31.2 operate to make them the best evidence available for that purpose. [21] Enacted in the year 2000, the general purpose of section 31.1 and Section 31.2 as gleaned from the statutory provisions themselves is to allow the
use of computerized information as either business, public documents or other types of documents provided the reliability of such documents can be established. It is a legislative attempt to grapple with the realities of modern business practice.

These comments reflect the likely intention of Parliament in enacting these provisions, namely the use of business documents that exist on computer databases, networks and hard drives. However, the broad definitions of “electronic document” and “data” clearly envelop digital images as well, whether so intended or not.

This does not change the way digital images should be approached. If anything, it simply formalizes what the common law and proper practice already requires. Integrity and reliability remain the watchwords.

d) Editing

One of the concerns with video evidence (both analog and digital) is that the images have been edited in such a way as to present a false picture of what really happened. This is different from concerns of authentication. Editing in this context applies to both video and audio editing.

Editing a video recording will not necessarily render the video evidence inadmissible. The person tendering the video evidence, whether the forensic video analyst or another witness, must thoroughly explain any editing in such a fashion as to instill confidence in the evidence led in court.

Editing is quite legitimate. For example, if the original surveillance video records seven images and the robbery in question lasted three minutes, editing out the balance of the images is appropriate because they are irrelevant. A forensic video analyst must be careful to ensure that there is nothing else relevant on the tape such as an earlier or later appearance by the suspect (or victim as the case may be).

In general, editing goes to weight, not admissibility.\(^\text{21}\) However, edited video will likely be included where the editing causes a disruption in the chronology or continuity of the event, or otherwise causes confusion. Inadmissibility on this basis results from the fact that the tendered images do not accurately establish and depict the events in question.\(^\text{22}\) Further, where the probative value of the remaining images is outweighed by the prejudicial effect, the evidence can be excluded. More on this latter test will be discussed later in this paper.

The use of time-lapse surveillance video and multiplex cameras, though they involve forced editing by the cameras, is permissible provided the time-lapse operation or multiplex function is adequately explained to the court.

e) Accuracy of the Images

Accuracy of the images, while related to authentication, is a separate issue. The accuracy of the images portrayed on the video can affect both admissibility and weight. The overriding test to
be applied is that the video evidence must be a consistent, true reflection of reality.

The primary objects in the video as well as the secondary or surrounding elements must all be accurately shown. Distortion of material elements of the video may affect the admissibility of the evidence. Distortion of non-material elements will likely only affect the weight of the evidence.

A forensic video analyst must ensure that the proper aspect ratio is used so as to ensure that accurately proportioned images are shown.

Digital video surveillance equipment is being marketed as the solution to almost any commercial (and private) surveillance security concern. On its face, there is an attraction to a digital video security system. No videotapes to handle or store. Many hours of surveillance can be recorded and erased. Some systems are quite inexpensive. One of the concerns that affect the admissibility of images from these systems is compression. If the images are compressed so as to produce artifacts or otherwise create inaccurate images, then the images are not accurate and counsel will likely face a significant hurdle in having such images ruled admissible.

f) Chain of Custody
A forensic video analyst must have confidence that the chain of custody of the video evidence is intact. This is not just a concern for the prosecutor. The analyst should be satisfied that he/she is working on the original evidence and that the integrity of that evidence is intact. It follows that the forensic video analyst must also account for the chain of custody of the video evidence while in his/her possession.

Standard Operating Procedures (SOPs) should adequately address these issues.

g) Probative Value v. Prejudicial Effect
A final, overriding consideration for the admissibility of any evidence is whether the probative value of the evidence outweighs the prejudicial effect. The “prejudice” referred to in the term “prejudicial effect” does not refer to the increased likelihood of conviction. Rather, it refers to evidence which operates unfairly against the accused - evidence that may be used improperly by the trier of fact.

In the context of video evidence, if as a result of editing, the videotape is found to operate unfairly to the accused, it may be ruled inadmissible on the basis that the probative value of the evidence is outweighed by its prejudicial effect. For example, in Toronto (City) v. Debono,22 the court refused to admit television news video that had been edited for television purposes because the edited version was inflammatory and unfair.

This is a common law principle. This principle is codified in Federal Rule of Evidence 403, which provides:
Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.

In Ballou v. Henri Studios, the Court stated:

[U]nfair prejudice as used in Rule 403 is not to be equated with testimony simply adverse to the opposing party. Virtually all evidence is prejudicial or it isn't material. Unfair prejudice within the context of Rule 403 means an undue tendency to suggest a decision on an improper basis, commonly, though not necessarily, an emotional one.

Forensic video analysis itself is unlikely to violate this principle but it is an important principle to keep in mind.

Adapted Forensic Video Analysis and the Law, by from Jonathan W. Hak. The entire document can be found in the Appendices of this Desk Reference.

Endnotes
1 Jonathan W. Hak is a Crown Prosecutor by Alberta Justice in Calgary. He primarily prosecutes major crimes and specializes in forensic video analysis. He is also an instructor in Forensic Video Analysis and the Law for LEVA and has instructed in this field at the FBI Academy in Quantico, Virginia, the Los Angeles Sheriffs Academy in California, the University of Indianapolis, the United Kingdom, and other locations. He received his legal education in the United States, Canada and England. He may be contacted at jonathan.hak@gov.ab.ca and (403) 297-2344.
4 Hannewacker v. City of Jacksonville Beach, 419 So. 2d 827 ( Fla. 1st DCA), review denied, 717 So. 2d 542 (1998, Florida).
5 Simpson Timber Co. (Sask.) Ltd. v. Bonville, [1986] 5 W.W.R. 180 (Saskatchewan Court of Queen's Bench).
12 See note 10.
13 See Authentication of Digital Video Evidence, note 11, for details.
14 See note 10.


17. Under s. 31(1) of the Personal Information Protection and Electronic Documents Acts, “secure electronic signature” means a signature that results from the application of a technology or process prescribed by regulations made under s. 481(1) of the Act.


23. Unreported, June 1, 1990, Ontario High Court of Justice.

Additional Resources

Technology today has become a critical component in every law enforcement agency’s arsenal against crime. It is imperative that all law enforcement agencies have at their disposal the latest technology to not only solve crime but also to be used as a force multiplier in an era of shrinking personnel resources. It is important for every law enforcement executive to maximize both their awareness of technology and know where to find technology resources. As we all know, technology is expensive and it is often time-consuming to ascertain which is the best technology for a specific application within a law enforcement agency. To make this task easier, the following approaches are suggested:

• The chief law enforcement executive should be committed to staying current on technology issues
• Develop and maintain a working partnership with the International Association of Chiefs of Police, a leader in developing and implementing technology
• Maintain an awareness of the role of the federal government with law enforcement technology, especially the National Law Enforcement and Corrections Technology Centers, and use them as a research and development program
• Refine the ability to learn from other’s successes as well as failures

Technology today is often the difference between solving a current or cold criminal case, saving a life and protecting our officers from harm. An agency executive who fails to bring modern technology into their law enforcement agency is truly doing a disservice to the agency, the officers, and the community. It is the intention of this publication to assist the law enforcement executive with this exact task, to utilize technology to make our communities safer, our officers safer, prevent and solve crime.

