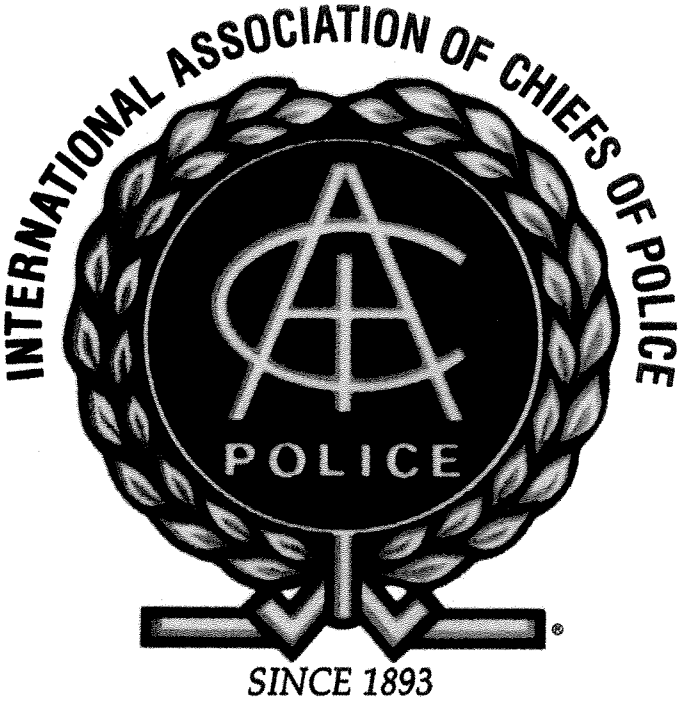


ABSTRACT

I. ABSTRACT

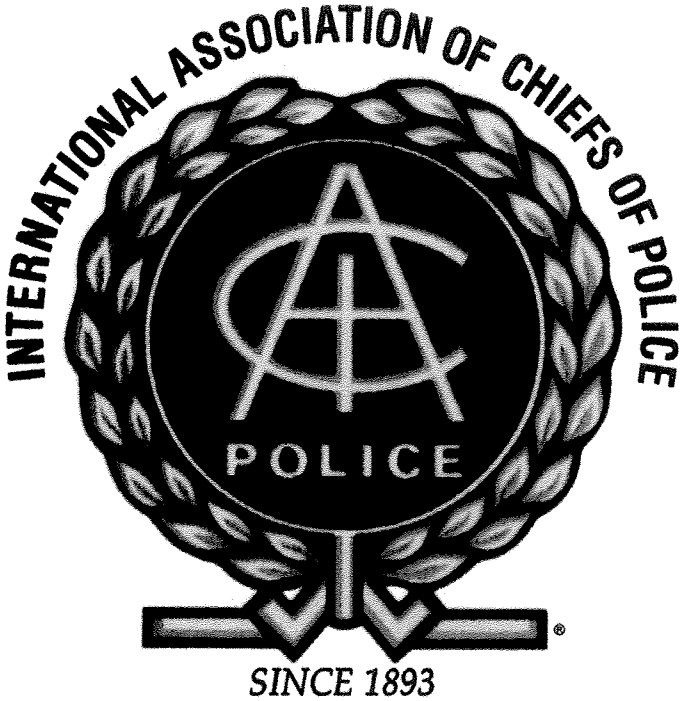
The International Association of Chiefs of Police (IACP), through its **Cutting Edge of Technology: Enhancing Local and State Law Enforcement's Understanding and Use of Emerging Technology** project, and in partnership with the Office of Science and Technology is committed to addressing the information needs of local police agencies as they assess and acquire new technology. This project has been a leader in providing law enforcement leadership with the tools and resources to expand the use of technology, train practitioners, and reduce departmental risk and liability.

In previous years, the Cutting Edge project has made significant contributions to the law enforcement profession through publications and activities such as:

- The Executive Brief, *Electro-Muscular Disruption Technology, A Nine-Step Strategy For Effective Deployment*
- The Resource Guide, *Digital Imaging For Safe Schools: A Public Safety Response to Critical Incidents*
- The Executive Brief, *Managing Police Pursuits: Findings From IACP's Police Pursuit Database*
- The development of the Framework for Digital In-Car Video Systems Minimum Performance Specifications, modeled after the IACP's radar/lidar testing and certification program.

During year six of the project, the IACP sought $424.830 to continue the development of digital in-car camera minimum performance specifications and a mobile video camera product certification and testing program. The progress made during year five in developing minimum performance specifications, combined with the assistance of the National Institute of Standards and Technology (NIST) in developing the design for testing of video systems provided the impetus to continue the specifications-development process.

In addition, the IACP was tasked with evaluating the impact/meaning of the information contained in the IACP's Police Pursuit Database. The database was developed to assist law enforcement agencies nationwide in controlling, managing and analyzing pursuit data in order to make more informed policy and training decisions. This web-based application has attracted national attention, with more than fifty agencies participating and information on more than 7,000 records contained in the database. With the assistance of the George Mason University, Administration of Justice Department, the IACP performed an analysis of the database, resulting in the report, *Police Pursuits in an Age of Innovation and Reform: The IACP Police Pursuit Database.*



SUMMARY

II. SUMMARY

Year six of the **Cutting Edge of Technology** program encompassed two tasks. Each of the tasks will be summarized individually. The IACP received $424.830 to accomplish the following tasks.

Task 1: Development of comprehensive digital in-car camera minimum performance specifications and the testing and certification program.

The rapid deployment of digital video cameras in police patrol vehicles has heightened the need for the development of performance specifications for these devices. The ability to assess the true capabilities of these systems will enable law enforcement agencies to deploy video equipment that protects and holds accountable officers and managers; collect video evidence that will meet the demands of the courts; and ensure efficiency and economy in all phases of the mobile video system lifecycle.

Since the publication of the IACP Brief on "The Use of CCTV/Video Cameras in Law Enforcement" (March 2001), much has been written regarding the proper use of these systems in patrol vehicles. What is evident is that these systems have a high degree of acceptance and use in law enforcement agencies nationwide. They are a proven, effective tool for officers and administrators alike in enforcing the law impartially and with a high degree of respect for public safety and security.

Once a department reaches a decision to purchase and deploy in-car camera systems, the task of determining system requirements, vendor selection, and training needs for those who will use the new system is critical in the final outcome of the program. During the planning and evaluation phase of video equipment selection, much attention will be given to the placement of equipment, operational guidelines, and community and officer acceptance. What is often absent, however, are recognized standards against which equipment can be measured to allow law enforcement administrators to clarify program choices among the many competing products and services offered by vendors.

The need for performance specifications is especially important with the growing popularity of digital recording systems. Many of these systems have yet to undergo rigorous field testing by an independent scientific body, an important consideration if the recorded information is to be used as evidence in court. In addition, the proprietary recording and storage formats developed by many vendors can greatly limit an agency's ability to subject the recorded video evidence to forensic examination or, in some cases, even to view or duplicate the images. Compression schemes applied by some digital recording devices or storage systems can severely degrade image quality, and in some cases can render the video unsuitable for admission as evidence in court.

There is a recognized need in the law enforcement community for the development of minimum performance specifications and a testing and certification program to support law enforcement acquisition, deployment and maintenance of in-car video systems. Based on the recommendations from the inaugural meeting of the Digital Video

Standards Advisory Panel meeting, IACP has modeled the specifications program for in-car video systems on the successful specifications program developed by the IACP for speed measuring and automated enforcement devices. This program is administered by the IACP through a cooperative agreement with the US Department of Transportation, National Highway Traffic Safety Administration (NHTSA). This program utilizes a technical advisory group to advise and make recommendations to the IACP Highway Safety Committee regarding performance specifications for these systems.

At the conclusion of year one, the IACP submitted for public review and comment the framework document for the minimum performance specifications for digital video systems. Following the 60-day review period, the Advisory Panel established a working group to develop objective, scientific and measurable testing protocols for in-car video systems. This group met several times during the project period to develop testing standards and protocols for in-car video systems.

During the project period, IACP staff attended and presented at several IACP and DOJ/NIJ sponsored conferences and meetings. These included the IACP Law Enforcement Information Managers US and international conferences, the IACP Annual Conference, the NIJ Applied Technology Conference, and the Government Video Expo.

In conjunction with the activities of the specifications development, a draft document, "Chiefs Guide to Digital In-Car Video Systems" was developed. The purpose of this document was to provide law enforcement administrators with guidance on problem identification, needs assessment, product selection and deployment considerations.

Task 2: Conduct a statistical analysis of the IACP "Police Pursuit Database".

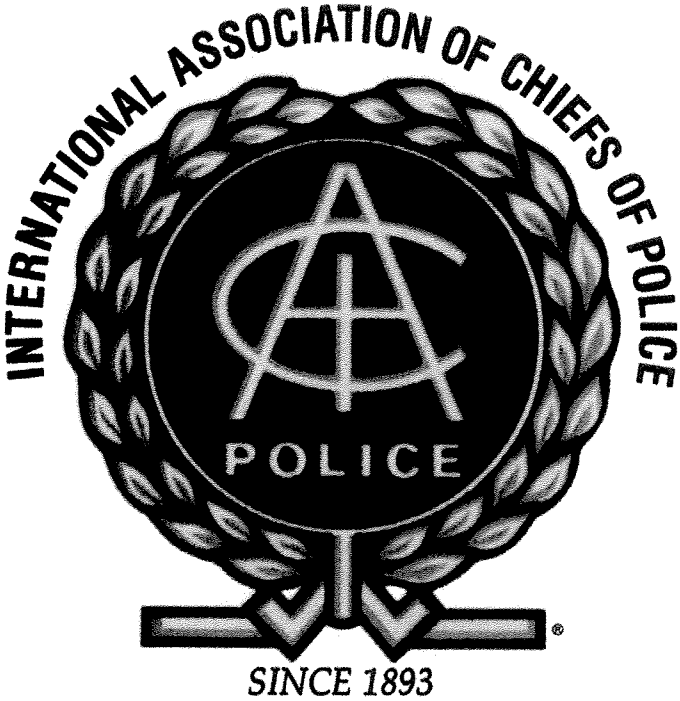
During the development phase of the "Police Pursuit Database", a core group of practitioners (users) were responsible for identifying data elements and designing forms to capture these elements for input in either an online or paper format. This users group has continued to provide suggestions/comments for enhancements to the program and to provide valuable feedback for the program.

In 2006, the IACP recommended, and the NIJ approved, a transfer of ownership of the database from IACP to a private organization, where the application will be maintained and marketed as a package with other law enforcement-related data and information tools. IACP will maintain access to the data contained within the database for analytical purposes, and will continue to actively support the database and encourage its use by member agencies.

Before the transfer of ownership was to take place, the National Institute of Justice requested the IACP to conduct a statistical analysis of the existing data in the database and to issue a report on our findings.

