Part IA – Technical Proposal	
RFP Title:	Body Worn Cameras
RFP:	3273
Vendor Name:	Digital Ally, Inc.
Address:	9705 Loiret Blvd, Lenexa, KS, 66219
Opening Date:	9/28/16
Opening Time:	2:00 PM

Table of Contents

Vendor Information Sheet 3

State Documents 5

Addendum Acknowledgement 5

Attachment A 6

Attachment C 7

Licensing Agreements/Hardware and Software Maintenance Agreements 8

Applicable Certifications and Licenses 20

Attachment B 21

Scope of Work 23

Company Background and References 219

Attachment G 227

Other Informational Material 233

VENDOR INFORMATION SHEET FOR RFP 3273

Vendor Must:

A) Provide all requested information in the space provided next to each numbered question. The information provided in Sections V1 through V6 will be used for development of the contract;

B) Type or print responses; and

C) Include this Vendor Information Sheet in Tab III of the Technical Proposal.

V1	Company Name	***Digital Ally, Inc.***

V2	Street Address	***9705 Loiret Blvd***

V3	City, State, ZIP	***Lenexa, Kansas, 66219***

V4	Telephone Number		
	Area Code: ***913***	Number: ***814-7774***	Extension:

V5	Facsimile Number		
	Area Code: ***913***	Number: ***814-7775***	Extension:

V6	Toll Free Number		
	Area Code: ***800***	Number: ***440-4947***	Extension:

V7	***Contact Person for Questions / Contract Negotiations, including address if different than above***
	Name: ***Brian Hill***
	Title: ***Regional Sales Manager***
	Address: ***9705 Loiret Blvd, Lenexa, KS, 66219***
	Email Address: ***bids@digitalallyinc.com***

V8	Telephone Number for Contact Person		
	Area Code: ***913***	Number: ***814-7774***	Extension:

V9	Facsimile Number for Contact Person		
	Area Code: ***913***	Number: ***814-7775***	Extension:

V10	***Name of Individual Authorized to Bind the Organization***	
	Name: ***Jessica Bishop***	Title: ***Bids and Contracts Manager***

V11	Signature ***(Individual must be legally authorized to bind the vendor per NRS 333.337)***	
	Signature:	Date: ***9/21/2016***

ALL ELSE REMAINS THE SAME FOR RFP 3273.

Vendor must sign and return this amendment with proposal submitted.

Vendor Name:	***Digital Ally, Inc.***		
Authorized Signature:			
Title:	***Bids and Contracts Manager***	Date:	***9/21/2016***

This document must be submitted in the "State Documents" section/tab of vendors' technical proposal.

ATTACHMENT A – CONFIDENTIALITY AND CERTIFICATION OF INDEMNIFICATION

Submitted proposals, which are marked "confidential" in their entirety, or those in which a significant portion of the submitted proposal is marked "confidential" **will not** be accepted by the State of Nevada. Pursuant to NRS 333.333, only specific parts of the proposal may be labeled a "trade secret" as defined in NRS 600A.030(5). All proposals are confidential until the contract is awarded; at which time, both successful and unsuccessful vendors' technical and cost proposals become public information.

In accordance with the Submittal Instructions of this RFP, vendors are requested to submit confidential information in separate binders marked "**Part I B Confidential Technical**" and "**Part III Confidential Financial**".

The State will not be responsible for any information contained within the proposal. Should vendors not comply with the labeling and packing requirements, proposals will be released as submitted. In the event a governing board acts as the final authority, there may be public discussion regarding the submitted proposals that will be in an open meeting format, the proposals will remain confidential.

By signing below, I understand it is my responsibility as the vendor to act in protection of the labeled information and agree to defend and indemnify the State of Nevada for honoring such designation. I duly realize failure to so act will constitute a complete waiver and all submitted information will become public information; additionally, failure to label any information that is released by the State shall constitute a complete waiver of any and all claims for damages caused by the release of the information.

This proposal contains Confidential Information, Trade Secrets and/or Proprietary information as defined in ***Section 2 "ACRONYMS/DEFINITIONS."***

Please initial the appropriate response in the boxes below and provide the justification for confidential status.

Part IB – Confidential Technical Information			
YES		NO	**X**
Justification for Confidential Status			

A Public Records CD or Flash Drive has been included for the Technical and Cost Proposal			
YES		NO (See note below)	**X**
Note: By marking "NO" for Public Record CD or Flash Drive included, you are authorizing the State to use the "Master CD or Flash Drive" for Public Records requests.			