Chief Paul Schultz
Lafayette Police Department—Colorado
Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993)—place appropriate limits on the admissibility of purportedly scientific evidence
http://www.daubertontheweb.com

FBI Forensic Laboratory—As one of the largest and most comprehensive forensic laboratories in the world, the FBI Laboratory provides forensic and technical services to federal, state, and local law enforcement agencies at no expense to these agencies.
http://www.fbi.gov

Frye v. United States, 293 F. 1013 (D.C. Cir. 1923)—“Frye” refers to a United States Federal Court opinion dealing with the admissibility of scientific evidence. The court established that new or novel scientific evidence, or the novel application of scientific principles, must be shown to have met with general acceptance in the relevant scientific community before it can be admitted.
http://www.daubertontheweb.com

“To summarize: ‘general acceptance’ is not a necessary precondition to the admissibility of scientific evidence under the Federal Rules of Evidence, but the Rules of Evidence — especially Rule 702—do assign to the trial judge the task of ensuring that an expert’s testimony both rests on a reliable foundation and is relevant to the task at hand.” — Justice Blackmun

International Association Chiefs of Police—The International Association of Chiefs of Police has completed their comprehensive evaluation on the Impact of Video Evidence of Modern Policing. This 18-month study examined the installation, use and impact of police in-car cameras in 47 state police and highway patrol agencies.
http://www.iacp.org/research/RCDTechPoliceInCar.html

The Law Enforcement and Emergency Services Video Association—A non-profit organization committed to improving the quality of video training and promoting the use of state-of-the-art, effective equipment in the law enforcement and emergency services community. View the Best Practices Guide for Forensic Video Analysis on the LEVA website.
http://www.leva.org

National Institute of Justice Forensic Sciences—NIJ is the national focal point for research and development of new technology to support the criminal justice system. NIJ funds development of technologies to improve the safety and effectiveness of law enforcement and corrections professionals. NIJ develops new forensic science technologies and assists crime laboratories enhance their capacity to access and use new technology. NIJ also develops standards and best practices to guide the work of criminal justice professionals in the use of technology.
http://www.ojp.usdoj.gov/nij/topics/forensics/welcome.html
Glossary

A

Absolute Time Code (ATC)—is generally recorded in the subcode or control track region of any digital tape. This is the code that digital tape machines use to locate specific points on a tape for autolocation or other functions.

Active Storage—A storage location or device (i.e. Server), which videos are transferred from the in-vehicle recorder using any method. Active Storage shall provide ready access to recently recorded videos, which have not been moved to Archival Storage due to elapsed time from original recording creation date. Access to videos in Active Storage may or may not require Administrator interaction based on departmental policy.

Audio Interchange File Format (AIFF)—Format for both compressed and uncompressed audio data.

Algorithm—a) A set of rules or processes for solving a problem in a finite number of steps. In audio, video and data coding, the step-by-step procedure (often including repetition) which provides suitable compression and/or encryption for the specific application. When used for compression, this mathematical process results in a significant reduction in the number of bits required for transmission and may be either lossless or lossy. b) Step-by-step procedure for the solution to a problem. First the problem is stated and then an algorithm is devised for its solution.

Alphanumeric—Set of all alphabetic and numeric characters.

Ambient Lighting—Light that emanates from no one particular source, coming from all directions with equal intensity.

Amplitude—a) The height of a waveform above or below the zero line. The maximum value of a varying waveform. b) The maximum distance an oscillating body (e.g., a pendulum) or wave travels from a mean point.

Amplitude Modulation (AM)—a) The process used for some radio (AM broadcast, in North American audio service broadcast over 535 kHz-1705 kHz) and television video transmission. A low frequency (program) signal modulates (changes) the amplitude of a high frequency RF carrier signal (causing it to deviate from its nominal base amplitude). The original program signal is recovered (demodulated) at the receiver. This system is
extensively used in broadcast radio transmission because it is less prone to signal interference and retains most of the original signal quality. In video, FM is used in order to record high quality signals on videotape. b) The process by which the amplitude of a high-frequency carrier is varied in proportion to the signal of interest. In the PAL television system, AM is used to encode the color information and to transmit the picture. Several different forms of AM are differentiated by various methods of sideband filtering and carrier suppression. Double sideband suppressed carrier is used to encode the PAL color information, while the signal is transmitted with a large-carrier vestigial sideband scheme.

**Analog**—a) A continuous electrical signal that carries information in the form of variable physical values, such as amplitude or frequency modulation. b) A signal which moves through a continuous range of settings or levels. c) An adjective describing any signal that varies continuously as opposed to a digital signal that contains discrete levels representing the binary digits 0 and 1. d) A signal that is an analogy of a physical process and is continuously variable, rather than discrete. See also Digitization.

**Analog Video**—a) A video signal represented by a smooth and infinite number of video levels. b) A video signal made of a continuous electrical signal. A television and VCR can be analog video devices. To be stored and manipulated on a computer, analog video must be converted to digital video.

**Aperture**—An adjustable opening in a lens which, like the iris in the human eye, controls the amount of light entering a camera. The size of the aperture is controlled by the iris adjustment and is measured in F-stops. A smaller F-stop number corresponds to a larger opening that passes more light.

**Archive**—a) Off-line storage of video/audio onto backup tapes, floppy disks, optical disks, etc. b) A collection of several files bundled into one file by a program (such as ar, tar, bar, or cpio) for shipment or archiving. This method is very reliable and can contain large amounts of data. c) Long-term off-line storage. In digital systems, pictures are generally archived onto some form of hard disk, magnetic tape, floppy disk or DAT cartridge.

**Archival Storage**—A storage location or device which video are moved to after a designated amount of time. Access to videos contained within the Archival Storage may be limited and require Administrator authorization to review or move back to Active Storage. Media for Archival Storage may include: tapes, spinning optical media (CD, DVD, Blue-Ray, HD-DVD, etc.), hard drives, etc.

**American Standard Code for Information Interchange (ASCII)**—a) Character code used for representing information as binary data in most computer systems. b) A standard code for transmitting data, consisting of 128 letters, numerals, symbols and special codes each of which is represented by a unique binary number.
Asynchronous Transfer Mode (ATM)—a) A digital transmission system using packets of 53 bytes for transmission. ATM may be used for LANs and WANs. ATM is a switching/transmission technique where data is transmitted in small, 53 byte fixed sized cells (5 byte header, 48 byte payload). The cells lend themselves both to the time-division-multiplexing characteristics of the transmission media, and the packet switching characteristics desired of data networks. At each switching node, the ATM header identifies a virtual path or virtual circuit that the cell contains data for, enabling the switch to forward the cell to the correct next-hop trunk. The virtual path is set up through the involved switches when two endpoints wish to communicate. This type of switching can be implemented in hardware, almost essential when trunk speed range from 45 Mbps to 1 Gbps. The ATM Forum, a worldwide organization, aimed at promoting ATM within the industry and the end user community was formed in October 1991 and currently includes more than 500 companies representing all sectors of the communications and computer industries, as well as a number of government agencies, research organizations and users. b) A digital signal protocol for efficient transport of both constant-rate and burst information in broadband digital networks.