The IACP agreed to contract with a suitable individual or organization, identify the data elements to be analyzed, decide on a methodology and format for the data analysis and presentation, and to publish the report. In addition, the IACP would promote the database and report to member agencies.

The IACP contracted with the George Mason University Administration of Justice Department to perform the analysis of the IACP Police Pursuit Database. The resulting report, *Police Pursuits in an Age of Innovation and Reform: The IACP Police Pursuit Database"* was published and is available in print and online through the IACP Website.



GOALS AND ACCOMPLISHMENTS

III. GOALS AND ACCOMPLISHMENTS

Funds for completion of this project were awarded to IACP on September 14, 2006.

Grant Tasks for the Project:

Development of comprehensive digital in-car camera minimum performance specifications and the testing and certification program

During the project period, the IACP convened the Digital Video Standards Advisory Panel and the Executive Committee on the following occasions:

- October 2006 – IACP convened the Executive Committee in conjunction with the IACP Annual Conference in Boston, MA . The Executive Committee created the Testing and Certification Working Group to develop testing procedures and protocols for the DVS testing program.

- January 2007 – The Advisory Panel and Executive Committee met and continued deliberations by the working groups to develop performance specifications.

- March 2007 – The Testing and Certification Working Group met in Indianapolis, IN to perform field tests in developing scenes to be used by NIST in development of the prototype video quality measurement device.

- April 2007 – The Testing and Certification Working Group met at Burtonsville, MD to develop testing protocols and finalize specifications for the measures to be used by the NIST prototype testing instrument.

Project staff attended and made presentations on the Cutting Edge of Technology Project and the DVS Performance Specifications at the following conferences and meetings:

- November 2006 – Project staff made a presentation on *Digital Imaging for Safe Schools* to the OJJDP Safe Schools Workshop in Elk Grove IL.

- November 2006 – Project staff attended and made a presentation on the DVS specifications project to the First International Conference of the Law Enforcement Information Managers (LEIM) Conference.

- December 2006 – Project staff hosted a workshop on In-car video systems at the Government Video Expo in Washington, DC.

- March 2007 - IACP staff presented a workshop, "Digital Imaging for Safe Schools" to the IACP School Safety Project in March 2007.

- April 2007 – Project staff attended and made a presentation on the DVS specifications project at the NIJ Applied Technology Conference.

- May 2007 - Project staff attended and provided a project update to the IACP Communications and Technology and Criminal Justice Information Sharing Committees during the IACP Law Enforcement Information Management (LEIM) Conference in Greensboro, NC.

- May 2007 - IACP staff presented a workshop, "Digital Video Systems" at the LEIM Conference in Greensboro, NC.

Conduct a statistical analysis of the IACP Police Pursuit Database

The IACP Police Pursuit Database was initiated in 2000 by the IACP with support from the National Institute of Justice. The goal of the project was to create an internet-based interactive reporting system to allow police agencies to track and manage their own pursuits, as well as compile statistical reports from all pursuits contained in the database. The pursuit database now contains information on over 7,000 pursuits, submitted by more than fifty agencies.

In order to assure the continuation of the database as a service and resource to the law enforcement community, the IACP began negotiations with LogIn, a private company that manages other law enforcement related databases and online services. In November 2007, the IACP and LogIn reached agreement on the transfer of the

The IACP contracted with the George Mason University Administration of Justice Department to perform an analysis of the IACP Police Pursuit Database. Dr. Cynthia Lum, Deputy Director for the Center for Evidence Based Crime Policy, performed the analysis and completed the report, *Police Pursuits In An Age of Innovation and Reform: The IACP Police Pursuit Database.* This report was introduced at the IACP Annual Conference in San Diego in October 2008, as well as being made available for download via the IACP Website, www.theiacp.org.

Additional Activities

Throughout the contract period, IACP staff provided technical assistance in the form of dissemination of Cutting Edge publications to agencies throughout the United States. The following is a summary of the publications provided to law enforcement and others during the contract period:

- *Electro-Muscular Disruption Technology: A Nine-Step Strategy for Effective Deployment*
    - In 2nd reprint of Executive Brief (500 copies)
    - Electronic distribution (July 1, 2006 to Dec 31, 2006): 1715 copies
    - Hard copy distribution (July 1, 2006 to Dec 31, 2006): 483 copies
    - Total distribution (July 1, 2006 to Dec 31, 2006): **2198 copies**

- *Digital Imaging for Safe Schools: A Public Safety Response to Critical Incidents*
  - Electronic distribution (July 1, 2006 to Dec 31, 2006): 2293 copies
  - Hard copy distribution (July 1, 2006 to Dec 31, 2006): 424 copies
  - Total distribution (July 1, 2006 to Dec 31, 2006): **2717 copies**

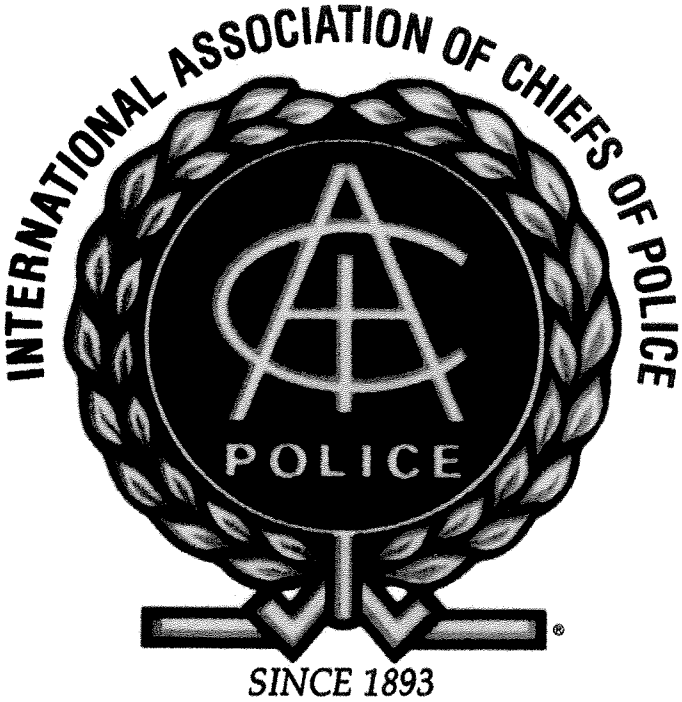
  - Requests for Digital Imaging Technical Assistance: **11** agencies
    - Amity Township, PA Police Department
    - West Bridgewater, MA Police Department
    - Baltimore County, MD Public Schools
    - Sumpter Township, MI Police Department
    - Southern University, LA Police Department
    - Tinley Park, IL Police Department
    - Environmental Protection Agency, CID
    - Oregon Department of Corrections
    - Delaware City, OH Police Department
    - Farmington, ME Police Department
    - Marshall County, AL Emergency Management Agency

- *Digital Video Systems for Public Safety: Minimum Performance Specifications Draft*
  - Electronic distribution (July 1, 2006 to Dec 31, 2006): 2566 copies
  - Total distribution (July 1, 2006 to Dec 31, 2006): **2566 copies**

- *Electro-Muscular Disruption Technology: A Nine-Step Strategy for Effective Deployment*
  - 3rd reprint of Executive Brief (500 copies)
  - Electronic distribution (January 1 to June 30, 2007): 2100 copies
  - Total electronic distribution (January 1 to June 30, 2007): 2100 **copies**

- *Digital Imaging for Safe Schools: A Public Safety Response to Critical Incidents*
  - Electronic distribution (January 1 to June 30, 2007): 2400 copies
  - Total distribution (January 1 to June 30, 2007): **2400 copies**

- *Digital Video Systems for Public Safety: Minimum Performance Specifications Draft*
  - Electronic distribution (January 1 to June 30, 2007): 2700 copies
  - Total distribution (January 1 to June 30, 2007): **2700 copies**



PROGRESS REPORTS

Grant Project Progress Report
Short Title: The Cutting Edge of Technology
Project Manager: Albert Arena
Date of Report: December 31, 2006

Project Summary

The Cutting Edge of Technology: Enhancing Local and State Law Enforcement's Understanding and Use of Emerging Technologies, is a multi-task and multi-year project to strengthen the ongoing collaboration between the IACP and OST on emerging technology issues. The ultimate goal of this project is to help law enforcement agencies better understand and utilize emerging technology.

Major objective of this project:

- The development of minimum performance specifications for digital in-car camera systems

The current award period for Cooperative Agreement 2005-DE-BX-K001is effective from September 1, 2006 through August 31, 2007.

I. Current Grant Goals for Project

The development of minimum performance specifications for digital in-car camera systems: Creation of minimum performance specifications will provide a safe and reliable context within which police agencies can identify, select, and purchase highly reliable digital in-car camera systems.

II. Grant Goals Status for this Reporting Period

The development of minimum performance specifications for digital in-car camera systems

Accomplishments:

- Developed draft framework for DVS Minimum Performance Specifications.
- Released draft document for sixty-day public comment and review period beginning June 30, 2006 and ending August 28, 2006. Received 118 public submissions for revisions to draft.
- Created DVS Testing and Certification Task Group to develop objective, scientific, and measurable testing protocols.
- Digital Imaging Guide for Safe Schools presentation at Office of Juvenile Justice Delinquency Prevention Safe Schools Workshop in Elk Grove, IL (November 2006).
- Hosted an Executive Committee at the 2006 IACP Annual Conference in Boston, MA (October 2006).

Additional Activities (pending)

- DVS Executive Committee and Advisory Panel Meeting scheduled for January 17-18, 2007 at the National Transportation Safety Board Training Center in Ashburn, VA.
- DVS Testing and Certification Task Group tentatively scheduled for February 26-28, 2007 in Indianapolis, IN to assist in development of scenes for proposed NIST prototype video quality measurement device.
- DVS informational workshop is planned for the 2007 IACP's Law Enforcement Information Management Conference in Greensboro, NC in May, 2007.
- DVS informational workshop is planned for the 2007 IACP's Annual Conference in New Orleans, LA in October, 2007.