Part III – Confidential Financial Information			
YES		NO	**X**
Justification for Confidential Status			

Digital Ally, Inc.

Company Name

Signature

Jessica Bishop — ***9/21/2016***

Print Name — Date

This document must be submitted in Tab IV of vendor's technical proposal

ATTACHMENT C – VENDOR CERTIFICATIONS

Vendor agrees and will comply with the following:

(1) Any and all prices that may be charged under the terms of the contract do not and will not violate any existing federal, State or municipal laws or regulations concerning discrimination and/or price fixing. The vendor agrees to indemnify, exonerate and hold the State harmless from liability for any such violation now and throughout the term of the contract.

(2) All proposed capabilities can be demonstrated by the vendor.

(3) The price(s) and amount of this proposal have been arrived at independently and without consultation, communication, agreement or disclosure with or to any other contractor, vendor or potential vendor.

(4) All proposal terms, including prices, will remain in effect for a minimum of 180 days after the proposal due date. In the case of the awarded vendor, all proposal terms, including prices, will remain in effect throughout the contract negotiation process.

(5) No attempt has been made at any time to induce any firm or person to refrain from proposing or to submit a proposal higher than this proposal, or to submit any intentionally high or noncompetitive proposal. All proposals must be made in good faith and without collusion.

(6) All conditions and provisions of this RFP are deemed to be accepted by the vendor and incorporated by reference in the proposal, except such conditions and provisions that the vendor expressly excludes in the proposal. Any exclusion must be in writing and included in the proposal at the time of submission.

(7) Each vendor must disclose any existing or potential conflict of interest relative to the performance of the contractual services resulting from this RFP. Any such relationship that might be perceived or represented as a conflict should be disclosed. By submitting a proposal in response to this RFP, vendors affirm that they have not given, nor intend to give at any time hereafter, any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant or any employee or representative of same, in connection with this procurement. Any attempt to intentionally or unintentionally conceal or obfuscate a conflict of interest will automatically result in the disqualification of a vendor's proposal. An award will not be made where a conflict of interest exists. The State will determine whether a conflict of interest exists and whether it may reflect negatively on the State's selection of a vendor. The State reserves the right to disqualify any vendor on the grounds of actual or apparent conflict of interest.

(8) All employees assigned to the project are authorized to work in this country.

(9) The company has a written equal opportunity policy that does not discriminate in employment practices with regard to race, color, national origin, physical condition, creed, religion, age, sex, marital status, sexual orientation, developmental disability or handicap.

(10) The company has a written policy regarding compliance for maintaining a drug-free workplace.

(11) Vendor understands and acknowledges that the representations within their proposal are material and important, and will be relied on by the State in evaluation of the proposal. Any vendor misrepresentations shall be treated as fraudulent concealment from the State of the true facts relating to the proposal.

(12) Vendor must certify that any and all subcontractors comply with Sections 7, 8, 9, and 10, above.

(13) The proposal must be signed by the individual(s) legally authorized to bind the vendor per NRS 333.337.

Digital Ally, Inc.

Vendor Company Name

Vendor Signature

Jessica Bishop — ***9/21/2016***

Print Name — Date

This document must be submitted in Tab IV of vendor's technical proposal

7

Sample VuVault.com Service Level Agreement

VU-VAULT.COM WEBSITE ACCOUNT AND CLOUD STORAGE

LICENSE AGREEMENT

This VuVault.Com™ Website Account And Cloud Storage License Agreement (the "Agreement") is made on this _____ day of _____, 201_ (the "Effective Date"), by and between Digital Ally, Inc. ("Digital Ally"), a Nevada corporation having its principal place of business at 9705 Loiret Boulevard, Lenexa, Kansas 66219, and _____ ("Customer"), a _____ having its principal place of business at _____.

Unless otherwise defined in this Agreement, all capitalized terms will have the meanings given to them in Section 11 of this Agreement. The terms "you," "your," "yours," and "Customer" refer to the law enforcement customer using the Digital Ally™ website. The terms "Digital Ally," "we," "us," "our" or words of similar import refer to Digital Ally, Inc. The term "Website" refers to any and all Digital Ally™ or VuVault™ websites.