Audiotape Recorder (ATR)—A device for recording and reproducing sound on magnetic recording tape.

Audio—a) Signals consisting of frequencies corresponding to a normally audible sound wave ranging between the frequencies of 20 Hz to 20,000 Hz. b) A DC signal with varying amounts of ripple. It is sometimes possible to see the ripple on the DC signal to convey information of widely variable degrees of usefulness.

Authentication—a) A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator. b) A means of identifying individuals and verifying their eligibility to receive specific categories of information. c) Evidence by proper signature or seal that a document is genuine and official. d) In evasion and recovery operations, the process whereby the identity of an evader is confirmed. e) A means of proving the origin of the evidence and that it has not subsequently been altered (or, where alteration has occurred, that such alterations are properly identified). f) The process of determining whether a recording or image is original, continuous, and free from unexplained alterations (e.g., additions, deletions, edits, or artifacts) and is consistent with the stated operation of the recording device used to make it.

Authenticity—The quality or condition of being authentic, trustworthy, or genuine.

AutoSave—A feature that saves your work at intervals you specify. Backups are placed in the attic folder.
B

**Back Up**—To copy a certain set of files and directories from your hard disk to a tape or other non-volatile storage media.

**Backup**—A duplicate copy of a file or disk in another location if the original file or disk becomes corrupted. See also Attic Folder.

**Backup Tape**—A tape that contains a copy of a set of files and directories that are on your hard disk. A full backup tape contains a copy of all files and directories, including IRIX, which are on your hard disk.

**Backward Compatibility**—A new coding standard that is backward compatible with an existing coding standard if existing decoders (designed to operate with the existing coding standard) are able to continue to operate by decoding all or part of a bit stream produced according to the new coding standard.

**Bandwidth**—The range of frequencies over which signal amplitude remains constant (within some limits) as it is passed through a system. More specific definitions include: a) The difference between the upper and lower limits of a frequency, often measured in megahertz (MHz). b) The complete range of frequencies over which a circuit or electronic system can function with less than a 3 dB signal loss. c) The information carrying capability of a particular television channel. d) A measure of information capacity in the frequency domain. The greater the bandwidth of a transmission channel, the more information it can carry.

**Bar Code**—A pattern of vertical stripes of varying width and spacing that encodes information. Bar codes can be used to encode time code on film.

**Binary**—A base-2 numbering system using the digits 0 and 1 (as opposed to digits, 0-9) in the decimal system. In computer systems, the binary digits are represented by two different voltages or currents, on corresponding to 0 and the other corresponding to 1.

C

**Computer Aided Design (CAD)**—This usually refers to a design of system that uses computer specialized software.

**CB**—Scaled version of the B-Y signal.

**Closed Circuit (CC)**—The method of transmission of programs or other material that limits its target audience to a specific group rather than the general public.
Closed Circuit TV (CCTV)—a) A video system used in many commercial installations for specific purposes such as security, medical and educational. b) A television system intended for only a limited number of viewers, as opposed to broadcast TV.

Compact Disc (CD)—a) A 4.75” disc used to store optical, machine-readable, digital data that can be accessed with a laser-based reader such as a CD player. b) A standard medium for storing digital data in machine-readable form, accessible with a laser-based reader. Readers are typically referred to as CD-ROM drives.

Compact Disc Read Only Memory (CD-ROM)—a) CD-ROM means “Compact Disc Read Only Memory”. A CD-ROM is physically identical to a Digital Audio Compact Disc used in a CD player, but the bits recorded on it are interpreted as computer data instead of music. A CD-ROM can hold about 650 megabytes of data, the equivalent of thousands of floppy disks. The data on a CD-ROM can be accessed much faster than a tape, but CD-ROMs are 10 to 20 times slower than hard disks. b) A flat metallic disk that contains information that you can view and copy onto your own hard disk; you cannot change or add to its information.

Chain of Custody—The chronological documentation of the movement, location and possession of evidence.

Clip—A video file.

CMYK—Refers to the colors that make up the subtractive color system used in pigment printers: cyan, magenta, yellow and black. In the CMYK subtractive color system these pigments or inks are applied to a white surface to filter that color light information from the white surface to create the final color. Black is used because cyan, magenta and yellow cannot be combined to create a true black.

Coaxial Cable—a) A transmission line with a concentric pair of signal carrying conductors. There is an inner conductor and an outer conductor metallic sheath. The sheath aids in preventing external radiation from affecting the signal on the inner conductor and minimizes signal radiation from the transmission line. b) A large cable composed of fine foil wires that is used to carry high bandwidth signals such as cable TV or cable modem data streams. c) The most common type of cable used for copper transmission of video signals. It has a coaxial cross-section, where the center core is the signal conductor, while the outer shield protects it from external electromagnetic interference.

Coding/Decoding (CODEC)—a) The algorithm used to capture analog video or audio onto your hard drive. b) Used to implement the physical combination of the coding and decoding circuits. c) A device for converting signals from analog to coded digital and then back again for use in digital transmission schemes. Most codecs employ proprietary coding algorithms for data compression.
Compact Disc (CD)—A compact disc is a 12cm optical disc that stores encoded digital information (typically audio) in the constant linear velocity (CLV) format. For high-fidelity audio/music, it provides 74 minutes of digital sound, 90 dB signal-to-noise ratio and no degradation from playback.

Central Processing Unit (CPU)—Computer module in charge of fetching, decoding, and executing instructions. It incorporates a control unit, an ALU, and related facilities (registers, clocks, drivers).

CRT Terminal—Computer terminal using a CRT display and a keyboard, usually connected to the computer by a serial link.

Cue— a) An editing term meaning to bring all source and record VTRs to the predetermined edit point plus pre-roll time. b) An audio mixer function that allows the user to hear an audio source (usually through headphones) without selecting that source for broadcast/recording; the audio counterpart of a preview monitor. c) The act of rewinding and/or fast-forwarding a video or audiocassette so that the desired section is ready for play.

Cue Channel—A dedicated track for sync pulses or time code.

D

D1—A non-compressed component digital video recording format that uses data conforming to the ITU-R BT.601-2 standard. Records on high-end 19 mm (3/4") magnetic tape recorders. Systems manufactured by Sony and BTS. Most models can record 525, 625, ITU-R BT.601-2 and SMPTE 125M. The D1 designation is often used incorrectly to indicate component digital video.

D16—A format to store film resolution images on D1 format tape recorders. Records one film frame in the space normally used for 16 video frames.

D2—A non-compressed composite digital video recording format originally developed by Ampex that uses data conforming to SMPTE 244M and four 20 bit audio channels. Records on high-end 19 mm (3/4") magnetic tape recorders. It uses the same tape cassette cartridge but the tape itself is metal particle tape like Beta SP and MII. The D2 designation is often used incorrectly to indicate composite digital video.