Project Publications Distribution Status

- *Electro-Muscular Disruption Technology: A Nine-Step Strategy for Effective Deployment*
  - In 2nd reprint of Executive Brief (500 copies)
  - Electronic distribution (July 1, 2006 to Dec 31, 2006): 1715 copies
  - Hard copy distribution (July 1, 2006 to Dec 31, 2006): 483 copies
  - Total distribution (July 1, 2006 to Dec 31, 2006): **2198 copies**

- *Digital Imaging for Safe Schools: A Public Safety Response to Critical Incidents*
  - Electronic distribution (July 1, 2006 to Dec 31, 2006): 2293 copies
  - Hard copy distribution (July 1, 2006 to Dec 31, 2006): 424 copies
  - Total distribution (July 1, 2006 to Dec 31, 2006): **2717 copies**

  - Requests for Digital Imaging Technical Assistance: **11** agencies

    - Amity Township, PA Police Department
    - West Bridgewater, MA Police Department
    - Baltimore County, MD Public Schools
    - Sumpter Township, MI Police Department
    - Southern University, LA Police Department
    - Tinley Park, IL Police Department
    - Environmental Protection Agency, CID
    - Oregon Department of Corrections
    - Delaware City, OH Police Department
    - Farmington, ME Police Department
    - Marshall County, AL Emergency Management Agency

- *Digital Video Systems for Public Safety: Minimum Performance Specifications Draft*
  - Electronic distribution (July 1, 2006 to Dec 31, 2006): 2566 copies
  - Total distribution (July 1, 2006 to Dec 31, 2006): **2566 copies**

IACP Conference and Committee Presentations

- DVS informational workshop presented at Government Video Expo in Washington, DC (December 2006).
- Attended 2006 first annual International Law Enforcement Information Management Conference in Vancouver, Canada (November 2006).
- A DVS status update was presented to the IACP's Executive Board at the 2006 IACP Annual Conference in Boston, MA (October 2006).
- A DVS status update was presented to the IACP's Communications and Technology Committee meeting at the 2006 IACP Annual Conference in Boston, MA (October 2006).
- Two DVS informational workshops were presented at the 2006 IACP Annual Conference in Boston, MA (October 2006).

III. Corrective Action to Solve Implementation Problems

There are no current corrective actions required on this project.

IV. Potential Changes in Implementation Plan Specified in Grant Application

None at this time.

V. What Technical Assistance Grant Agency Might Provide

Dependant on Technical Assistance requests.

Grant Project Progress Report
Short Title: The Cutting Edge of Technology
Project Manager: Albert Arena
Date of Report: June 30, 2007

Project Summary

The Cutting Edge of Technology: Enhancing Local and State Law Enforcement's Understanding and Use of Emerging Technologies, is a multi-task and multi-year project to strengthen the ongoing collaboration between the IACP and NIJ on emerging technology issues. The ultimate goal of this project is to help law enforcement agencies better understand and utilize emerging technology.

Major objective of this project:

- The development of minimum performance specifications for digital in-car video systems
- A report on findings from the Police Pursuit Database

The current award period for Cooperative Agreement 2005-DE-BX-K001is effective from September 1, 2006 through August 31, 2007.

I. Current Grant Goals for Project

The development of minimum performance specifications for digital in-car video systems: Creation of minimum performance specifications will provide a safe and reliable context within which police agencies can identify, select, and purchase highly reliable digital in-car video systems.

The publication of a report on findings from the Police Pursuit Database: A report on findings will enable law enforcement practitioners to validate database content as reliable and representative of actual incidents captured by departments regardless of size and jurisdiction.

II. Grant Goals Status for this Reporting Period

The development of minimum performance specifications for digital in-car video systems

Accomplishments:

- Meeting of Advisory Panel held at the National Transportation and Safety Board Training Center in Ashburn, Virginia January 17-18, 2007
- DVS Testing and Certification Task Group met in Indianapolis, Indiana March 7-9, 2007 to assist in development of scenes for proposed NIST prototype video quality measurement device

- Met with members of the Testing & Certification Committee in Burtonsville, Maryland to develop protocols and finalize specifications for the objective measures used by the test instrument
- Revised draft performance specifications based on objective measurements and testing protocols

The publication of a report on findings from the Police Pursuit Database

Accomplishments:

- Contracted with George Mason University Administration of Justice Center to analyze the data and develop a PowerPoint presentation to support the findings.

Additional Activities (pending)

- Presentation at NIJ Technology Conference on status of database
- Transfer of database ownership to Login, Inc
- Issue final report to NIJ in August 2007

Project Publications Distribution Status

- *Electro-Muscular Disruption Technology: A Nine-Step Strategy for Effective Deployment*
    - In 3rd reprint of Executive Brief (500 copies)
    - Electronic distribution (January 1 to June 30, 2007): 2100 copies
    - Total electronic distribution (January 1 to June 30, 2007): 2100 **copies**

- *Digital Imaging for Safe Schools: A Public Safety Response to Critical Incidents*
    - Electronic distribution (January 1 to June 30, 2007): 2400 copies
    - Total distribution (January 1 to June 30, 2007): **2400 copies**

- *Digital Video Systems for Public Safety: Minimum Performance Specifications Draft*
    - Electronic distribution (January 1 to June 30, 2007): 2700 copies
    - Total distribution (January 1 to June 30, 2007): **2700 copies**

Conference and Committee Presentations

- Digital Video Systems presentation at the LEIM Conference in Greensboro, North Carolina May 2007
- Digital Imaging presentation for School Safety Project March 12, 2007
- Digital Video Systems presentation at NIJ Applied Technology Conference, April 2007

III. Corrective Action to Solve Implementation Problems

In the final stages of hiring a new Coordinator to support project goals and initiatives.

IV. Potential Changes in Implementation Plan Specified in Grant Application

None at this time.

V. What Technical Assistance Grant Agency Might Provide

Dependant on Technical Assistance requests.

Grant Project Progress Report (7863)
Short Title: The Cutting Edge of Technology
Project Manager: Albert Arena
Date of Report: December 31, 2007

Project Summary

The Cutting Edge of Technology: Enhancing Local and State Law Enforcement's Understanding and Use of Emerging Technologies, is a multi-task and multi-year project to strengthen the ongoing collaboration between the IACP and NIJ on emerging technology issues. The ultimate goal of this project is to help law enforcement agencies better understand and utilize emerging technology.

Major objectives of this project:

- The development of minimum performance specifications for digital in-car video systems
- A report on findings from the Police Pursuit Database

The current award period for Cooperative Agreement 2005-DE-BX-K001 is effective from September 1, 2006 through November 30, 2007.

I. Current Grant Goals for Project

The development of minimum performance specifications for digital in-car video systems: Creation of minimum performance specifications will provide a safe and reliable context within which police agencies can identify, select, and purchase highly reliable digital in-car video systems.

The publication of a report on findings from the Police Pursuit Database: A report on findings will enable law enforcement practitioners to validate database content as reliable and representative of actual incidents captured by departments regardless of size and jurisdiction.

II. Grant Goals Status for this Reporting Period

The development of minimum performance specifications for digital in-car video systems

Accomplishments:

- Revised draft performance specifications (version 12.7) based on objective measurements and testing protocols
- Developed a draft police chief's companion guide for the selection, acquisition, maintenance, and evaluation of digital in-car video systems
- Identified a list of objective measurements for use in testing the quality and accuracy of digital in-car video systems

The publication of a report on findings from the Police Pursuit Database

Accomplishments:

- Finalized Police Pursuit Database transfer contract between IACP and Login Inc.
- PowerPoint presentation with George Mason University on preliminary findings from the Police Pursuit Database

Project Publications Distribution Status

- *Electro-Muscular Disruption Technology: A Nine-Step Strategy for Effective Deployment*
  - Electronic distribution (July 1 to September 30, 2007): **1151 copies**
  - Total electronic distribution (July 1 to September 30, 2007): **1151 copies**
- *Digital Imaging for Safe Schools: A Public Safety Response to Critical Incidents*
  - Electronic distribution (July 1 to September 30, 2007): **757 copies**
  - Total distribution (July 1 to September 30, 2007): **757 copies**
- *Digital Video Systems for Public Safety: Minimum Performance Specifications Draft*
  - Electronic distribution (July 1 to September 30, 2007): **533 copies**
  - Total distribution (July 1 to September 30, 2007): **533 copies**

Conference and Committee Presentations

- 'Law Enforcement Expo' – Cleveland, OH (July)
- DVS/In-Car Camera Presentation – Rome, NY (August)
- OJJDP Safe Schools Digital Imaging Presentation – Washington, DC (August)
- 'CopsWest' – Ontario, CA (October)
- Canadian Chiefs of Police Infomatics Committee Meeting – St. Johns, Newfoundland (October)
- Sensors and Surveillance Technical Working Group Meeting – Orlando, FL (October)
- Attended & Exhibited at NIJ Critical Incident Conference – San Francisco, CA (November)
- NIJ Aviation Technology Working Group – Annapolis, MD (November)
- IACP Intelligence Sharing Summit – Washington, DC (November)
- IACP LEIM International Conference – Nassau, The Bahamas (November)

II. Corrective Action to Solve Implementation Problems

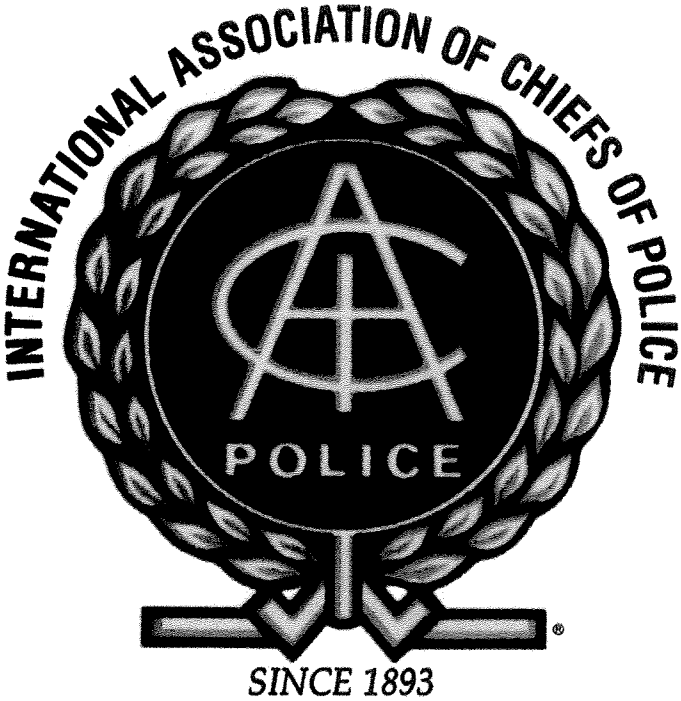
Hired a new Project Coordinator.

III. Potential Changes in Implementation Plan Specified in Grant Application

None at this time.

IV. What Technical Assistance Grant Agency Might Provide

Dependant on Technical Assistance requests.



PROJECT DELIVERABLES

International Association of Chiefs of Police

Digital Video Systems Minimum Performance Specifications Document

Version 12.5 Dated May 4, 2007

In-Car Video Camera Systems

Performance Specifications:

Digital Video Systems Module

DRAFT

FOREWORD

Over a period of 18 months, a panel of law enforcement representatives, scientists, and equipment manufacturers worked together in an unprecedented effort to develop a set of minimum performance benchmarks for digital in-car video systems. This open letter to all the participants in this project is to thank you – and commend you – for the spirit of cooperation, collegiality, and dedication to common goals that made this a true collaboration.

We all recognized the value of video technology for enhancing officer safety, fighting crime, and strengthening public support of the police.