1. VUVAULT.Com™ PROGRAM AND SERVICES

1.01 VuVault.Com™ Program. The VuVault.Com™ back office software suite (hereinafter, "VuVault program") enables law enforcement agencies to quickly and easily manage their digital video evidence across all of Digital Ally's products. The VuVault program is utilized for playing back, downloading, archiving, reviewing, unit configuration and management, running customizable reports and chain of custody logs as well as exporting/burning videos for court. This data is made available to the Customer over the Internet through each Customer's account on the VuVault program website ("Website Account"). The VuVault program offers law enforcement agencies a large range of capabilities, including video evidence reporting, chain of custody reporting, cloud software storage options, and case management, redaction, and storyboarding applications. The VuVault program is designed to work in conjunction with Digital Ally's event recording hardware, sold by separate purchase order in conjunction with the VuVault program ("Units"), including, if selected by the Customer, the VuVault.Com ™ All-In Package, which includes the VuVault program with the Pro Plan as the Cloud Storage Plan, and the Units designated in the VuVault.Com ™ All-In Package. This Agreement applies to the Services (as defined in Section 1.02) only; Units (including all hardware) are sold by Digital Ally pursuant to their own terms and conditions.

1.02 Services. The term "Services" used in this Agreement means all services offered by Digital Ally in conjunction with the VuVault program, including the cloud storage plan and any options you select and use ("Cloud Storage Plan"), and the VuVault program and Digital Ally software, applications, and Website Accounts, and the hosting and other services we supply as part of the Website operation. By selecting to use the Services, you are authorizing Digital Ally to arrange to store and provide access to your data pursuant to VuVault program policies and procedures and all agreements between you and Digital Ally, and you agree that you will not resell the Services or use the Services in any manner that is

prohibited by Digital Ally. You agree to be solely responsible for your stored data and for complying with all applicable copyright and other laws, including import and export control laws and regulations, and with the terms of any licenses or agreements to which you are bound. You warrant that the data you send or are storing in your Website Account is, and will be, free from any malware, viruses, Trojan horses, spyware, worms, or other malicious or harmful code. You further agree to use the Services in accordance with all applicable state, federal, and local laws, rules, regulations, and this Agreement.

1.03 Cloud Storage Plans. The VuVault program offers Cloud Storage Plans designed specifically for Customer's needs in accordance with the provisions and pricing provided on Exhibit A to this Agreement, which is attached hereto and incorporated herein by this reference. Exhibit A may contain pricing for both the Services pursuant to this Agreement, as well as for the Units, sold pursuant to the Unit Terms of Sale. Exhibit A will record the Services you have selected, which may be modified from time to time by written agreement between Digital Ally and Customer.

2. GRANT OF LICENSE; LICENSE RESTRICTIONS

2.01 Access to Website Account And Services. During the term of this Agreement and subject to the terms and conditions herein, Digital Ally hereby grants to Customer a limited, non-exclusive, non-transferable, non-sub-licensable, revocable, royalty-bearing license to access Customer's Website Account and to use the Services that Customer has selected and paid for ("License").

2.02 Primary Administrator; Authorized Users. Customer shall authorize a "Primary Administrator" to oversee this Agreement and the use of this License, and shall provide the name and contact information for the Primary Administrator to Digital Ally to further communications between Customer and Digital Ally. Customer may authorize department officers who wear Units that record events, and other personnel in its employ, and law enforcement advisors of Customer that are authorized by the Primary Administrator, including Customer's independent advisors such as Customer's attorneys and prosecutors (collectively with the Primary Administrator, "Authorized Users"), to use the License issued to Customer under this Agreement so long as Customer agrees to be responsible for the Authorized Users' compliance with this Agreement.

If Customer is required to take any action, or prohibited from taking any action, under this Agreement, such requirements or prohibitions equally apply to all Authorized Users. Customer may not transfer or sublicense the License to any third party, in whole or in part, in any form, whether modified or not. Each Authorized User must be at least eighteen (18) years old to access or use the Services.