D3—A non-compressed composite digital video recording format that uses data conforming to SMPTE 244M and four 20 bit audio channels. Records on high end 1/2" magnetic tape similar to M-II. The format was developed by Matsushita and Panasonic.
D4—A format designation never utilized due to the fact that the number four is considered unlucky (being synonymous with death in some Asian languages).

D5—A non-compressed, 10 bit 270 Mbit/second, component or composite digital video recording format developed by Matsushita and Panasonic. It is compatible with 360 Mbit/second systems. It records on high end 1/2” magnetic tape recorders.

D6—A digital tape format which uses a 19 mm helical-scan cassette tape to record uncompressed high definition television material at 1.88 Gbps (1.2 Gbps).

D7—DVCPRO. Panasonic’s development of native DV component format.

D9—Digital-S. A 1/2-inch digital tape format developed by JVC which uses a high-density metal particle tape running at 57.8 mm/s to record a video data rate of 50 Mbps.

DAT (Digital Audio Tape)—a) A consumer digital audio recording and playback system developed by Sony, with a signal quality capability surpassing that of the CD. b) A magnetic tape from which you can read and to which you can copy audio and digital information.

Data—General term denoting any or all facts, numbers, letters, and symbols or facts that refer to or describe an object, idea, condition, situation or other factors. Connotes basic elements of information that can be processed or produced by a computer. Sometimes data is considered to be expressible only in numerical form, but information is not so limited.

Data Base—Systematic organization of data files for easy access, retrieval, and updating.

Data Compression—Application of an algorithm to reduce the bit rate of a digital signal, or the bandwidth of an analog signal while preserving as much as possible of the information usually with the objective of meeting the constraints in subsequent portions of the system.

Data integrity—The accuracy of data and its conformity to its expected value, especially after being transmitted or processed.

Data Set—A group of two or more data essence or metadata elements that are pre-defined in the relevant data essence standard or Dynamic Metadata Dictionary and are grouped together under one UL Data Key. Set members are not guaranteed to exist or be in any order.

Decibel (dB)—a) dB is a standard unit for expressing changes in relative power. Variations of this formula describe power changes in terms of voltage or current. dB = 10log10 (P1/P2). b) A logarithmic ratio of two signals or values, usually refers to power, but also voltage and current. When power is calculated the logarithm is multiplied by 10, while for current and voltage by 20.
**Decode**—a) To separate a composite video signal into its component parts. b) To reconstruct information (data) by performing the inverse (reverse) functions of the encode process.

**Decoder**—a) Device used to recover the component signals from a composite (encoded) source. Decoders are used in displays and in various processing hardware where components signals are required from a composite source such as composite chroma keying or color correction equipment. b) Device that changes NTSC signals into component signals; sometimes devices that change digital signals to analog (see DAC). All color TV sets must include an NTSC decoder. Because sets are so inexpensive, such decoders are often quite rudimentary. c) An embodiment of a decoding process.

**Decompress**—The process of converting video and audio data from its compact form back into its original form in order to play it. Compare Compress.

**Decryption**—The process of unscrambling signals for reception and playback by authorized parties. The reverse process of encryption.

**Defaults**—A set of behaviors specified on every system. You can later change these specifications which range from how your screen looks to what type of drive you want to use to install new software.

**Degauss**—To demagnetize (erase) all recorded material on a magnetic videotape, an audiotape or the screen of a color monitor.

**Delete**—Edit term to remove.

**Depth of Field**—a) The range of objects in front of a camera lens which are in focus. Smaller F-stops provide greater depth of field, i.e., more of the scene, near to far, will be in focus. b) The area in front of and behind the object in focus that appears sharp on the screen. The depth of field increases with the decrease of the focal length, i.e., the shorter the focal length the wider the depth of field. The depth of field is always wider behind the objects in focus.

**Digital**—a) Having discrete states. Most digital logic is binary, with two states (on or off). b) A discontinuous electrical signal that carries information in binary fashion. Data is represented by a specific sequence of off-on electrical pulses. A method of representing data using binary numbers. An analog signal is converted to digital by the use of an analog-to-digital (A/D) converter chip by taking samples of the signal at a fixed time interval (sampling frequency). Assigning a binary number to these samples, this digital stream is then recorded onto magnetic tape. Upon playback, a digital-to-analog (D/A) converter chip reads the binary data and reconstructs the original analog signal. This process virtually eliminates generation.
loss as every digital-to-digital copy is theoretically an exact duplicate of the original allowing multi-generational dubs to be made without degradation. In actuality of course, digital systems are not perfect and specialized hardware/software is used to correct all but the most severe data loss. Digital signals are virtually immune to noise, distortion, cross talk, and other quality problems. In addition, digitally based equipment often offers advantages in cost, features, performance and reliability when compared to analog equipment.

**Digital 8**—Digital 8 compresses video using standard DV compression, but records it in a manner that allows it to use standard Hi-8 tape. The result is a DV “box” that can also play standard Hi-8 and 8 mm tapes. On playback, analog tapes are converted to a 25 Mbps compressed signal available via the iLink digital output interface. Playback from analog tapes has limited video quality. New recordings are digital and identical in performance to DV; audio specs and other data also are the same.

**Digital Asset**—Recorded video, audio, and associated metadata.

**Digital Audio**—Audio that has been encoded in a digital form for processing, storage or transmission.

**Digital Compression**—A process that reduces storage space and/or transmission data rate necessary to store or transmit information that is represented in a digital format.

**Digital Evidence**—Information of probative value that is stored or transmitted in binary form.

**Digital Recording**—A method of recording in which the information (usually audio or video) is first coded in a digital form. Most commonly, a binary code is used and recoding takes place in terms of two discrete values of residual flux.

**Digital Storage Media (DSM)**—a) A means of storage (usually magnetic tape, disk or DVD) for audio, video or other information, that is in binary form. b) A digital storage or transmission device or system.

**Digital Storage Media, Command and Control (DSM-CC)**—DSM-CC is part 6 of ISO/IEC 12818 MPEG-2 standard. It specifies open interfaces and protocols for delivery of multimedia broadband services and is transport-layer independent.

**Digital Video Cassette (DVC)**—a) Tape width is 1/4”, metal particle formula. The source and reconstructed video sample rate is similar to that of CCIR-601, but with additional chrominance subsampling (4:1:1 in the case of 30 Hz and 4:2:0 in the case of 25 Hz mode). For 30 frames/sec, the active source rate is 720 pixels/lines x 480 lines/frame x 30 frames/sec x 1.5 samples/pixel average x 8 samples/pixel = ~124 Mbit/sec. A JPEG-like still image compression algorithm (with macroblock adaptive quantization) applied with a 5:1 reduction
ratio (target bit rate of 25 Mbit/sec) averaged over a period of roughly 100 microseconds (100 microseconds is pretty small compared to MPEG’s typical 1/4 second time average!) b) A digital tape recording format using approximately 5:1 compression to produce near-Betacam quality on a very small cassette. Originated as a consumer product, but being used professionally as exemplified by Panasonic’s variation, DVC-Pro.