Now it is up to all of us – equipment manufacturers, scientists, and police officers – to carry the message of this document forward to our customers and colleagues. It is our collective responsibility to make sure the technology in use by law enforcement is capable of providing high quality evidence to protect both the public and the police.

Industry representatives should use this opportunity to forge new relationships with each other. Use your renewed commitment to high quality video technology to identify to your customers the products that will best support police officers and the citizens they serve.

Law enforcement officials must use the power of peer-to-peer communication to inform colleagues of the critical importance of the quality of the images. In recent years, numerous court cases have depended on video from mobile recorders to help defend officers against charges of misconduct or, sadly, to speak for officers who are unable to speak for themselves.

The scientific community must help us find objective methods of measuring image quality, push the boundaries of current technology, and identify emerging technologies. Sharing this knowledge will benefit all stakeholders.

We want to sincerely thank all who have participated in this project, but remind you that the work is not yet complete. Some formidable challenges still lie ahead, and we will continue to count on your dedicated support of the goals of this project as we enter the next phase.

Chief Mike Burridge, Farmington, NM Police Department
Steve Lisiewicz, Motorola, Inc.
"Digital Video Standards for Public Safety" Advisory Panel Co-Chairs

ACKNOWLEDGEMENTS

The International Association of Chiefs of Police wishes to express its appreciation to the following individuals that have contributed to the publication of this document.

Chief Joseph C. Carter
President
International Association of Chiefs of Police
Chief Mary Ann Viverette
Immediate Past President
International Association of Chiefs of Police
Daniel N. Rosenblatt
Executive Director
International Association of Chiefs of Police
James McMahon
Deputy Executive Director
International Association of Chiefs of Police
John Firman
Research Center Director
International Association of Chiefs of Police

David W. Hagy
Director
National Institute of Justice

John Morgan
Deputy Director for Science & Technology
National Institute of Justice

Chris Miles
Senior Program Manager
Office of Science & Technology
National Institute of Justice

Patricia Wolfhope
Technical Program Analyst
National Institute of Justice

The IACP Research Center Directorate
Digital Video Systems Project Staff

Albert Arena
Project Manager
Cutting Edge of Technology

William Albright
Project Coordinator
Cutting Edge of Technology

Michael Fergus
Project Manager
Regional Forensic Video Laboratories

Digital Video Standards for Public Safety: Developing Minimum Performance Specifications" Advisory Panel Executive Committee Members

Co-Chairs

Deputy Superintendent Mark Seifert
Delaware State Police

Michael Burridge
L-3 Communications, Display Systems

Task Group Chairs

Lieutenant James D. Wells, Jr.
Florida Highway Patrol
Officer Safety Task Group

Greg Dertz
Motorola Inc.
Chair, Data Security Task Group

D. Miles Brissette
Tarrant County, TX Criminal District Attorney's Office
Testing and Certification Task Group

Sergeant Scott Galbreath
Delaware State Police
Operational Measurements Task Group

Members of the "Digital Video Standards for Public Safety: Developing Minimum Performance Specifications" Advisory Panel
(See Appendix G for full listing)

Past Contributors

Wm. Grady Baker, IACP
Kristy Fowler, IACP
Melissa Hays, IACP
Darron Mason, IACP
Victoria Kallini, IACP
Tiffany Williams, IACP

Steve Lisiewicz, Motorola
Bill Salveson, Panasonic
Mike Siemens, Shiftwatch

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Section 1 – General Information

1.1 SCOPE

This specifications document is limited in scope to digital in-car video systems used by law enforcement agencies.

1.2 PURPOSE

The purpose of this document 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. To achieve this mission, the performance of digital systems must be objectively measured and the level of performance necessary and appropriate to meet the needs of law enforcement must be identified.
These standards apply to any mobile digital video equipment delivered to a law enforcement agency 18 months from the date of publication of the minimum performance specifications and must meet the minimum performance standards and show proof of certification and compliance, as determined by the International Association of Chiefs of Police (IACP).

1.3 DEFINITIONS

"Recommended, Should, May;" state preferred practices that agencies "may" deviate from.
"Will, Shall, Must;" "will" denote mandatory key safety items that are crucial for officer safety and "shall" not be deviated from.

1.3.1 Absolute Time Code: 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. In some machines it is even used to synchronize the tape to other equipment. ATC is very accurate and usually conforms to the IEC standard, which is easily converted to the more commonly used SMPTE time code. Unlike SMPTE, ATC always begins at zero at the beginning of a digital tape. Some DAT machines have the ability to function without ATC on a tape while others simply will not play a tape without it. Almost all current machines record it automatically so it should always be on every tape.

1.3.2 Acceptance test: This refers to any procedure used when a new product is received, or a product is returned from maintenance, to verify that a product or software is performing according to the manufacturer's specifications for a specific use. Common examples include but are not limited to: the use of diagnostic software to test a new computer before it is used to process evidence, and the processing of a set of know standards to verify that the known standards can be processed within an acceptable range of results.

1.3.3 Accuracy: 1) This can refer to the overall range of values within which the actual value obtained is considered to be within tolerance or acceptable. For example in the early days of color printing, machine prints (amateur quality you get from the 1-hour mini lab today) were considered to be acceptable if the color balance was within ±30CCs of the ideal color balance. However, for custom (professional lab) printing the acceptable range of variation was ±5CCs of the ideal color balance. 2) This can refer to how close the actual value obtained is to the range of acceptable values. For example, is the color balance close enough to the optimal color balance so that it can be considered a fair and accurate photographic reproduction. 3) This can refer to the margin of error in measuring something.

1.3.4 Active Storage: A storage location or device (i.e. Server), which videos are transferred to 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.

1.3.5 Administrative Review: A procedure used to check for consistency with agency/laboratory policy and for editorial practice.

1.3.6 Amperage: A measurement of electrical current.

1.3.7 Archival Image: Any image placed on media that is suitable for long-term storage.

1.3.8 Archival Storage: A storage location or device which videos are moved to after a designated amount of time. Access to videos contained within 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.

1.3.9 Archive: Off-line storage of video/audio intended for long-term storage and retrieval.

1.3.10 Archive Copy: A copy of data placed on media suitable for long-term storage and retrieval.

1.3.11 Archive Image: 1) Any image placed on media that is suitable for long-term storage. 2) A bit stream duplicate of the original data placed on media that is suitable for long-term storage and retrieval.

1.3.12 Archiving: Long-term storage of data.

1.3.13 Authentication: 1) 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. 2) A means of identifying individuals and verifying their eligibility to receive specific categories of information. 3) Evidence by proper signature or seal that a document is genuine and official. 4) In evasion and recovery operations, the process whereby the identity of an evader is confirmed. 5) 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). 6) 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.

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

1.3.15 Bundled: Accessories or software that is included in the purchase of the main item such as a computer or a major software application.

1.3.16 Capture: The process of recording data, such as an image, video sequence, or audio stream.

1.3.17 Capture Device: A device used to record audio, photographic, graphic, or video data.

1.3.18 CD/DVD (compact disc/digital versatile disc): Optical disc formats designed to function as digital storage media.

1.3.19 Chamfer: To cut off the edge or corner of, bevel.

1.3.20 Chain Of Custody: The chronological documentation of the movement, location and possession of evidence.

1.3.21 Consistency: The degree of uniformity, standardization, and freedom from contradiction among the Video/Data or parts of a system or component

1.3.22 Copy: An accurate reproduction of information.

1.3.23 Corruption: A process wherein data in memory or on disk is unintentionally changed, with its meaning thereby altered or obliterated.

1.3.24 DAT: Digital Audio Tape.

1.3.25 Data Capture: The collection of information at the time of a transaction.

1.3.26 Data Extraction: The identification and recovery of information contained within a recording, which may not be immediately apparent through visual/aural inspection.

1.3.27 Data File: A file consisting of data in the form of text, numbers, or graphics, as compared to a program file of commands and instructions.

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

1.3.29 Date stamping: A software feature that automatically inserts the current date into a document.

1.3.30 Digital Evidence: Information of probative value that is stored or transmitted in binary form.

1.3.31 Digital Asset: Recorded video, audio, and associated metadata.

1.3.32 Digital Image: A photographic image that is represented by discrete numerical values organized in a two-dimensional array. Each discrete block is called a pixel.

1.3.33 Digital Recording: The storage of information in a binary-encoded (digital) format. Digital recording converts information—text, graphics, sound, or pictures—to strings of 1s and 0s that can be physically represented on a storage medium.

1.3.34 Download: The process of receiving data from another digital source.

1.3.35 Duplicate: An acceptably accurate and complete reproduction of all data objects independent of the physical media.

1.3.36 Encryption: 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.

1.3.37 Export: To move information from one system or program to another. Files that consist only of text can be exported in ASCII (plain text format). For files with graphics, however, the receiving system or program must offer some support for the exported file's format.

1.3.38 Format Conversion: To transfer audio and/or video information from one media type to another and/or from one recording method to another.

1.3.39 Hash: A mathematical formula that generates a numerical identifier based on input data. If any bit of the input data used to calculate the numerical identifier changes, the output number changes.

1.3.40 Image: 1) A bit stream duplicate of the original data. 2) An imitation or representation of a person or thing, drawn, painted, or photographed.

1.3.41 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).

1.3.42 Image Capture: The transducing of the information in a real image into the photographic or electronic medium. Normally in motion-reproducing systems, synchronous audio information is simultaneously transduced.

1.3.43 Image Transmission: The act of moving images from one location to another.

1.3.44 Import: To bring information from one system or program into another. The system or program receiving the data must somehow support the internal format or structure of the data.

1.3.45 Integrity: 1) The completeness of the potential evidence throughout its lifecycle. 2) The degree to which a system or component prevents unauthorized access to, or modification of, digital Video and or data associated with such video. 3) The

steadfast adherence to a strict moral or ethical code set by guidelines in the policy and procedures process of handling in car video.

1.3.46 Intermediate Storage: Any media or device on which data is temporarily stored for transfer to permanent or archival storage.

1.3.47 Locked file: A file on which one or more of the usual types of manipulative operation cannot be performed—typically, one that cannot be altered by additions or deletions.

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

1.3.49 Logical Copy: An accurate reproduction of information contained within a logical volume.

1.3.50 Mass Storage: Any device for the storage of large amounts of data.

1.3.51 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.

1.3.52 Multimedia Evidence: Analog or digital media, including, but not limited to, film, tape, magnetic and optical media, and/or the information contained therein.

1.3.53 Native File Format: The original form of a file. This usually refers to a file format that is associated with and unique to a specific software application program.

1.3.54 Network Topology: Graphical representation of a network.

1.3.55 Physical Copy: An accurate reproduction of information contained on the physical device.

1.3.56 Physical Image: A bitstream duplicate of data contained on a physical device.

1.3.57 Pinch Points: Points at which it is possible to be caught between moving parts, or between moving and stationary parts of a piece of equipment.

