AVS

Forensic Video Surveillance Best Practices

A CSI Perspective

Who Should Read this Guide

This guide is intended for CIOs, CTOs and IT directors faced with the challenge of ensuring failsafe video capture and retention in high-risk environments

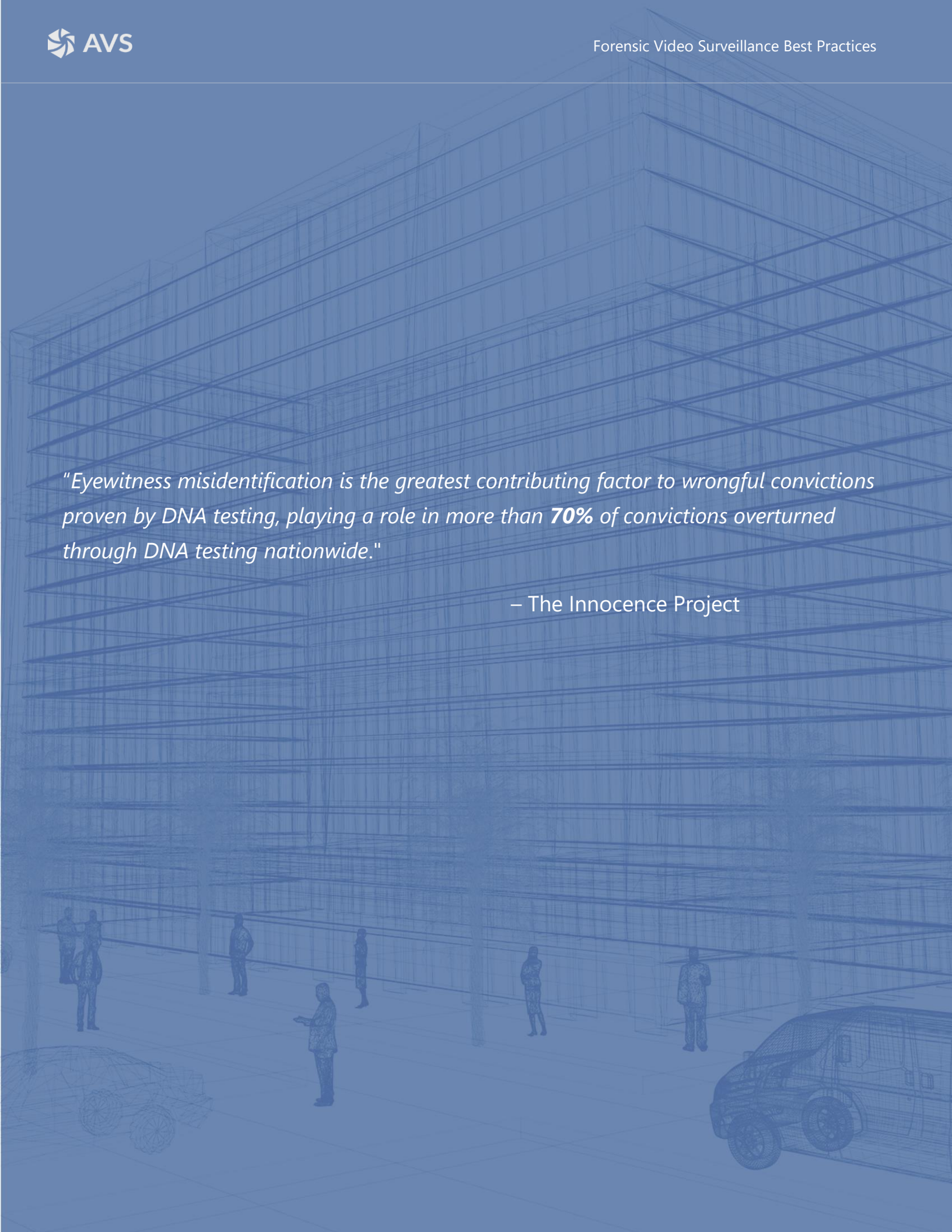
It is of particular interest to C-level executives, VPs, managers and directors whose professional responsibility is involved with the safety, security and performance of the enterprise

Law enforcement, corporate security and risk mitigation executives

ADVICE OFFERED ABOUT

- The four tests criminal courts use to accept video as admissible evidence
- The seven things professional forensic video analysts look for when evaluating surveillance footage in court
- Planning and deployment of effective network architectures
- Functional specifications for forensic-compliant systems

Table of Contents



*"Eyewitness misidentification is the greatest contributing factor to wrongful convictions proven by DNA testing, playing a role in more than **70%** of convictions overturned through DNA testing nationwide."*

– The Innocence Project

Abstract

The thousands of industry professionals in charge of maintaining one or more video surveillance networks know it's only a matter of time before the footage their systems capture will wind up in court.