**Digital Video Cassette Recorder (Digital VCR)**—Digital VCRs are similar to analog VCRs in that tape is still used for storage. Instead of recording an analog audio/video signal, digital VCRs record digital signals, usually using compressed audio/video.

**Digitize**—a) The process of turning an analog signal into digital data. b) To convert an image from hard copy (a photo) into digital data for display on a computer. c) To convert an analog signal into digital form for storage on disk arrays and processing.

**Drop Frame Time Code**—a) SMPTE time code format that skips (drops) two frames per minute except on the tenth minute, so that the time code stays coincident with real time. b) The television broadcast standard for time code. c) The NTSC color coding system uses a 525/60 line/field format, it actually runs at 59.94 fields per second, or 29.97 frames per second (a difference of 1:1000). Time code identifies 30 frames per second, whereas drop frame time code compensates by dropping two frames in every minute except the tenth. Note that the 625/50 PAL system is exact and does not require drop frame.

**Encode**—a) The process of combining analog or digital video signals, e.g., red, green and blue, into one composite signal. b) To express a single character or a message in terms of a code. To apply the rules of a code. c) To derive a composite luminance-chrominance signal from R, G, B signals. d) In the context of Indeo video, the process of converting the color space of a video clip from RGB to YUV and then compressing it. See Compress, RGB, YUV. Compare Decode.

**Encryption**—a) The process of coding data so that a specific code or key is required to restore the original data. In broadcast, this is used to make transmission secure from unauthorized reception as is often found on satellite or cable systems. b) The rearrangement of the bit stream of a previously digitally encoded signal in a systematic fashion to make the information unrecognizable until restored on receipt of the necessary authorization key. This technique is used for securing information transmitted over a communication channel with the intent of excluding all other than authorized receivers from interpreting the message. Can be used for voice, video and other communications signals.
F

**Frequency Division Multiplex (FDM)**—A technology that transmits multiple signals simultaneously over a single transmission path, such as a cable or wireless system. Each signal travels within its own unique frequency range (carrier), which is modulated by the data (text, voice, video, etc.).

**Feedback**—

a. Information from one or more outputs to be used as inputs in a control loop.
b. A loop caused by audio or video signal being fed back into itself. In video the effect is caused when a camera is directed at its receiving monitor. In audio the effect, manifested as an echo or squeal, is caused when a microphone is aimed at a speaker.  
c. A loud squeal or howl caused when the sound from a loudspeaker is picked up by a nearby microphone and reamplified. Also caused when the output of a tape recorder is fed back into the record circuit.

**Floppy Disk**—Mass-storage device that uses a flexible (floppy) diskette to record information. See Disk.

**FM Recording**—The data signal is used to modulate the frequency of a “carrier” having a frequency much higher than any spectral component of the data signal. Permits the recording of DC or very low signal frequencies.

**Format**—

a. The configuration of signals used for interconnecting equipment in a specified system. Different formats may use different signal composition, reference pulses, etc. A variety of formats are used to record video. They vary by tape width (8 mm, 1/2", 3/4", 1"), signal form (composite, Y/C, component), data storage type (analog or digital) and signal standard (PAL, NTSC, SECAM).  
b. For data storage media (hard disks, floppies, etc.), the process of initializing the media prior to use. Formatting effectively deletes any data that was previously on the media. See Format Disk.

**Format Disk**—The process of preparing a disk for data storage by determining where data is to be placed and how it is to be arranged on disk.

**Formatting**—The transfer and editing of material to form a complete program, including any of the following: countdown, test patterns, bars and tone, titles, credits, logos, space for commercial, and so forth.

**Frame**—

a. A frame consists of all the information required for a complete picture. For interlaced scan systems, there are two fields in a frame. For progressive video, these lines contain samples starting from one time instant and continuing through successive lines to the bottom of the frame.  
b. A complete picture composed of two fields. In the NTSC...
system, 525 interlaced horizontal lines of picture information in 29.97 frames per second.
In the PAL system, 625 interlaced horizontal lines of picture information in 25 frames per second. c) The metal cabinet, which contains the switcher’s circuit boards. d) One complete video image, containing two fields. There are 30 frames in one second of NTSC video.

H

Hash or Hash Value—Numerical values, generated by hashing functions, used to substantiate the integrity of digital evidence and/or for inclusion/exclusion comparisons against known value sets. It is a method for confirming the integrity of a file. A hash value is assigned to a file by special software programs then compared with the file after it is copied (or transferred to another medium or location). If the hash values match, the integrity of the file is confirmed. If not, something – maybe only one pixel – changed, which could diminish the evidentiary value of the file.

I

Image—A two dimensional (usually) picture. The picture may be represented in digital form or mathematically, as an image is a set of planes in two dimensions. The two dimensions are the resolution in X and Y (columns, lines). The origin (0, 0) of the image is sometimes its lower left corner. There are four basic types of images: black & white or color, mask or no mask, Z plane or no Z plane, IPR information or no IPR information.

Image Authentication—This is the scientific examination process used to verify that the information content of the analyzed material is an accurate rendition of the original data by some defined criteria. These criteria usually involve the interpretability of the data, and not simple format changes that do not alter the meaning or content of the data. Examples include: Determining the degradation of a transmitted image; Determining whether a video is an original recording or an edited version; Evaluating the degree of information loss in an image saved using lossy compression. Determining whether an image contains feature-based modifications such as the addition or removal of elements in the image (e.g., adding bruises to a face).

Image Compression—a) Process used to reduce the amount of memory required to store an image. See JPEG, MPEG and Decimation. b) Application of an appropriate transfer function to the image signal so as to limit dynamic range. c) Application of bandwidth limiting or bit rate reduction to an image signal in order to bring it within the limitations of a lower capacity channel.
Image File—A format for storing digital images. To save disk space, images are compressed in a binary file. The image format is contained in a file header which is read by all the programs. The header contains: the image name, the resolution, the type of image.

Institute of Electrical and Electronics Engineers (IEEE)—Is the world’s largest technical professional society. Founded in 1884 by a handful of practitioners of the new electrical engineering discipline, today’s Institute includes 46,000 students within a total membership of nearly 320,000 members who conduct and participate in its activities in 150 countries. The technical objectives of the IEEE focus on advancing the theory and practice of electrical, electronics and computer engineering and computer science. The main IEEE information system is in Piscataway, New Jersey, USA.

Integrity—a) The completeness of the potential evidence throughout its lifecycle. b) The degree to which a system or component prevents unauthorized access to, or modification of, digital video and or data associated with such video. c) The steadfast adherence to a strict moral or ethical code set by guidelines in the policy and procedures process of handling in car video.

Jogging—Single-frame forward or backward movement of videotape.