1.3.58 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

1.3.59 Primary Image: Refers to the first instance in which an image is recorded onto any media that is a separate, identifiable object. Examples include a digital image recorded on a flash card or a digital image downloaded from the Internet.

1.3.60 Processed Image: Any image that has undergone enhancement, restoration or other operation.

1.3.61 Proxy: A Type 2 duplicate of a Primary Image.

1.3.62 Recorded Evidence Reference Lifecycle: The stages or states in which a recording will exist from the time it is created until it is destroyed.

1.3.63 Reference Lifecycle: The stages or states that are applicable to the recommendations in this document.

1.3.64 Reliability: The extent to which information can be depended upon.

1.3.65 Removable Media: Storage media that can be removed from the camera and/or computer.

1.3.66 Storage Media: Any object on which data is preserved.

1.3.67 Transcoding: (FV) This refers to converting a data stream from one format to another, such as MPEG-1 to H.263, or an H.320 video conferencing session to H.323.

1.3.68 Type 1 Digital Asset: A duplicate recording that has been created that passes the applicable Integrity, Consistency, and Authenticity checks. The record contains all chain of custody evidence and support.

1.3.69 Type 2 Digital Asset: A duplicate recording has been created that does not contain the chain of custody evidence and support.

1.3.70 Validation: The process of performing a set of experiments, which establishes the efficacy and reliability of a tool, technique or procedure or modification. This is a requirement for any custom application software before it can be used for forensic applications. This is also recommended for commercial applications. In the forensic setting, this usually involves the processing of what the user considers to be a representative sample of the type or types of evidence to be processed.

1.3.71 Validation Testing: An evaluation to determine if a tool, technique or procedure functions correctly as intended for a specific application using a representative sample.

1.3.72 Validity check: The process of analyzing data to determine whether it conforms to predetermined completeness and consistency parameters.

1.3.73 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.

1.3.74 Verification: 1) A scientific procedure followed by a second qualified examiner to confirm that the examination performed by the first examiner is scientifically valid. In most forensic laboratory settings this also includes the procedures to be followed in the event that there is a disagreement over the scientific validity of the examination performed by the first examiner. 2) The process of confirming the accuracy of an item as compared to its original.

1.3.75 Video: The electronic representation of a sequence of images, depicting either stationary or moving scenes. It may include audio.

1.3.76 Video Capture: This is the process of converting analog video to digital video.

1.3.77 Video clip: A file that contains a short continuous video recording, usually of one scene.

1.3.78 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.

1.3.79 Write Block/Write Protect: Hardware and/or software methods of preventing modification of media content while the media content is being read. In the forensic examination of evidence these devices perform a critical function by

allowing the examiner to make an image, recover deleted files that have not been overwritten, examine files, and/or copy files without altering any data on the storage media being examined.

1.3.80 Work Copy: A copy or duplicate of a recording or data that can be used for subsequent processing and/or analysis.

1.4 ACRONYMS

ABA	American Bar Association
AFSC	United States Air Force Standard Charts
ANSI	American National Standards Institute
ASR	Aerosol Subject Restraint
ASCLD–LAB	American Society of Crime Lab Directors/Laboratory Accreditation Board
CPSC	Consumer Product Safety Commission
DSS	Digital Spread Spectrum
DVS	Digital Video System
EDD	Electronic Disruption Devices
EIA	Electronics Industry Association
ESSID	Extended Service Set Identification
ETATS	Enforcement Technologies Advisory Technical Subcommittee
FCC	Federal Communications Commission
FMVSS	Federal Motor Vehicle Safety Standards
HF	High Frequency
IACP	International Association of Chiefs of Police
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ISO	International Standards Organization
MDT	Mobile Data Terminal
MDVR	Mobile Digital Video Recorder
MVS	Mobile Video System
NFPA Intl	National Fire Protection Association International
NHTSA	National Highway Transportation Safety Administration
NTSC	National Television System Committee
RC4	Rivest Cipher 4
RFP	Request for Proposal
SAE	Society of Automotive Engineers
SIA	Security Industry Association
SMPTE	Society of Motion Picture and Television Engineers
SSID	Service Set Identification

SSL	Secure Sockets Layer
UHF	Ultra High Frequency
UL	Underwriters Laboratories
UL of Canada	Underwriters Laboratories of Canada
VHF	Very High Frequency
VVCS	Vehicle Video Capture System
WMV	Windows Media Format
WORM	Write Once, Read Many

1.5 UNITS OF MEASURE

Reference the standards to which the measurements apply. In all other cases, Society of Automotive Engineers (SAE) measurement standards will be used.

Section 2 - Applicable Standards

2.1 All mobile video systems and related audio equipment must conform to the applicable minimum standards as set by the:

a) Electronic Industries Association (EIA)
b) Federal Communications Commission rules and regulations (FCC)
c) Institute of Electrical and Electronic Engineers (IEEE)
d) International Electrotechnical Commission (IEC)
e) International Organization for Standardization (ISO)
f) National Fire Protection International (NFPA)
g) National Highway Transportation Safety Administration (NHTSA)
h) Society of Automotive Engineers (SAE)
i) Underwriters Laboratories Inc. (UL)
j) Underwriters Laboratories of Canada (Canada UL)

2.2 Vendors must be able to provide a White Paper that establishes that it adheres to the minimum specifications of this document, and that the technology used is generally accepted in the relevant field.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 3 - Officer/Occupant Safety

3.1 Items installed or located in the passenger compartment of the vehicle

3.1.1 No item installed in the interior of the passenger compartment shall increase the risk of injury to occupants during events related to a vehicle crash as defined below.
Not Verifiable

3.1.1.1 Items installed or located in the interior of the vehicle shall remain in place during a reasonably foreseeable crash. This will be determined by a static pull test. The force applied to the item will correspond to *50* times its own weight (*50*g). This force must be maintained for at least one (1) full second. The test shall be conducted from a minimum of three (3) different angles to simulate frontal, side and rear collision directions. The item must remain attached to its mounting points during this test. The item will be allowed to move or pivot on any adjustable mounts or joints as long as it does not move into a location that could increase the likelihood of impact with an occupant or into a hazardous area such as an airbag deployment zone.

3.1.1.2 Any items installed in the interior of the vehicle shall meet the requirements stated in Federal Motor Vehicle Safety Standard 201 [October 1, 2002] *Occupant Protection in Interior Impact* (see Appendix A).

3.1.1.3 Exposed exterior surfaces, corners, fasteners, and controls that could be contacted by an occupant during a collision shall be of a design that minimizes the potential for injury. Edges and corners shall have a minimum 1/8-inch (3.2mm) radius or chamfer or be padded with an energy absorbing material to minimize the risk of injury.

3.1.1.4 Note: This correlates to Federal Motor Vehicle Safety Standard 201(S5.4) [October 1, 2002] (See Appendix A).

3.1.1.5 No equipment will be installed in any original vehicle manufacturer's designated air bag deployment zone. Alternatively, this requirement can be met if the airbag corresponding to the air bag deployment zone that is violated is turned off or disabled in accord with National Highway Traffic Safety Administration guidelines and any vehicle occupants are clearly warned with a readily visible placard or illuminated indicator that the airbag has been disabled.

3.1.1.6 Any equipment placed between the front seats should not be higher than the bottom seat cushion for the entire length of the cushion.

3.1.1.7 Manufacturers shall specify brackets, hardware and mounting locations to be used to meet this standard in their installation guide or owner's manual.

3.1.2 All controls and components should be located and designed to minimize driver distraction.

The control pad should be designed and organized to minimize officer workload. The record button should be readily identifiable by size, color, location and/or other design features. The record button should be easily accessible by officers wearing gloves.

3.1.2.1 All controls should be easily activated by a wide range of officers/operators. Reach requirements shall correspond to guidelines set forth by the Society of Automotive Engineers for the placement of automotive controls. The reach range shall correspond to the 10% female through the 90% male sizes.

3.1.2.2 All cameras should default to auto focus. The manufacturer may provide an auto focus override system if desired. The override system should be configurable to prevent operation while the vehicle is in motion.

3.1.2.3 System components shall be capable of being illuminated for ready identification during periods of darkness. Backlit controls are preferred. The illumination level shall be capable of being controlled over a range from bright to dark. The illumination level shall be set by either a discrete control within the unit itself or by linking to the vehicle dash illumination control. The viewing screen light level shall be controlled simultaneous with the controls or independently. The viewing screen shall be capable of being completely dimmed. The operator must have the ability to blackout the system on demand.

3.1.2.4 Only monitoring of information being or capable of being recorded should be displayed on the viewing screen while the vehicle is in motion. Viewing of previously recorded or externally supplied digital asset should not be allowed while the vehicle is in motion.

3.1.3 Installed equipment shall be located to minimize interference with the view of the driver.

3.1.3.1 Installed equipment shall be located to minimize interference with the view of the front seat passenger.

3.1.3.2 No item in the system that is installed in the vehicle, other than the camera shall, extend below the AS-1 line. This line has been determined in Federal Motor Vehicle Safety Standard 205 [October 1, 2002] *Glazing Materials* (ANSI/SAE Z26.1) (See Appendix B) to be the minimum vertical sight line necessary for safe vehicle operation. It can commonly be located on the vehicle at the bottom of the factory-installed tint band at the top of the windshield. At one or both sides of the windshield near the "A-pillar" is a printed designation visible from outside the vehicle marked "AS-1". To ensure safe vehicle operation, equipment located in other locations shall not impair the driver's view to the front, sides or rear of the vehicle. Alternatively, a manufacturer may elect to perform the SAE tests for vertical visibility that determine the AS-1 line if they want to extend below this line at locations rearward of the windshield. The minimum height for eye level above the seat cushion will be as determined for an SAE 90% male model.

3.1.3.3 No part of any equipment in the interior of the passenger compartment will obscure for the 10% female through the 90% male SAE sizes any speedometer, warning lights, gauges, essential controls, or mirrors placed in the vehicle by the original equipment manufacturer. Further, no installed

equipment will interfere with the operation of vehicle controls such as the transmission shifter, headlamp controls, windshield wipers, electric door locks, window defroster controls, etc. See Federal Motor Vehicle Safety Standards 101[October 1, 2002], "Controls and Displays" for a complete list of included devices. (See Appendix C). This does not include controls for convenience items, such as a commercial broadcast radio.

3.1.3.4 Manufacturers shall specify equipment-mounting locations to comply with this specification in their installers guide or owner's manual, or will provide a list of vehicles for which the vendor's systems will meet this specification.

3.1.4 Installed equipment shall be properly fused to minimize shock and fire hazards.

3.1.4.1 All wiring shall meet industry standards applicable to the wire application. For example, wiring and electronic components contained within the system housings such as the camera body, control panel body and monitor meet applicable Underwriters Laboratory (UL) standards for gauge, insulation type, fusing, connectors, heat sinks, etc. Wiring exterior to these components will meet all applicable Society of Automotive Engineers (SAE) standards for gauge, insulation type, fusing, connectors, etc.