2.03 License Restrictions. Customer may not use the Services in any manner or for any purpose other than as expressly permitted by this Agreement. Customer will not engage in any of the following prohibited acts: (i) willfully tamper with the security of any of the Services; (ii) access data not associated with Customer's Website Account; (iii) log into an unauthorized server or a third party's Website Account without authorization; (iv) attempt to probe, scan or test the vulnerability of any of the Services or to breach Digital Ally's website security or authentication measures without proper authorization from Digital Ally; (v) willfully render unusable any part of the Services; (vi) reverse engineer, de-compile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of any of the Services; (vii) modify, translate, or create derivative works based on any of the Services; (viii) rent, lease, distribute, license, sublicense, sell, resell, assign, or otherwise commercially exploit any of the Services, or make any Services available to a third-party other than as contemplated in this Agreement; (ix) publish or disclose to third parties any evaluation of the Services without Digital Ally's prior written consent; (x) remove, modify, or obscure any copyright, trademark, patent or other proprietary notice that

appears on the Website; or (xi) use the Services for any unlawful purpose or in violation of any applicable law (including, without limitation, data protection and privacy laws). The software and related technology incorporated into the VuVault program are subject to applicable United States export laws and regulations. Customer must comply with all applicable United States and international export laws and regulations with respect to such software and related technology. Without limitation, Customer may not export, re-export or otherwise transfer such software or related technology, without a United States government license: (a) to any person or entity on any United States export control list; (b) to any country subject to United States sanctions; or (c) for any prohibited end use.

Customer agrees to immediately report to Digital Ally, and to use its best efforts to promptly stop, any violation of the terms and conditions set forth in this Section, this Agreement, and/or any other Digital Ally agreement or policy to which Customer has agreed to be bound, including but not limited to the Digital Ally Privacy Policy (collectively, "Terms and Conditions"), all of which are incorporated herein by this reference. In the event of any suspected violation of the Terms and Conditions, Digital Ally may immediately disable Customer's access to the Services and suspend its provision of such Services.

2.04 Ownership of Intellectual Property. The Services, and all content and services on the Website, including, but not limited to, trademarks and logos, designs, text, graphics, sounds, images, software, and other website materials or other asset provided under this License and Agreement, and all modifications and enhancements thereof ("Digital Ally Materials"), are the intellectual property of Digital Ally, its successors, assigns, licensors, or other vendors. The Digital Ally Materials are protected by United States and foreign intellectual property laws. Except as stated herein, none of the Digital Ally Materials may be copied, reproduced, or distributed in any form without the prior written permission of Digital Ally. Customer warrants that it will not infringe upon or violate, and will take appropriate steps and precautions for the protection of, the Services and related intellectual property rights of Digital Ally referred to in this Section.

2.05 **Feedback.** If Customer elects to provide any suggestions, comments, improvements, ideas or other feedback or materials to Digital Ally regarding Digital Ally's products and services (collectively, "Feedback"), Customer hereby grants to Digital Ally a non-exclusive, royalty-free, irrevocable, perpetual worldwide right and license to freely copy, reproduce, license, use, disclose, exhibit, display, transform, create derivative works and distribute any such Feedback without limitation. Further, Digital Ally will be free to use any ideas, concepts, know-how or techniques contained in such Feedback for any purpose whatsoever, including, without limitation, developing, making, marketing, distributing and selling products and services incorporating such Feedback. Digital Ally will have no obligation to consider, use, return or preserve any Feedback Customer provides to Digital Ally. Except with respect to Customer Confidential Information contained in Feedback, any Feedback Customer provides to Digital Ally may or may not be treated confidentially by Digital Ally, and Digital Ally will have no obligation or liability to Customer for the use or disclosure of any Feedback. Customer should not expect any compensation of any kind from Digital Ally with respect to Feedback. Digital Ally will exclusively own any improvements or modifications to the Services based on or derived from any Feedback, including all intellectual property rights therein.

3. PURCHASED SERVICES

3.01 Service Availability. Subject to the terms and conditions of this Agreement, Digital Ally will use commercially reasonable efforts to provide the Services on a twenty-four (24) hour, seven (7) day a week basis. Digital Ally may use third party vendors or service providers to assist it in providing the Services. From time to time the Services may become unavailable for reasons that include (but are not limited to) (i)

equipment malfunctions; (ii) scheduled maintenance or needed repairs; (iii) interruption, limitation, or failure of telecommunication or digital transmission links, network problems or other similar interruptions (including bandwidth problems); or (iv) any force majeure or cause beyond Digital Ally's reasonable control. You will not be entitled to any setoff, discount, refund or other credit as a result of unavailability of the Services. Digital Ally reserves the right as it deems necessary in its sole discretion to modify or discontinue any Services, or any part of the Services, with or without notice.