Joint Photographic Expert Group (JPEG)—Compression technique for still images, such as photographs, a single video frame, etc. JPEG can be used to compress motion video however it is not as efficient as MPEG, which has been optimized for motion video compression applications.

JPEG-1—ISO/IEC DIS 10918-1 begins with a digital image in the format Y, CB, CR (such as defined in CCIR 601-2) and provides several levels of compression. Predictive coding and transforms are employed, with the higher compression ratios selectively recognizing the decrease in human visual acuity with increasing spatial frequencies. It is optimized for about 15:1 compression. As increased data storage and increased processing capabilities are becoming available, there is exploration of adapting JPEG-1 for application to successive frames in real time; i.e., full-motion JPEG.

JPEG-2—ISO/IEC CD 11172 describes procedures for compliance testing in applications of JPEG-1.

JPG—Filename extension for graphic image files stored using JPEG compression.
Key-Length-Value (KLV)—The grouping of information concerning a single metadata element that combines three pieces of information: its UL Data Key; the Length of its instantiation Value in the next field; its instantiated Value in the allowed format.

Key, Length, and Value (KLV)—A data-encoding protocol (SMPTE 336M) that complies with International Standards Organization rules for Object Identifier data and SMPTE Universal Label (SMPTE 298M). This is the “header” information in a metadata stream that will identify the data and which metadata dictionary of definitions should be used for the metadata that follows. KLV and UMIDs (Unique Material Identifiers) are the basic engineering building blocks that have been designed to make metadata easier to exchange between different media (such as tapes or files) and metadata standards.

Layer—a) A term used to describe which video is on top of which background versus foreground and subsequent keys superimposed. b) One of the levels in the data hierarchy of the video and system specification. c) In a scalable hierarchy, denotes one out of the ordered set of bit streams and (the result of) its associated decoding process. d) The plane of a DVD disc on which information is recorded in a pattern of microscopic pits. Each substrate of a disc can contain one or two layers.

Liquid Crystal Display (LCD)—A screen for displaying text/graphics based on a technology called liquid crystal, where minute currents change the reflectiveness or transparency of selected parts of the screen. The advantages of LCD screens are: very small power consumption (can be easily battery driven) and low price of mass-produced units. Its disadvantages presently include narrow viewing angle, somewhat slower response time, and invisibility in the dark unless the display is backlit, difficulties displaying true colors and resolution limitations.

Legacy—a term used to describe a hybrid disc that can be played in both a DVD player and a CD player.

Lens—The curved glass on a video camera or camcorder that collects light and focuses it.

Letterbox—a) An MPEG video term for which the parameters have a defined set of constraints within a particular profile. b) A television system that limits the recording or transmission of useful picture information to about three-quarters of the available vertical picture height of the distribution format (e.g., 525-line) in order to offer program material
that has a wide picture aspect ratio. c) Term generally used for the form of aspect ratio accommodation involving increasing vertical blanking.

Library—As in a book library, it is somewhere one might keep effects, i.e., on a disk or collection of disks hence a library of canned effects.

Log File—A record of actions, events, and related data.

Lossless (Compression)—a) Reducing the bandwidth required for transmission of a given data rate without loss of any data. b) Image compression where the recovered image is identical to the original. c) The reconstructed data is degraded relative to the source material by the method of removal of redundant information from the media while compressing.

Lossy (Compression)—a) Image compression where the recovered image is different from the original. b) Compression after which some portion of the original data cannot be recovered with decompression. Such compression is still useful because the human eye is more sensitive to some kinds of information than others, and therefore does not necessarily notice the difference between the original and the decompressed image. c) Reducing the total data rate by discarding data that is not critical. Both the video and audio for DTV transmission will use lossy compression.

**M**

Media—The video, audio, graphics, and rendered effects that can be combined to form a sequence or presentation.

Metadata—Data, frequently embedded within a file that describes information about or related to the file or directory in which it is embedded. This may include but is not limited to the locations where the content is stored, dates and times, application specific information, and permissions.

Metadata Dictionary—The standard database of approved, registered data element tags, their definitions and their allowed formats.

Mole Technology—A seamless MPEG-2 concatenation technology developed by the ATLANTIC project in which an MPEG-2 bit stream enters a Mole-equipped decoder, and the decoder not only decodes the video, but the information on how that video was first encoded (motion vectors and coding mode decisions). This “side information” or “metadata” in an information bus is synchronized to the video and sent to the Mole-equipped encoder. The encoder looks at the metadata and knows exactly how to encode the video. The video is encoded in exactly the same way (so theoretically it has only been encoded once) and
maintains quality. If an opaque bug is inserted in the picture, the encoder only has to decide how the bug should be encoded (and then both the bug and the video have been theoretically encoded only once). Problems arise with transparent or translucent bugs, because the video underneath the bug must be encoded, and therefore that video will have to be encoded twice, while the surrounding video and the bug itself have only been encoded once theoretically. What Mole cannot do is make the encoding any better. Therefore, the highest quality of initial encoding is suggested.

**Motion JPEG**—Applications where JPEG compression or decompression is speeded up to be able to process 25 or 30 frames per second and is applied real-time to video. Even though a video signal is being processed, each field is still individually processed.

**Moving Picture Experts Group (MPEG)**—An international group of industry experts set up to standardize compressed moving pictures and audio. The first release of the MPEG standard was called MPEG-1 (ISO/IEC 11172-1).

**Moving Picture Experts Group 1 (MPEG-1)**—ISO/IEC CD 11172 is the first of the standards designed for handling highly compressed moving images in real-time. It accepts periodically chosen frames to be compressed as in JPEG-1, predicts the content of intervening frames, and encodes only the difference between the actual and the prediction. Audio is compressed synchronously. The encoder includes a decoder section in order to generate and verify the predictions. At the display, a much simpler decoder becomes possible. MPEG-1 is optimized for a data rate of up to 1.5 Mbps. MPEG expects to develop a series of compression codes, optimized for higher bit rates.

**Moving Picture Experts Group 2 (MPEG-2)**—MPEG-2 expands the MPEG-1 standard to cover a wider range of applications.

**Moving Picture Experts Group 3 (MPEG-3)**—MPEG 3 was originally intended for HDTV applications but has since been incorporated into MPEG 2.

**Moving Picture Experts Group 4 (MPEG-4)**—The goal of MPEG-4 is to establish a universal and efficient coding for different forms of audio-visual data, called audio-visual objects. Coding tools for audio-visual objects are being developed to support various functionality’s, such as object-based interactivity and scalability. The syntax of the audio-visual objects is being developed to allow for description of coded objects and to describe how they were coded. This information can then be downloaded into a decoder.

**MPEG Audio**—Audio compressed according to the MPEG perceptual encoding system. MPEG-1 audio provides two channels, which can be in Dolby Surround format. MPEG-2 audio adds data to provide discrete multichannel audio. Stereo MPEG audio is the mandatory audio compression system for 625/50 (PAL/SECAM) DVD-Video.
Multimedia Evidence—Analog or digital media, including, but not limited to, film, tape, magnetic and optical media, and/or the information contained therein.