Well-designed surveillance systems compress the time between the crime, the police investigation, and ultimately, a successful criminal conviction. Companies with poorly-designed or outdated surveillance systems could see their footage not admitted as evidence, or even inadvertently help a suspect walk free.

This white paper explores industry best practices that will help you produce better video footage today, and tips on how to improve the design of your next surveillance system. It also explores the four legal tests criminals court use to measure video evidence, and the seven things forensic video analysts look for when testifying in court.

San Francisco's Robbery Ring

Before surveillance cameras, it would have been the perfect crime.

A group of young people enter a store at once, spread out and begin shoveling tens of thousands of dollars worth of high-end products into big shopping bags. Within 60 seconds, they're gone--sometimes after threatening store employees with pepper spray and knives on their way out.

In San Francisco, the group was so active that police in 2014 nicknamed them the Rainbow Crew, for their brightly colored outfits and dyed hair. For the next year and a half, they evaded police, along the way stealing hundreds of thousands of dollars worth of merchandise across the western United States.

Blitz-style robberies have historically been difficult to analyze on older surveillance systems. Teenagers running through a store showed up as pixelated figures. Individual facial features were tough to pick out. A low frame rate might result in one suspect disappearing offscreen, while a second takes her place.

Good defense lawyers would pick apart each of these inconsistencies, casting doubt on the video evidence in court.

How Police Made a Break in the Case

What the Rainbow Crew didn't know was that their robberies in San Francisco's Union Square were being recorded by more than 300 next-generation surveillance cameras installed and managed by AVS. These cameras captured smooth, high-resolution video so clear that police in one case were able to name individual suspects within days of the robbery.

That video footage later formed the foundation of the criminal charges filed against more than a dozen suspected members of the Rainbow Crew. It's very likely this crime spree would have been more difficult to solve, and harder to prosecute, without high-definition video.

The value of a surveillance system is only as good as its ability to capture forensic-grade evidence, help police identify suspects and eventually aid prosecutors in making convictions.

In this white paper, we'll examine what it takes to consistently produce forensic-grade video, and share best practices that will be universally useful to everyone tasked with maintaining North America's 62 million surveillance cameras.

For our purposes, it's useful to start by looking at where video evidence eventually ends up—in court—and work our way back to the source.

Forensic Video Analysts

In criminal cases where surveillance footage gets entered as evidence, prosecutors and defense attorneys typically hire a professional forensic video analyst to closely examine the footage and later testify about its content in court.

On the witness stand (and in subsequent cross examination), lawyers ask video analysts to answer a few key questions: What is happening in the video? Is the video accurate? If there are inconsistencies, why do they exist? Why is the video choppy or low-quality, and does that cast doubt on its accuracy? Can a jury say, without any doubt, that the person committing the crime on the video is the same person being charged with the crime?

How Courts Determine Evidence Admissibility

The judge in the case will look for four things before allowing video surveillance to be entered as evidence:

1. ***Authenticity:*** Is the footage a true and accurate reflection of the alleged crime?
2. ***Preservation:*** How did the company managing the surveillance footage keep and maintain their video storage devices?
3. ***Policy:*** Did the company or government agency that captured the footage have a formal policy in place for evidence collection and preservation?
4. ***Admissibility:*** Is the evidence relevant to the fact that either side is trying to prove in court? Generally, if the evidence passes the first three steps, its admissibility is all but guaranteed.

Let's unpack this idea of *authenticity*, as it's where companies often see their video evidence put into question. A little later, we'll touch on preservation and policy, as both are more straightforward.

Accurate Timestamps

Forensic video analysts begin by *examining the timestamp* on the video footage, and whether it was accurate at the time the alleged crime occurred.

This is particularly important in cases where the video footage only captures part of the crime's timeline—say, if a car pulled into a parking space, two people got out and walked around a blind corner. Can prosecutors prove the two people in the video later committed the crime? An inaccurate timestamp throws that evidence into question.

CONSIDER THIS EXAMPLE

A woman calls 911 at 10 a.m. to report an active burglary at her neighbor's house. The burglars flee on foot. Later, police investigators reviewing nearby surveillance footage find the suspected burglars leaving the house at 9:00:12, but they know the woman called 911 at 10:00:12. The one-hour discrepancy is likely a time error due to Daylight Savings time, but that error nonetheless calls into question the accuracy and authenticity of the evidence.