3.02 Security. Digital Ally will use commercially reasonable efforts to protect Customer's Website Account and Customer Information against unauthorized disclosure or access. We comply with all applicable laws, including those pertaining to security breach notification, and we will notify you of any known security breaches to your Website Account. You are responsible for maintaining the confidentiality of your account access information, including your user names and passwords, for use of the Services, and for establishing and maintaining appropriate security, protection and backup of your Customer Information. You agree to change that access information and notify us immediately regarding any possible misuse of your Website Account and the Services.

3.03 VuVault Program Technical Support. Technical support is available to customers with questions regarding the Services and their Website Account during regular business hours. Contact information and access hours for our customer support services are available on the Website.

4. ROYALTIES AND PAYMENT

4.01 Royalties. Royalty payments from Customer to Digital Ally, in exchange for the right to use intellectual property or physical assets owned by Digital Ally and covered by this Agreement, are based upon the Cloud Storage Plan and service options you select. You agree to make payments (including all fees, compensation, and other amounts) for the Services in accordance with this Agreement and the terms and conditions of the invoice you receive from Digital Ally for your VuVault program Services. All amounts payable under this Agreement are denominated in United States Dollars and Customer will pay all such amounts in lawful currency of the United States.

4.02 Unpaid Charges; Interest. You will be responsible for all costs and expenses incurred by Digital Ally in connection with the collection of unpaid amounts and fees, including court costs and reasonable attorneys' fees. Any amount not paid when due will bear interest at the rate of one and one-half percent (1.5%) per month or the maximum rate permitted by applicable usury law, whichever is less, computed and compounded daily from the date due until the date paid.

4.03 Taxes. Unless otherwise agreed upon in writing, and subject to all tax exemptions available to Customer, the fees, compensation and other amounts payable to Digital Ally under this Agreement do not include any taxes, customs, duties, fees or other charges assessed or imposed by any governmental authority other than taxes imposed on or measured by Digital Ally’s net income. Customer will pay or reimburse Digital Ally for all such taxes and charges imposed on Customer with respect to the Services under this Agreement upon demand, or provide certificates or other evidence of exemption from such taxes.

5. CUSTOMER INFORMATION

5.01 Customer Information Use. Digital Ally collects information from its customers, including all customer records, data, and customer content of any kind that Digital Ally receives from Customer (collectively, "Customer Information") in order to provide the Services. Customer Information will be used to provide the Services, technical support and for other business purposes, such as for billing,

marketing, and evaluating the Services. The Digital Ally Privacy Policy provides more information on how Digital Ally collects, uses and shares the Customer Information, which can be viewed on the VuVault program website. Digital Ally may use, access, and retain Customer Information in order to provide the Services to you and enforce the terms of the Agreement, and you grant Digital Ally all authority it requires to do so. This authority includes, for example, the rights to copy Customer Information for backup purposes, modify Customer Information to enable access in different formats, use Customer Information to organize it, and access Customer Information to provide technical support.

5.02 Retention of Customer Information. Customer Information compiled by Digital Ally from rendering the Services will be retained as long as a legitimate business need exists to do so, in Digital Ally's sole discretion, and will be made available to law enforcement and other government agencies pursuant to legally valid requests for such information. Customer is solely responsible for preserving Customer Information during and beyond the term, and beyond the provisions of, this Agreement. Following termination of this Agreement for any reason, Digital Ally is not obligated to maintain Customer Information, unless required by a court, or other government entity, with jurisdiction over this Agreement.

5.03 Customer Information Ownership. Customer Information received by Digital Ally from Customer, or compiled by Digital Ally from rendering the Services, shall be and is hereby deemed, as between Digital Ally and Customer, to be the exclusive property of Customer including any related intellectual property rights. Customer is solely responsible for (i) the development, content, operation, maintenance, use, and retention of its Customer Information in contracting for and using the Services; (ii) for insuring that in compiling and providing its Customer Information to Digital Ally, and in using the Services, Customer at all times complies with the terms of this Agreement and all applicable laws, (iii) any claims relating to its Customer Information, including claims by third parties; and (iv) for insuring that Customer or its licensors own all right, title, and interest in and to the Customer Information, including those necessary to grant to Digital Ally the rights of use contemplated by this Agreement.