National Television System Committee (NTSC)—The organization that formulated the “NTSC” system. Usually taken to mean the NTSC color television system itself, or its interconnect standards. NTSC is the television standard currently in use in the U.S., Canada and Japan. NTSC image format is 4:3 aspect ratio, 525 lines, 60 Hz and 4 MHz video bandwidth with a total 6 MHz of video channel width. NTSC uses YIQ. NTSC-1 was set in 1948. It increased the number of scanning lines from 441 to 525, and replaced AM sound with FM.

Non-Drop Frame Time Code—SMPTE time code format that continuously counts a full 30 frames per second. Because NTSC video does not operate at exactly 30 frames per second, non-drop frame time code will count 108 more frames in one hour than actually occur in the NTSC video in one hour. The result is incorrect synchronization of time code with clock time. Drop frame time code solves this problem by skipping or dropping 2 frame numbers per minute, except at the tens of the minute count.

Pack—A layer in the MPEG system coding syntax for MPEG systems program streams. A pack consists of a pack header followed by zero or more packets. It is a layer in the system coding syntax.

Peripheral—Any interface (hardware) device connected to a computer that adds more functionality.

Perm’ed—Magnetized to a level which cannot be remove with a handheld degausser.

Pixel (Picture Element)—Related to a particular image address in digital systems or to the smallest reproducible element in an analog system. A single point on the screen. As an example, if a system is said to have a display resolution of 1280 by 1024, there are 1280 pixels per horizontal line and 1024 horizontal lines from the top of the screen to the bottom.

Playback—The reproduction of sound previously recorded on a tape.

Playback Demagnetization—A loss of magnetization and thus a degradation of recorded information caused by repeated playing of a recorded tape.
Potential Evidence—Items that have yet to be determined if it will be used in the adjudication of civil or criminal activity. The items under consideration are: Video recordings; Audio recordings; Metadata associated with the recorded potential evidence.

Print-to-Tape—Outputting a digital video file for recording onto a videotape.

Print-to-Video—A feature of Adobe Premiere that enables you to play a clip or the timeline centered on a monitor. If the clip or timeline is smaller than the full screen, it will play alone or on a black background. Print-to-video is useful for previewing the program in the timeline, for viewing source clips or individual files, or for video playback because it allows you to play a quarter screen video at full screen size. Some capture cards do not support print-to-video.

RCA Connector—A type of connector used on all consumer VCRs and camcorders to carry the standard composite video and audio signals.

Real Time—a) Actual elapsed time (as opposed to “tape time”). b) Displaying an image or responding to a user’s request almost simultaneously. When you display an animation in real time, you perform the movements at the speed you made them in the animation. c) Computation or processing done in the present to control physical events occurring in the present. For example, when a digital effects system operator moves a joystick and the video images on the monitor appear to move simultaneously, the computations required to make the images move are said to have occurred in real time. d) A transmission that occurs right away, without any perceptible delay. Very important in video conferencing, as much delay will make the system very unusable.

Recorder, Video—Equipment for making a record of a video waveform so that the mapped images may be stored and subsequently retrieved as the video waveform.

Reference Video—a) Video signal which is used to synchronize different pieces of video equipment by providing a common timing signal. It is generated from a single source and distributed. Typically, reference video consists of black color or color bars, and control track pulses. b) A composite video signal used to compare all other video signals to for timing purposes.

Reflections or Echoes—In video transmission, this may refer either to a signal or to the picture produced. a) Signal: Waves reflected from structures or other objects; waves which are the result of impedance or other irregularities in the transmission medium. b) Picture: “Echoes” observed in the picture produced by the reflected waves.
**Restore (Files)**—To copy files that once resided on your hard disk from another disk or a tape back onto your hard disk.

**Read-Only Memory (ROM)**—Permanently programmed memory. Mask programmed ROMs are programmed by the chip manufacturer. PROMs (Programmable ROMs) can be programmed by the user. EPROMs (Erasable PROMs) can be erased with ultraviolet light and then reprogrammed.

**Scalability**—a) Scalability is the ability of a decoder to decode an ordered set of bit streams to produce a reconstructed sequence. Moreover, useful video is output when subsets are decoded. The minimum subset that can thus be decoded is the first bit stream in the set which is called the base layer. Each of the other bit streams in the set is called an Enhancement Layer. When addressing a specific Enhancement Layer, lower layers refer to the bit stream which precedes the Enhancement Layer. b) A characteristic of MPEG-2 that provides for multiple quality levels by providing layers of video data. Multiple layers of data allow a complex decoder to produce a better picture by using more layers of data, while a more simple decoder can still produce a picture using only the first layer of data. c) The degree video and image formats can be combined in systematic proportions for distribution over communications channels for varying capacities. d) Scalability implies that it is possible to decode just a fraction of the information in a bit stream. In MPEG we find SNR scalability, spatial scalability, and temporal scalability, and even in combination (hybrid scalability). In connection with scalability we find the terms “lower layer”, which represents the basic information, and the “Enhancement Layer”, which represents the additional information. In case of hybrid scalability, up to three layers are found. All types of scalability may be utilized for transmission systems with split data channels with different error rate. The lower layer is transmitted on a channel with high protection rate, whereas the Enhancement Layer then is transmitted on a channel with higher bit error rate. e) A feature of the Indeo video codec with which quality can be optimized during playback depending on the system resources being used to play the video.

**Scrambling**—a) Usually used as a synonym for encryption, controlled disordering of a signal to prevent unauthorized reception. b) Sometimes used to describe controlled disorganization of a signal to improve its robustness. This form is more often called shuffling. c) To transpose or invert digital data according to a prearranged scheme in order to break up the low-frequency patterns associated with serial digital signals. d) The digital signal is shuffled to produce a better spectral distribution. e) The alteration of the characteristics of a video, audio, or coded data stream in order to prevent unauthorized reception of the information in a clear form. This alteration is a specified process under the control of a conditional access system.
Standard—The specific signal configuration, reference pulses, voltage levels, etc., that describe the input/output requirements for a particular tape of equipment. Some standards have been established by professional groups or government bodies (such as SMPTE or EBU). Others are determined by equipment vendors and/or users.

Standard Input Format—Video format developed to allow the storage and transmission of digital video. The 625/50 SIF format has a resolution of 352 x 288 active pixels and a refresh rate of 25 frames per second. The 525/59.94 SIF format has a resolution of 352 x 240 active pixels and a refresh rate of 29.97 frames per second. MPEG 1 allows resolutions up to 4095 x 4095 active pixels, however, there is a “constrained subset” of parameters defined as SIF. The computer industry, which uses square pixels, has define SIF to be 320 x 240 active pixels, with a refresh rate of whatever the computer is capable of supporting.

Start of Active Video (SAV)—Digital data that indicate the start of active video time in serial digital component video systems.