In court, prosecutors can submit documentation explaining why the timestamp was inaccurate at the time, and how far off it really is. During a surveillance system's initial setup, technicians should document the timestamp's accuracy, and again in subsequent maintenance cycles. Intelligent video surveillance systems are able to automatically notify operators when the timestamp is inaccurate, and adjust for Daylight Savings Time and leap year.

Image Quality Best Practices

Forensic video analysts will next look for *image quality*, *camera placement* and *lighting*. Good video footage is capable of capturing uniquely identifying facial features, tattoos, birthmarks, specific clothing patterns, license plates or an object the suspect was holding in their hand at the time of the crime.

Let's take a look at a few examples. The following image is badly pixelated, and would likely not provide forensic level evidence:

This image shows multiple suspects committing "grab and run" thefts before dashing out the door. It's hard to pick out the color of their clothing, or any defining facial features. Such issues could be due to number of factors like -- camera placement, image resolution, lighting, color representation specific to the make and model of the camera, type of video compression, or an unusually low frame rate setting.

Compare that to this image, which provides much clearer, forensic-quality detail. This still image contains faces with identifiable features, clothing patterns and details like the color of a person's sunglasses and headphones.

Consider the man in the foreground, wearing a t-shirt and a backward Golden State Warriors baseball cap. If he were to be involved in a crime, a trained, experienced forensic video analyst would likely be able to testify on the details of the baseball cap, and compare it to a baseball cap found at the scene.

How to Improve Frame Rate

Image quality partly hinges on the surveillance systems' frame rate, or the number of images it captures per second. 30 frames per second is typically sufficient to capture smooth, normal motion. Systems that capture fewer frames per second run the risk of missing key moments in time--for example, an armed robbery where the suspect briefly flashes a weapon that the video fails to pick up, or a fight that shows two people squaring off, and suddenly one of them on the ground.

In those two cases, defense lawyers will rightfully question whether their client was carrying a weapon at all, or who threw the first punch.

Optimal Camera Placement

Surveillance system designers should place cameras in key places, with correct angles and good lighting, to consistently capture useful video. This might be a building's choke point, an entrance or exit, or a turnstile with controlled lighting.

Cameras should be configured to capture three levels of detail--overall, intermediate and close-up. A wide-angle camera mounted overhead, with a dynamic range to adapt to various lighting conditions, captures the overall area--think parking lots and store layouts. Intermediate cameras capture specific avenues of travel--entrances and exits, cars entering through a gate, or the sidewalk outside a store. Close-up cameras capture a tightly-focused area, like a cash register.

Crime scene investigators use overall, intermediate and close-up video footage to establish a sequence of events in court. Ideally, each camera in a company's arsenal should be delivering forensic-level evidence.

In a related vein, police investigators often review video footage days or weeks before the actual crime, to look for evidence that the suspect "cased" the area in advance. Being able to prove the intent to commit a future crime could be crucial during the sentencing phase of a case.

Other Pillars of Admissible Video Evidence

Let's briefly touch on the two other pillars of admissible video evidence: Video preservation and written policy.

Both are fairly binary--does the company in charge of managing a surveillance system have consistent policies in place that cover how evidence is gathered and stored? Once stored, can the company ensure that footage hasn't been tampered with? How was the evidence delivered to police investigators, and does the raw footage match what's being shown in court?

Preserving Video

Raw high-definition video files can quickly consume all of the available storage on a physical hard drive or in the cloud. Most systems compensate by using codecs, which compress the footage into a smaller file for storage, and later decompress it for playback.

The system's decompressed video file is known as native video, and typically provides the highest quality playback. High-definition native video might allow investigators to advance the footage frame-by-frame, or zoom in on a subject's specific hand movements or gestures.

Police will often ask for an exported version of the native video in an open file format, like .mov with Apple QuickTime, or .avi with Windows Media Player. Open format video is typically lower quality, but sufficient to show prosecutors, defense attorneys, reporters and administrative personnel. Forensic video analysts will want to see the system's native video.

The Importance of Policy

A few tips before handing off video surveillance to the police, or a third-party: Scan flash drives and external drives for viruses before connecting them to the video surveillance system. Drives should not contain files, or any other media. Copy over both the native and open format video files captured from every relevant camera. Typically, it's helpful to include the 30 minutes before and after the suspected crime.