3.1.4.2 All systems shall be properly grounded using the same industry standards as above and if necessary, due to the presence of hazardous voltage or amperage levels, shall be equipped with ground fault interrupters to prevent shock and electrocution hazards. Properly grounded equipment will also provide the most reliable service for the user and minimize many sources of Electromagnetic Interference.

3.1.4.3 Manufacturers shall provide information in their installer's guide or owner's manual that specifies the proper wiring, fuses, connectors, connection points with the vehicle electrical system and grounding points.

3.1.5 Elimination of hazardous pinch points.

3.1.5.1 Doors, brackets or any other moving part shall be designed so that fingers or hands cannot be pinched and injured when the parts are moved.

3.2 Items Carried by the Officer

3.2.1 No parts that can come into contact with human skin shall be allowed to reach a temperature capable of causing a burn injury, Reference UL 60950 "Safety of Information Technology Equipment" as amended December 1, 2000. **Items carried on the officer's person or uniform shall not pose an undue risk of injury.**

3.2.2 Any system component carried on the officer's person shall meet all Underwriters Laboratory Standards for shock/electrocution and burn prevention. All batteries used in such devices shall meet Underwriters Laboratory Standards for safety.

3.2.3 The manufacturer shall provide a warning that components and controls shall not be placed on the officer's person so that it prohibits free access to and removal of firearm, baton, Pepper Spray, handcuffs, etc. The following proposed statement should be prominent in the owner's manual:

> "**Placement of items on the duty belt can restrict ready access to important equipment.** The location of the wireless transmitter or any other device provided with this system that is carried on the officer's person should be chosen with care and consideration. After a location is selected, the officer should test access to and practice drawing primary items such as service firearms and secondary defense devices such as Aerosol Subject Restraint, Batons, Electronic Disruption Devices, etc. Proper operation of handheld radios and other signaling devices should also be tested as should access to handcuffs and other restraining devices."

3.2.4 Any body-worn cords or wires shall be of such construction that they minimize the risk of strangulation or cause injury from strangulation, cutting off of blood flow or laceration during assault, slip, fall or other types of incidents or during a vehicle crash.

3.2.5 Any component worn or carried by the officer shall be of smooth construction properly rounded or chamfered to minimize the possibility of injury. The components shall be free of sharp points or edges that could cause injury during a fight, slip, fall or other types of incidents. In addition all clips and retention devices should be designed to minimize the possibility of pinch points that could cause injury.

3.3 Record indicators

3.3.1 A system should have an illuminated record indicator readily visible to persons outside the vehicle to the front and passenger side that indicates when the system is actively recording. This indicator does not need to be visible to occupants inside the vehicle. This record indicator shall comply with 3.1.2.4.

3.3.2 Unmarked patrol vehicles and surveillance vehicles may be exempt from this

requirement depending on local laws and policy requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 4 - General Mobile Video System Specifications

4.1 The mobile video system shall consist of a camera, a recording mechanism, control center, monitor, wireless microphone/transmitter system to capture audio outside of the vehicle for traffic stops, and a hard-wired microphone to capture audio from inside the police vehicle.

4.1.1 Emphasis should be placed on the video system's ability to maintain consistent audio/visual recording quality, while subject to interference from the following sources (See Appendix D for applicable UL Standards Reference):

a) High-powered television stations
b) Other radio frequency interference (including UHF, VHF and HF transmitters.)
c) Automobile alternator, ignition, and electrical systems
d) Automobile heaters / air conditioner fan motors
e) Other patrol vehicle electrical systems to include radios, emergency lights, siren, mobile data computers, and speed measuring devices
f) High voltage power lines, traffic signals, neon signs, etc.

4.1.2 When in operation, the mobile video system must not generate electromagnetic or radiation that interferes with communications or other electronic equipment found within a police vehicle. .

Vehicular System Electrical Conditions

4.2.1 The in-car recording system shall be protected from damage due to input of voltage, reverse polarity, and electrical transients that may be encountered.

4.2.2 The system shall operate on a filtered power source, regulated, and short-circuit-protected. The voltage supplied to the camera shall meet the manufacturer's specification and shall not vary with fluctuations of the system's electrical system voltage of between 9 and 18 volts.

4.2.3 Loss of power to the system shall not result in the unit requiring reprogramming. Sudden loss of power shall not cause loss of any recorded data.

Vehicular Recording System

4.3.1 The Vehicular Recording System shall operate within the range of temperatures from 0 to 120 degrees Fahrenheit and/or between –18 to 49 degrees Celsius.

4.3.2 The Vehicular Recording System shall be equipped with auto focus, automatic exposure, and automatic white balance.

4.3.3 The Vehicular Recording System shall have a backlight compensation setting.

The Vehicular Recording System's imaging sensor shall be of solid state design and shall not be subject to burn in.

4.3.4 The Vehicular Recording System shall have a minimum color resolution of 450 horizontal lines.

4.3.5 The Vehicular Recording System's Forward Facing Camera shall be capable of being rotated 180 degrees on a horizontal plane in either direction on its mount

without having to loosen any screws or knobs.

4.3.6 *The* The Vehicular Recording System Forward Facing Camera shall provide a minimum field of view of 24 feet width at distance of 35 feet (40 degrees) with all optional zoom settings at the full wide angle view.

4.3.7 The Vehicular Recording System should provide both automatic and manual focus capabilities, which are user selectable.

4.3.8 The camera shall offer a signal-to-noise ratio of at least 46db.

4.3.9 The Vehicular Recording System's monitor shall be a minimum of 3 inches (diagonally measured) and able to display color.

4.3.10 The Vehicular Recording System monitor shall be capable of displaying a live picture from the system camera(s) when the system is on (even if recording is not in progress).

4.3.11 The Vehicular Recording System shall include a speaker to provide monitoring of live audio from the wireless microphone as well as recorded sounds while in playback mode. The system shall contain a readily accessible control(s) to adjust the volume and enable and disable monitoring of live audio.

4.3.12 The Vehicular Recording System shall operate independently of the monitor.

4.3.13 The Vehicular Recording System should have the capability to display: date/time, user identification information, emergency light indication, siren indication, braking indicator and microphone activation indicator. These items shall not be embedded in the video stored on the recorder.

4.3.14 The Video Recording System shall be capable of recording audio from a wireless microphone at a range of 1000 feet, line of sight, under ideal conditions.

4.3.15 The Video Recording System wireless microphone shall contain an internal antenna.

4.3.16 The Vehicle Recording System's Operator shall have the ability to deactivate audio from the wireless microphone , without stopping or disabling the recording of video.

4.3.17 The Vehicle Recording wireless microphone shall be able to activate audio and video recording.

4.3.18 The Vehicle Recording wireless microphone shall contain a redundant microphone built into the device worn by the user.

4.3.19 The Vehicle Recording wireless microphone shall use FCC approved frequency bands.

4.3.20 Digital transmission to ensure clarity of audio without distortion throughout the range of the transmitter (Use of spread spectrum technology is recommended). .

4.3.21 The Vehicle Recording wireless microphone shall be able to be synchronized to receiver in the vehicle without manual adjustment by the user.

4.3.22 The Vehicle Recording Wireless microphone shall contain a rechargeable battery with a minimum talk time of 3.5 hours before needing recharging.

4.3.23 The Vehicle Recording Wireless microphone should be able to be placed into active or talk mode for a minimum of 15 hours without needing to be recharged .

4.3.24 The Vehicular Recording System shall provide the following controls

a) Power on/off
b) Play
c) Record start/stop
d) Fast Forward
e) Rewind
f) Stop
g) Pause
h) Zoom in/out
i) Auto Focus on/off
j) Backlight Compensation

4.3.25 The Vehicular Recording System shall provide the following Indicators:

a) System Power on
b) Microphone on
c) Media inserted and operational with remaining capacity/time available
d) Recording
e) Fast Forward
f) Stop
g) Time Counter
h) Diagnostic Indicator

4.3.26 The Vehicle Recorder System's recording functions shall be activated by any of the following methods

a) User pushes record button.
a) Activation of the emergency lights and/or sirens.
b) User activates the record button on the wireless microphone transmitter.

Section 5 - Security Features

5.1 The in-car recording system shall have the capability to restrict access to the programming functions, including but not limited to time/date features.

5.2 The recording device shall not allow the user to erasing or record over previously recorded information from either inside the vehicle or at the recording device controls.

5.3 Vehicle Recording System Integrity

5.3.1 Integrity of vehicle recording systems refers to the validity of the digital asset captured by the system, in which the system limits the potential for errors.

5.3.1.1 The Active and Archival Storage systems shall be capable of backing-up the digital assets.

5.3.1.2 The Active and Archival Storage systems should utilize fault tolerant storage or similar technology.

5.3.1.3 User interfaces should prevent the input of invalid data.

5.4 Consistency

5.4.1 Time Consistency

5.4.1.1 Time stamping in whatever format offered or selected, shall be consistent within all system components.

5.4.1.2 The Vehicle's recorder clocks should be capable of being synchronized with the Active and Archival Storage System within 0.5 seconds, when the vehicle recorders have electronic connectivity to the storage systems

5.4.1.3 Metadata, including time stamping, shall remain accurate with respect to the recording as it was captured, despite any time sync irregularities in a secondary unit, archival system, or viewer.

5.4.1.4 Time-stamping between the components of the digital asset shall be consistent and maintained.

5.4.1.5 Each component in the system maintaining an independent clock shall contain a mechanism to backup the clock for a minimum of fourteen days in the case of primary power failure to the component.

5.4.2 Digital Asset Consistency

The Vehicle Recording, Active Storage, and Archival Storage systems shall be able to recognize, move, and verify all data exchanged.

5.4.2.1 The Vehicle Recording System shall compute a Hash function, or some other method, to verify all digital assets

5.4.2.2

5.4.2.3 All components in the Active and Archival Storage Systems shall perform a verification of the digital asset.

5.4.2.4 Authenticity

5.4.2.5 The Vehicle Recording System shall identify the vehicle in which the recorder is mounted.

5.4.2.6 Removable Media shall, at a minimum, indicate either the badge number(s) of the officer(s) assigned to the media or the vehicle ID.

5.5.1 Non-Removable Media shall, at a minimum, indicate the badge number(s) of the officer(s) assigned to the vehicle or the vehicle ID. This shall be individually associated with each digital asset.

5.5.2

5.5.3 The Vehicle Recording System shall provide a mechanism to capture the time and date of the recording. The time and date of the recording shall become part of the Chain of Custody Audit Log associated with Type 1 and Type 2 recordings.

5.5.4 All Type 1 digital asset Vehicle Recorder Systems using electronic transfer of the recorded material shall have an automated verification mechanism. Digital asset verification information consisting of a minimum 32 hexadecimal hash value shall be attached to the digital asset sequence when first transferred. The automated verification mechanism shall not introduce any visible or audible artifacts into the digital asset.