5.04 Customer Information At Termination. Although it is all customers' obligation to maintain, retain, and back up its Customer Information at all times during and following the term of this Agreement, as long as Customer is not in default of the Agreement at and following termination of this Agreement, if Customer delivers written notice to Digital Ally within sixty (60) days following such termination that Customer requests the return of its Customer Information in Digital Ally's possession ("Timely Notice"), within sixty (60) days following such Timely Notice, Digital Ally will, at Customer cost and expense in accordance with Exhibit A hereto, provide Customer with post-termination and data retrieval authority and assistance as may be required for Customer to download and transfer its Customer Information to Customer servers. If a customer is in default of this Agreement at and/or following termination, it is a defaulting customer's obligation to have preserved its Customer Information and, unless required by a court or other government entity with jurisdiction over this Agreement, post-termination data retrieval assistance and/or preservation will not be provided to such defaulting customer by Digital Ally.

6. WARRANTIES AND CUSTOMER RESPONSIBILITES

6.01 Software Warranty. Digital Ally software will be repaired, replaced or upgraded ("Software Modifications"), in the discretion of Digital Ally, at Digital Ally's premises during the term of this Agreement. Customer shall be responsible for the installation of Software Modifications, at Customer's expense.

6.02 Customer Providers and Equipment. Customer is responsible, at its cost, for providing and maintaining Internet access and all necessary telecommunications equipment, software and other materials

necessary for accessing Customer's Website Account, for properly downloading Customer Information, and downloading, maintaining and using the Services.

6.03 Hosting Providers Waiver. Your Website Account is hosted by Digital Ally through one or more service providers that provide the Cloud Storage capacity and Website access used to provide the Services. CUSTOMER EXPRESSLY UNDERSTANDS AND AGREES THAT IT HAS NO CONTRACTUAL RELATIONSHIP WHATSOEVER WITH THE UNDERLYING WIRELESS AND/OR STORAGE SERVICE PROVIDERS OR THEIR AFFILIATES OR CONTRACTORS AND THAT CUSTOMER IS NOT A THIRD PARTY BENEFICIARY OF ANY AGREEMENT BETWEEN DIGITAL ALLY AND ITS SERVICE PROVIDERS. IN ADDITION, CUSTOMER ACKNOWLEDGES AND AGREES THAT DIGITAL ALLY'S SERVICE PROVIDERS AND ITS AFFILIATES AND CONTRACTORS SHALL HAVE NO LEGAL, EQUITABLE, OR OTHER LIABILITY OF ANY KIND TO CUSTOMER AND CUSTOMER HEREBY WAIVES ANY AND ALL CLAIMS OR DEMANDS THEREFOR AGAINST DIGITAL ALLY OR ITS SERVICE PROVIDERS.

6.04 No Responsibility for Service Interruptions or Lost Data. DIGITAL ALLY SHALL HAVE NO LIABILITY WHATSOEVER AS A RESULT OF THE UNIT(S) BEING LOCATED IN AN AREA NOT COVERED BY APPROPRIATE WIRELESS COVERAGE, OR IF THE UNIT(S) FAIL TO ESTABLISH A CONNECTION WITH WIRELESS SERVICES, OR IF SERVICES ARE DISABLED DUE TO ANY NETWORK OR STORAGE PROVIDER RELATED ISSUES OR FOR LOSS OF CUSTOMER INFORMATION. THE CLOUD STORAGE PLAN, THE SERVICES AND ALL INFORMATION, CONTENT, MATERIALS, AND SERVICES INCLUDED ON OR OTHERWISE MADE AVAILABLE TO YOU THROUGH THE WEBSITE ARE PROVIDED BY DIGITAL ALLY ON AN "AS IS" AND "AS AVAILABLE" BASIS, UNLESS OTHERWISE SPECIFIED IN WRITING.

6.05 No Other Warranties. EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, DIGITAL ALLY MAKES NO OTHER WARRANTIES AND DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE. IF CUSTOMER MADE ITS PURCHASE THROUGH A THIRD PARTY, DIGITAL ALLY IS NOT RESPONSIBLE FOR THE REPRESENTATIONS OR WARRANTIES MADE BY SUCH THIRD PARTY.