S-VHS (Super VHS)—a) An improved version of the VHS tape format capable of recording better picture resolution (definition). A higher-density tape is required which provides a wider luminance bandwidth, resulting in sharper picture quality (> 400 horizontal lines vs. 240 for standard VHS) and improved signal-to-noise ratio. Because the equipment is usually smaller and lighter than 3/4” equipment, it is ideally suited for ENG/EFP applications.
b) Super VHS, a consumer videotape format offering horizontal resolution somewhat greater than that offered by NTSC broadcasting but allowing component recording and playback without cross-luminance or cross-color artifacts through a four-pin S-Video connection.

Sync—a) Abbreviation for synchronization. Usually refers to the synchronization pulses necessary to coordinate the operation of several interconnected video components. When the components are properly synchronized, they are said to be “in sync”. b) Signals which control the sweep of the electron beam across the face of the display. The horizontal sync, or HSYNC for short, tells the display where to put the picture in the left-to-right dimension, while the vertical sync (VSYNC) tells the display where to put the picture from top-to-bottom. c) The portion of an encoded video signal which occurs during blanking and is used to synchronize the operation of cameras, monitors, and other equipment. Horizontal sync occurs within the blanking period in each horizontal scanning line, and vertical sync occurs within the vertical blanking period.

Syntax—a) The description of the binary format of an information unit. b) The rules governing construction or formation of an orderly system of information. For example, the syntax of the MPEG video encoding specification defines how data and associated instructions are used by a decoder to create video pictures.

Synthesizer—An analog or digital generator which can produce any wanted frequencies or sounds.
T1Q1.5—The T1Q1.5 Video Teleconferencing/Video Telephony (VTC/VT) ANSI Subworking Group (SWG) was formed to draft a performance standard for digital video. Important questions were asked, relating to video digital performance characteristics of video teleconferencing/video telephony: a) Is it possible to measure motion artifacts with VTC/VT digital transport? b) If it can be done by objective measurements, can they be matched to subjective tests? c) Is it possible to correlate the objective measurements of analog and digital performance specification? The VTC/VT Subworking Group’s goal is to answer these questions. It has become a first step to the process of constructing the performance standard.

Termination Switch—A switch that connects and disconnects a load resistance to a video input, used to terminate the line. In order for a video signal to be correctly transmitted without loss, proper end of line impedance is essential. Amplitude errors and reflections will otherwise result. A 50 or 75 ohm resistor is usually employed to accomplish this. When the termination switch is off, the unterminated video signal is looped to the next device where the signal can be transmitted in parallel. The final device in the chain must be terminated using the termination switch.

Time Code—a) A digital code number recorded onto a videotape for editing purposes. When decoded, the time code identifies every frame of a videotape using digits reading hours:minutes:seconds and frames. Each individual video frame is assigned a unique address, a must for accurate editing. The three time code systems used for video are VITC, LTC and RC (consumer). b) Electronically generated digital clock information which is recorded onto tapes on a special track such that an editor can accurately locate individual frames (fields) of video information for editing purposes. The SMPTE standard for encoding time in hours, minutes, seconds and frames and video.

Time Lapse Video Recording—The intermittent recording of video signals at intervals to extend the recording time of the recording medium. It is usually measured in reference to a 3-hour (180-minute) tape.

Time Stamp—a) A term that indicates the time of a specific action such as the arrival of a byte or the presentation of a presentation unit. b) A sampled value of a counter at an instant of time. It is used as a timing signal that may be contained in a synchronous data stream. c) An indication of a particular time instant relative to a time base.
Unique Material Identifier (UMID)—A SMPTE standard (SMPTE 300M/RP205) for metadata. The basic UMID contains 32 bytes of unique identification information (12 bytes identifying it as UMID data, followed by length and identification values). The extended UMID has an additional 32 bytes of information that contain “signature information” (time and data of creation, longitude, latitude, and altitude, as well as country, organization, and user codes).

Uncompressed Video—A recorded or digitized video stream that is not processed by a data compression scheme. The video signal remains uncompressed at all stages of the process: input, storage, and output. Uncompressed video conforms to the ITU-R 601 standard.

Uncompressed-Quality Video—Video that has the same image quality as uncompressed video, but has been compressed using mathematically lossless compression to optimize storage space.

Video Cassette Recorder (VCR)—An analog magnetic recording and playback machine. Generally used for recording and viewing full-motion video.

Vehicle Video Evidence Capture System Reference Lifecycle—The stages or states in which the recording equipment in the vehicle, e.g., recorder, camera, etc., will exist from the time it is first received by the operating agency until it is properly disposed of.

Video Home System (VHS)—Consumer videocassette record/playback tape format using half-inch wide magnetic tape. The most common home VCR format in the U.S.

VHS Hi-Fi—An improved stereo audio recording/playback system found on some camcorders and VCRs. Because the audio tracks are mixed and recorded with the video signal, audio only dubbing of these tracks is not possible.

VHS-Compact (VHS-C)—A miniature version of the VHS tape format utilizing smaller cassettes that may also be played on standard VHS machines by using an adapter cartridge. Video — a) A term pertaining to the bandwidth and spectrum position of the signal which results from television scanning and which is used to reproduce a picture. b) A complex and sophisticated electronic signal which, when properly processed by a television receiver can be used to provide full color pictures. c) An electrical signal used to carry visual information. Composite video includes sync and blanking signals. Non-composite video does not include sync.
Video Camera—A camera which contains an electronic image sensor rather than photographic film. The lens focuses an image on an electronic tube or CCD chip. A camera has electronic circuitry which generates color and sync pulses. Most portable consumer cameras are equipped with a full complement of audio circuitry, e.g., microphone, audio amplifier and additional audio electronics. In order to obtain better quality images, a professional camera has three tubes or a triple CCD system, one for each basic color. Most professional cameras have a genlock input, which allows the camera to be synchronized to an external source. Some cameras also include basic character generators for titling purposes.

Video Evidence Physical Recording Media Lifecycle—The stages or states in which the removable recording media used to capture video evidence, e.g. digital tape, Digital Video Disk (DVD) etc., will exist from the time it is first received by the operating agency until it is properly disposed of.

Video Format—A standard that determines the way a video signal is recorded onto videotape. Standards include: DV, Digital 8, 1-inch Type C, 3/4-inch U-Matic, 3/4" U-Matic, 8 mm, Beta, Beta ED, Betacam, Betacam SP, SP, D-1, DCT, D-2, D-3, D-5, Digital Betacam, Hi8, M-II, VHS, and S-VHS.

Video Recording—The converting of an image, moving or still, into a video signal that can then be recorded. Video recording is usually performed by using of a video camera.

Videocassette—A length of videotape wound around two reels and enclosed in a plastic shell.

Videocassette Recorder (VCR)—An electronic component consisting of a tuner, an R modulator, and a video deck used for recording and playback of a videocassette.

W

Wavelength—in tape recording, the shortest distance between two peaks of the same magnetic polarity; also, the ratio of tape speed to recorded frequency.

What You See Is What You Get (WYSIWYG)—Usually, but not always, referring to the accuracy of a screen display to show how the final result will look. For example, a word processor screen showing the final layout and typeface that will appear from the printer.