5.5.5 All metadata shall be attached to the Type I digital assets prior to the electronic transfer

5.6 Transfer of Digital Assets

The Archive and Active Storage systems shall provide a chain of evidence report detailing all Digital Assets activity listed below.

5.6.1 Physical Digital Asset Transfer Using Removable Media:

5.6.1.1 An Integrity check shall be used to validate that the digital asset on the Active Storage is an exact duplicate to any data on the removable storage media prior to the clearing of data on the removable storage media.

5.6.1.2 The Chain of Custody Audit Log for Type 1 digital asset included on the Active Storage System shall contain the following items when the digital asset on a removable media device (e.g., Spinning Optical, Flash, Digital Tape, or Removable Magnetic) is transferred to Active Storage:

a) Name or ID (badge number or employee number) of officer or person submitting digital asset for transfer;
b) Active Storage retention period for digital asset;
c) Integrity check performed to validate that the digital asset transferred to the active storage is an exact duplicate prior to any clearing of data on the removable storage media.

5.6.2. Wireless Data Transfer:

5.6.2.1. An Integrity check shall be used to validate that the digital asset on the Active Storage is an exact duplicate to any data on the recorder prior to the information being deleted from the recorder.

5.6.2.2 Wireless Transfer Network Topology:

5.6.2.2.1 A wireless network used to transfer the digital asset from the recorder to Active Storage shall, at a minimum, use 128-bit encryption to create a secure connection for the digital assets to be transferred. Manufacturers, at their customers' discretion, may provide other security technologies that surpass 128-bit encryption. See Section 8.9.3 for more information on additional forms of digital asset protection.

5.6.2.2.2 IEEE standards based wireless networking equipment shall use the following security guidelines:

a) Customized network name;
b) Disabled SSID/ESSID (Network Name) broadcast; and
c) 128-bit RC4 link encryption.

Additional security standards which exceed those set by the standards listed above may be applied to the wireless link as defined by the customer or manufacturer.

5.6.2.2.3 If a non-IEEE standards based wireless networking equipment is used, it should be configured to at least meet the equivalent minimums defined in 5.6.2.2.1 and 5.6.2.2.2.

5.6.2.2.4 Chain of Custody Audit Trail Items on the Active Storage

The Chain of Custody Audit Log for Type 1 digital assets included on the Active Storage System shall contain the following items when wireless (automated) digital asset transfer from the recorder to Active Storage is used:

a) Successful wireless connection with recorder made;
b) Time/date of transfer;
c) Active Storage retention period for digital asset;
d) Integrity check performed to validate that the digital asset transferred to the server is an exact duplicate prior to any clearing of data on the recorder storage medium.

5.6.3. Wired Data Transfer:

5.6.3.1 An Integrity check shall be used to validate that the digital asset on the Active Storage is an exact duplicate to any digital asset on the recorder prior the information being deleted from the recorder.

5.6.3.2 Wired transfer network topology:

5.6.3.2.1 A private network (i.e., separate from any other networks) used to transfer the digital assets from the recorder to Active Storage shall be considered secure since it is limited in its scope and is restricted from being accessed by any device except for the recorder and the Active Storage server.

5.6.3.2.2 A public network (i.e., where the data must cross over another non-private network) used to transfer the digital asset from the recorder to Active Storage or between Active Storage and Archival Storage shall, at a minimum, use 128-bit encryption to create a secure connection for the digital assets to be transferred. Manufacturers, at their customers' discretion, may provide

other security technologies that surpass 128-bit encryption. See Section 8.9.3 for more information on additional forms of digital asset protection.

5.6.3.3 Chain of Custody Audit Trail Items on the Active Storage

The Chain of Custody Audit Log for Type 1 digital assets included on the Active Storage System shall contain the following items when wired (automated) digital asset transfer from the recorder to Active Storage is used:

a) Successful wired connection with recorder made;
b) Time/date of transfer;
c)
d) Active Storage retention period for digital assets;
e) Integrity check performed to validate that the digital assets copied to the server is an exact duplicate prior to any clearing of data on the removable storage medium.

5.6.4 Transfer from Active Storage to Archival Storage

The Chain of Custody Audit Log for Type 1 digital asset shall contain the following items when the digital asset is transferred form Active Storage to Archival Storage:

a) The user identity initiating the transfer (if the process is not automated);
b) Time/date of transfer;
c) Archival Storage retention period for digital assets. It is anticipated that the Archival Storage retention period will be recomputed and not necessarily related to the previous Active Storage retention period associated with the digital asset;
d) Integrity check performed to validate that the digital asset transferred from Active Storage to Archival Storage is an exact duplicate prior to clearing of Active Storage.

5.6.4.1 Retrieval of Digital Assets from Archival Storage back to Active Storage

The Chain of Custody Audit Log for Type 1 digital assets shall contain the following items when the digital asset is transferred form Archival Storage to Active Storage:

a) The user identity initiating the transfer (if process is not automated);
b) Time/date of transfer;
c) Active Storage retention period for digital assets. It is anticipated that the Active Storage retention period will be recomputed and not necessarily related to the previous Archival Storage retention period associated with the digital asset;
d) Integrity check performed to validate that the digital assets transferred back to Active Storage is an exact duplicate should the digital assets stored in Archival Storage be removed.

5.6.5 The Chain of Custody Audit Log for Type 1 digital assets shall contain the date, time and an identifier that indicates the digital assets removed.

5.7 Vehicle Recorder System Security.

The following items shall be included to protect the vehicle recording system and removable media:

5.7.1 Equipment diagnostics

5.7.1.1 When powered, the recorder shall perform a self-test to insure complete functionality. If the recorder does not pass the self-test, it shall immediately notify the user.

5.7.1.2 The recorder shall be able to monitor itself while in operation. Should a component of the recorder fail while in operation, the recorder shall immediately notify the user.

5.7.1.3 The recorder shall provide the following minimum media diagnostics:

a) Indicate amount of storage space remaining on media; and
b) Send a notification to the user (audible/visual) that storage is reaching its maximum capacity.

5.7.2 Equipment Enclosure

5.7.2.1 The Vehicle Recording System should have the capability to visually indicate to the officer if the system has been tampered with.

5.7.2.2 Recording device shall be physically mounted in the vehicle, following the manufacturer's recommendations, to prevent removal without tools and deter theft of the device.

5.7.3.2 If removable, the recording device shall, at a minimum, be secured using a physical lock that prevents unauthorized removal of recorder from the vehicle. A key is required to unlock the recorder for removal from the vehicle.

a) Keys to the physical lock can include but are not limited to:
   i. A typical key, though one that can not be easily duplicated (cylindrical key, etc.)
   ii. A "credit card" style magnetic strip that can be "swiped" to release the lock.
   iii. An electronic "chip" which will release the lock when placed into proximity of a specific sensor.

5.7.3 Removable Media Security

5.7.3.1 The recording media shall be secured using a locking mechanism that prevents unauthorized removal of the storage media from the recorder.

5.7.3.2 The recording device shall indicate when media is inserted into the recorder

5.7.3.3 A key shall be used to unlock the recording media for removal from the recorder. Examples of the type of keys that may be used to secure the recording media are but not limited to:

a) A physical key, though one that can not be easily duplicated (e.g., cylindrical key);
b) A "credit card" style magnetic strip that can be "swiped" to release the lock;
c) An electronic "chip" which will release the lock when placed into proximity of a specific sensor; or
d) A password that is entered into the recorder.

5.7.3.4 Non-removable recording media shall be housed inside the recorder to prevent tampering with and/or destruction of the media.

5.7.3.5 The manufacturer shall provide guidelines on the media life cycle of the digital asset.

5.7.3.6 Removable media shall contain the following items and markings:

a) Tamper detection process;
b) Damage protection; and
c) The media must be marked on the exterior with an identifying number or markings that identify each media and makes that media unique.

Section 6 – Digital Asset Recording

6.1 The digital assets recorded shall accurately and reliably reproduce the viewed imaged, observed sound and associated metadata as the *Type 1 Digital Asset*.

6.1.1 The in-car system shall be capable of recording events uninterrupted for a minimum of three and a half hours (3.5) hours at a minimum resolution of 640x480 (VGA) and a minimum frame rate of 30 frames per second (fps).

6.1.2 The *1st instance / primary image* shall conform to accepted and known industry standards. (See Appendix D for applicable UL Standards Reference).

6.2 The exchange of the digital assets from the in-car system, active system, and archival storage system can be done in various ways. To that end all systems shall conform to the following:

a) All digital assets known as the *Type 1 Digital Asset* and accompanying audio tracks shall be capable of being rendered to a uncompressed file in industry standard file format. The associated metadata shall be transcoded into a file in standard file format.

b) All digital assets known as the *Type 1 Digital Asset* along with their accompanying audio tracks and associated metadata in an active storage system shall be capable of being rendered to a proxy Microsoft's Windows Media File format (WMV).

6.3 Interim Evaluation Tests

At the time of publication of this document, the National Institute of Standards (NIST) is working on but has not yet finalized a set of standards for testing in-car digital recording systems. .

Items being considered for specification are: Does the image and audio accurately represent what it purports to show?

- Aspect Ratio
- Color fidelity +- 50 nm
- Resolution
  - Static
  - Dymaic (motion)
- Noise
  - Color Shift
  - Motion prediction
  - Edge Noise
  - Others?
- Pincushinioning
- Fidelity
- Motion Artifcts
- Interlaced Artifacts
- Audio
  - Spectiral range
  - Signal to noise or equivalent
  - Total Harmonic Distortion or equivalent

6.7 System/Metadata

6.7.1 All metadata shall be capable of being super-imposed or absent on the screen during playback mode.

6.7.2 Recommended: ability to support enabled or disabled audio capture by system administrator for pre-event and post-event buffered/recorded video, along with backend evidence preparation/export tools for playback in court.

Section 7 - Interoperability

Active or Archival Storage Server

Interoperability of the digital assets shall begin after the transfer of the digital asset from the mobile digital video recording unit located in the field. Access and availability should be granted in order to conduct the sharing of the digital asset at this prescribed data point within the capture, transfer and archival process.

7.2 Types of Interoperable Exchange

7.2.1 Two levels of Interoperable Exchange

There shall be at least two Interoperable Digital Assets obtained from the Active or Archival Storage Server.

7.2.1.1 Type 1 Interoperable Digital Asset

The video, audio, and associated data that meet the criteria as defined by Section 6.2.a shall serve as the evidentiary digital asset.

7.2.1.2 Type 2 Interoperable Digital Asset

The video, audio, and associated data identified as the proxy in Section 6.2.b shall serve as the interoperable digital asset.

7.3 Active Storage and Archival Storage Interoperable Exchange

The Active Storage shall be interoperable with non-manufacturer specific Archival Storage systems.