In San Francisco, high-definition surveillance footage was key to securing the arrests of more than a dozen suspected members of the Rainbow Crew. The footage from Union Square was so good, police were able to quickly identify individual suspects.

The network of cameras allowed police to easily follow the suspects to their getaway vehicles and identify their license plates. Accurate time and date stamps helped establish a logical timeline of events with prosecutors.

Surveillance systems should be optimized to gather useful evidence for investigators, and stand up to legal scrutiny in court.

About the Author

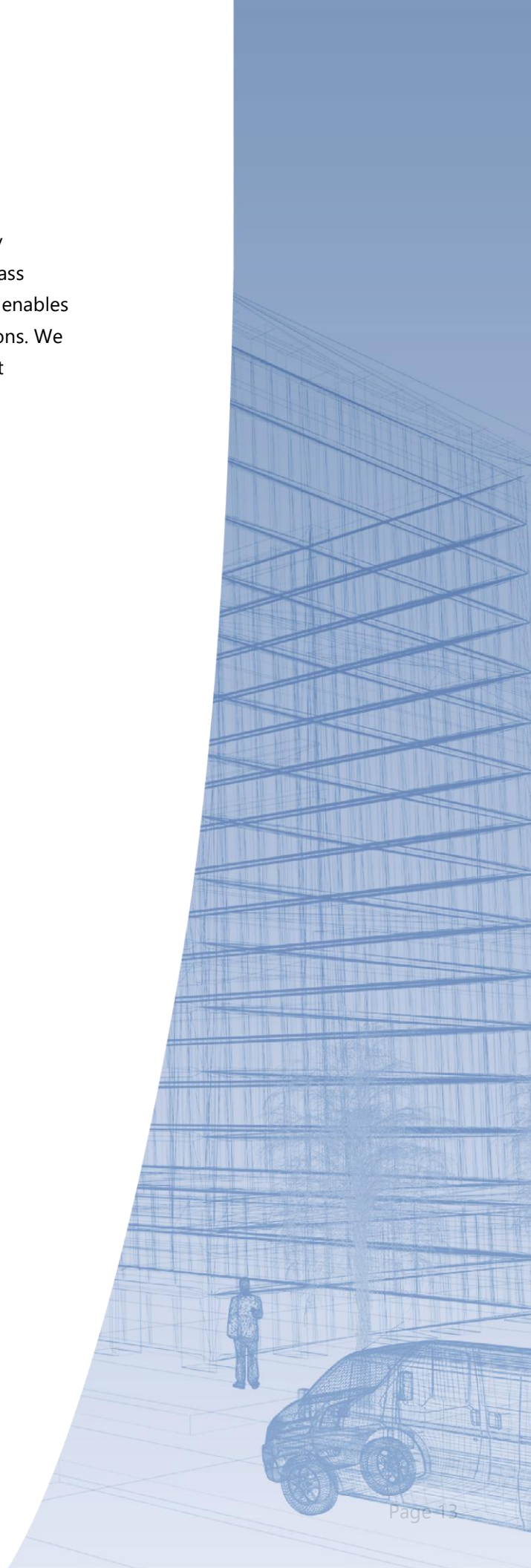
Roland Tolosa has retired after 32 years with the San Francisco Police Department. Roland has spent the last 16 years of his career as a crime scene inspector, investigating a variety of crime scenes and specializing in multimedia evidence. He has more than 500 hours of specialized training in video forensics and imaging, and has testified as a fingerprint and forensic video expert in municipal, superior and federal courts in California.

Roland co-authored LEVA's "Best Practices for the Recovery of Digital Multimedia Evidence" and SFPD/Project S.A.F.E.'s "Recommended CCTV Guidelines for Residential and Business Applications."

Prior to joining law enforcement, Roland worked in the retail security industry. He works at Applied Video Solutions as a solutions consultant.

About AVS

Applied Video Solutions (AVS) is a professional services and systems integration firm specializing in Digital Video Surveillance and Security Management Systems for a range of companies including Fortune-class enterprises. AVS also offers unique next-generation architecture that enables seamless enterprise surveillance for geographically distributed locations. We assist our clients in all phases of the surveillance network deployment lifecycle, ranging from strategic planning through system design, implementation and training.



CONTACT

Applied Video Solutions, Inc.
2601 Mission Street, Suite 401
San Francisco, CA 94110

Phone 415.824.1717
Sales sales@applyvideo.com
Support support@applyvideo.com

www.applyvideo.com