7.3.1 Interoperable format between the Active and Archival Storage Systems.

This format needs to be fully specified. Thoughts:

- Since this is an archival system and it is not expected that the digital asset will be directly viewed form the system, the actual coding format of the digital asset should not mater. Both proprietary coding formats and industry standard coding formats should be possible
- The chain of custody log, authentication data, and associated meta data needs to be transferred between the two systems. This shall be using an industry standard format. Suggested formats include AAF, MSF, and MPEG7. Current working group preference is MSF. However a study of the three needs to be completed before a firm recommendation can be made.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A – Recommended Policies and Best Practices

1.1 All mobile video systems shall be of industrial/commercial grade. No prototype models will be considered for testing.

1.2 Requirements

1.2.1 The mobile video system (in-car camera) shall have a proven, reliable record in actual vehicular use under a variety of conditions. This record shall be evidenced by wither manufacturers' testing results, or filed testing results by other law enforcement agencies.

1.2.2 The vendor must have experience in manufacturing and supporting such systems to include provisions for parts and service as needed.

1.2.3 The vendor shall provide business and financial history upon request.

1.2.3.1 Vendors that do not manufacture the components comprising the video system shall be authorized by the original component manufacturer to resell such components. A copy of a factory-authorized dealer certificate shall be provided.

1.2.3.2 The basic design of all equipment shall be in full production, no prototype models will be considered.

1.2.3.3 All components of the system must comply with Federal Communications Commission (FCC) standards.

1.2.3.4 To document vendors' experience in the manufacture, sales, and support of mobile video systems, the vendor shall list agencies to which mobile video systems were sold. Letters of reference for verification should be included.

1.2.4 Sample and Demonstration:

Prior to award, the agency reserves the right to require any bidder to provide complete video systems of the exact configuration offered for the purposes of evaluation to determine compliance with the specification requirements.

1.2.4.1 Any mobile video system may be field and laboratory tested by state or independent laboratories to verify its acceptable level of performance and conformity to specifications.

1.3 Warranty Section

1.3.1 All camera, recorder, environmental control components, wireless microphones and transmitters, receiver, monitor, and control circuit components, shall be warranted to ensure they are fit for their intended purpose for a minimum of one year.

1.3.2 All defective equipment shall be repaired or replaced within the contracted terms of the warranty. Law enforcement agencies should take into consideration the down time of a vehicle placed out of service due to equipment failure.

1.3.3 For warranty purposes, the warranty time begins with initial installation of said equipment in the vehicle.

1.4 Vehicle Recording System Integrity

1.4.1 The officer assigned to the vehicle shall log into the recorder prior to the use of the recorder. This login may be through a User Identification and authentication mechanism provided by the recorder or by standing in front of the camera and recording the Officer's image and voice.
1.4.2 Before each shift, the officer shall visually verify the equipment has not been tampered with or has been damaged.
1.4.3 A Visual "check" of removable media shall be made to ensure no tampering has occurred, tamper seals are in place (similar to tape used to seal evidence envelopes); and no scratch marks are on the storage device.
1.4.4 The IACP Model Policy requires the user officer to conduct an operational readiness test of the system prior to the beginning of their tour of duty. If the system is malfunctioning, they shall notify their supervisor and communications. The supervisor shall make the determination as to when and how the system is repaired or in some cases whether to keep the unit in service.

1.5 Active and Archival Storage Systems

1.5.1 The Active and Archival Storage system shall be located in a secured building (e.g., police station) in a room with restricted access (e.g., server room).
1.5.2 The Active and Archival Storage system should be cloned at another location.
1.5.3 When the media is being transferred to another medium during the back-up, the file should also be stored separately from the main server.
1.5.4 Access and authentication to the Active and Archival Storage System shall be governed by the agency's existing policies and procedures and *shall* include additional levels of user authentication prior to granting access
1.5.5 Electronic notification shall be provided for each digital asset intended to be removed from Active or Archival Storage at a time prior to removal based on operating agency policy according to the retention period for the digital asset(s).

1.6 Removable Media Security

1.6.1 Physical tamper detection.

1.6.1.1 The operator of the recorder shall perform a physical "check" of removable media to ensure no tampering has occurred:
a) No scratch marks on storage device; and
b) Physical tamper detection devices in place.

1.6.2 Key Management. Keys shall be managed via agency policies and procedures such as:

- Identification of individual with key to media;
- Identification of individual with a "master" key; and
- Identification of individual that can replicate keys.

1.7 Back Office Equipment Security

Any space used by the agency to house the Active Storage, Archival Storage, and associated equipment housed in the agency's back office shall include:

- Equipment housed in secured facility with limited employee access.
- Secured system access:
- System captures standard "audit" information when user logs into system;
- System captures number of times user attempts to log into system; and
- System user accounts become inoperable if more than three unsuccessful log-on attempts have been made.
- System "passwords" governed by agency policy requirements:

i. Passwords to user accounts should be changed on a regular basis per departmental policy, though the IACP recommends that the user account passwords to the digital video system be changed every 30 days for enhanced security.
ii. Force "character" requirements for passwords, e.g. numeric, alpha, caps, etc.

1.7.1 Operational Policy Considerations. These are questions that should be considered when setting operational policy related to the use of the recorder, recorded material, or archive. These considerations are items that support the recommendations in these specifications but are beyond the scope of the minimum recommendations.

1.8. Operational Digital Asset Transfer Policy

1.8.1 The agency should have a documented transfer policy with procedures establishing:

a) How the transfer of the digital asset from the vehicle takes place;
b) Available storage capacity remaining limit at which point the digital asset should be transferred from the vehicle recorder;
c) How equipment or removable media keys should be managed via policies and procedures, such as:
    i. Identification of individual with key to media;
    ii. Identification of individual with a "master" key;
d) Identification of individuals who can replicate keys;
e) Who is allowed to initiate the transfer or handle any removable media;
f) How to maintain a manual audit trail;
g) Recommended audit trail metrics for instances when the physical (manual) transfer of the digital asset from the recorder to Active Storage uses a removable media device (e.g., Spinning Optical, Flash, Digital Tape, Removable Magnetic);
h) A system for establishing the identification (badge number or employee number) of the officer or person submitting the digital asset for transfer. (It is recommended that when a major incident occurs, authorized personnel respond to the scene and take custody of the digital asset.);
i) Media identification numbering system (if tracked by the department);
j) The capture of time/date of the transfer;
k) The capture of the size of the digital asset transferred;

l) The capture of the number of "copies" made to other media (e.g., Tape, Spinning Optical Media, Other server storage location);
m) Acceptable retention periods for digital asset;
n) How integrity checks are to be performed as a means to validate that the digital asset transferred to the active storage as an *accurate* copy prior to any clearing of digital assets on the removable storage media;
o) Indicate successful transfer of digital asset capture; and
p) Dictate how metadata are specifically coordinated and managed, to include where and how a user or may not be permitted access.

1.8.2 Archival policies. How long the digital asset needs to be archived shall be mandated by the agency in accordance with local and state laws. It is an operational and departmental policy that needs to be established

1.8.3 Verification of location of capture of recorded digital assets. Proof of where the digital asset was captured through verification by officer in the stated location.

1.8.4 Electronic check of the Chain of Custody Audit Log on the media.

1.9 Manufacturer Considerations.

Although not part of the minimum recommendations, these are additional areas that should be considered when specifying an Vehicle Video Capture System.

1.9.1 Storage Solution

- What are the methods of digital asset retention offered by the manufacturer?
- Does the manufacturer provide a storage solution that facilitates the removal of the video from the vehicle?
- Types of storage solutions:
  - Hard drive;
  - Digital cassette;
  - Optical media;
  - Flash media.
- Transfer Methods:
  - Automatic;
  - Manual;
  - Wireless;
  - Wired.
- Ease of removal of the storage solution.
- Does the manufacturer provide a method to electronically identify when the media is removed from the vehicle recorder and individually logged into the system at the time the media was removed?
- Does the manufacturer's solution provide a method to configure an alert indicating when the maximum storage capacity in the vehicle equipment is being approached?
- Does the manufacturer's Active and Archival Storage systems provide protection against failure of the storage solution?

- Does the manufacturer's vehicular equipment contain mechanisms to minimize the damage to the digital assets in case of vehicle crash, fire, and/or physical abuse?
- Does the manufacturer's equipment contain tamper detection mechanisms?
- Does the manufacturer's equipment contain tamper resistance mechanisms?
- What is the cost-effectiveness of the storage solution?
- What is the shelf life of the storage solution? For a class 1 felony, can the digital asset be kept available for a minimum of 25 years and up to 75 years?
- Does the manufacturer's storage solution indicate when the recorder or removable media is operated outside of the manufacturer's specified temperature range? This indication may be used to determine when to recertify the equipment or replace the storage solution.
- Does the recorder include functionality to track the estimated remaining lifetime of the removable media?
- Does the manufacturer provide a method to electronically identify removable media?

1.9.2 Chain of Custody

- Does the manufacturer provide physical security for the vehicle equipment?
- Are there mechanisms to prove that the digital asset is original?
- Does the manufacturer include a CPU or Hardware ID of the vehicle recorder in the audit log of the digital asset?
- Is there an ability to indicate where and when digital asset was captured?
- Does the equipment provide electronic validation of location and time synchronization between recorders through use of GPS equipment?
- Is the time and date on the recorders synchronized to the back office equipment?
- Does the manufacture provide evidence that system components are synchronized in time?
- Can the manufacturer provide a recording stream that is not alterable?
- Does the manufacturer provide the capability of assigning individuals authorization to access the media?
- Does the manufacturer provide the capability of protecting the digital asset on removable media so that it cannot be accessed by unauthorized equipment?
- Does the manufacturer provide synchronization between the record streams and telemetry streams from one or more mobile systems for playback?
- Does the manufacturer provide a method for the user of the vehicle recorder to log in and authenticate?

1.9.3 Electronic Transfer

- Does the manufacturer provide other security methods?
- Cryptography methods other than 128-bit encryption may be used to create a private network connection for digital asset transfer. Does the manufacturer provide technical documentation to support admissibility hearings if an encryption method other than 128-bit encryption is used?

- Other forms of high security tunnels (e.g., VPN, IKE, PKI, DES, 3DES, IPSec, AES, TKIP) are commercially available and provide security beyond what is provided by 128-bit encryption. At their customers' discretion, manufacturers may provide a higher level of data confidentiality for the transfer of digital assets. Does the manufacturer provide technical documentation to support admissibility hearings that ensures that the link is secure and that the data transfer across the link meets the integrity requirements laid out in these specifications?
- Manufacturers, at their customers' discretion, may also provide encryption of the digital asset using commercially available, or proprietary methods prior to transfer to Active Storage using one. Does the manufacturer provide technical documentation to support admissibility hearings to ensure that the digital asset once decrypted on the other side of the transfer is an *accurate* copy of the original and meets the integrity requirements laid in these specifications?