7. INDEMNITY

7.01 Indemnity By Digital Ally. Digital Ally agrees, at its own expense, to defend or, at its option, to settle, any action brought against Customer to the extent it is based on a claim that the Services directly infringe any United States patent, copyright or trademark of a third party, and Digital Ally will indemnify and hold Customer harmless from and against any losses, damages, and expenses (including reasonable attorneys' fees) that are attributable to such action and are assessed against Customer in a final judgment. Digital Ally shall have the foregoing obligation to Customer only if Customer provides Digital Ally with a promptly delivered written request for indemnification and defense in such action and provides all available assistance and authority reasonably necessary for Digital Ally to defend such action. Digital Ally in such defense and indemnification will have sole control and authority over the defense and settlement thereof; and Digital Ally shall not be responsible to, and shall not compensate Customer for, any attorneys' fees or other expenses or costs incurred before Customer requests indemnification and defense. If any Services becomes, or in Digital Ally' opinion are likely to become, the subject of an infringement claim or action, Digital Ally may, at its option and in its sole discretion either procure, at no cost to Customer, the right for Customer to continue using the Services, or replace or modify the Services

to render them non-infringing, provided there is no material loss of functionality. If in Digital Ally's reasonable opinion, the aforementioned options are not commercially viable options, Digital Ally may in its sole discretion terminate any of the Services or the Agreement. The preceding remedy provision states Digital Ally's sole obligation and your exclusive remedy in the event any claim or action for infringement is commenced or is likely to be commenced. This indemnification obligation will not apply to (i) any action caused by the use of the Services not in accordance with the terms of this Agreement; (ii) modifications to the Services by a person or entity other than Digital Ally or its third-party licensors; (iii) where the Services are combined with processes or materials not supplied under this Agreement by Digital Ally, or (iv) where Customer continues an allegedly infringing activity after being notified thereof.

7.02 Indemnification By Customer. Except for claims covered by Digital Ally's indemnification obligation in Section 7.01, Customer agrees to defend, indemnify and hold Digital Ally and its officers, directors, shareholders, employees, suppliers and re-sellers, its agents, licensees, licensors, and subcontractors ("Indemnified Party(ies)") harmless from and against all losses, damages and expenses, including reasonable attorneys' fees, in connection with any claims against the Indemnified Parties in any way arising out of or related to: (i) Customer's negligent or willful acts or omissions in using the Services,; (ii) a violation by Customer of this Agreement, including engaging in any prohibited conduct hereunder; or (iii) any claim that Customer or its Authorized Users used the Services improperly, illegally, or for unauthorized or illegal monitoring. Customer will have the foregoing indemnification obligation only if an Indemnified Party provides Customer with a promptly delivered written request for indemnification and defense in such action and provides all available assistance and authority reasonably necessary for Customer to defend such action.

8. LIMITATION OF LIABILITY

IN NO EVENT WILL DIGITAL ALLY OR ITS AGENTS, SUBCONTRACTORS, LICENSEES, SUPPLIERS OR LICENSORS OR RE-SELLERS, TOTAL AGGREGATE LIABILITY ARISING FROM OR RELATED TO THIS AGREEMENT (INCLUDING FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION, AND OTHER CONTRACT OR TORT CLAIMS), EXCEED THE AMOUNT OF DIRECT DAMAGES ACTUALLY INCURRED BY CUSTOMER, UP TO THE AMOUNT OF FEES PAID FOR THE BLOCK CLOUD STORAGE PRICING COMPONENT YOU HAVE SELECTED, AS LISTED ON EXHIBIT A, DURING THE SIX (6) MONTHS IMMEDIATELY PRECEDING THE EARLIEST EVENT GIVING RISE TO THE DAMAGES. UNDER NO CIRCUMSTANCES SHALL DIGITAL ALLY OR ITS AGENTS, SUBCONTRACTORS, LICENSEES, SUPPLIERS OR LICENSORS OR RE-SELLERS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS OTHER THAN THOSE IDENTIFIED IN SECTION 7.01; (II) LOSS OR DAMAGE TO ANY RECORDS OR CUSTOMER INFORMATION; (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS), EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; (IV) ACTIONS OR CONDUCT OF CUSTOMER OR ITS AUTHORIZED USERS; (V) THE LOSS OF SIGNALS FROM ANY GPS SATELLITE, THE LOSS OF SIGNALS FROM ANY MOBILE NETWORK CELL OR PROVIDER, THE LOSS OF TELEPHONE SYSTEM SIGNALS, THE LOSS OF INTERNET CONNECTIVITY, THE LOSS OF OR FAILURE OF THE CLOUD STORAGE SYSTEM; OR (VI) ANY OTHER FACTORS OUTSIDE THE CONTROL OF DIGITAL ALLY.

9. CONFIDENTIALITY

Each party agrees to use commercially reasonable efforts to maintain the other party's Confidential

Information in confidence and shall not use or disclose any portion of the other party's Confidential Information to third parties, except as expressly authorized by this Agreement or as reasonably necessary to perform this Agreement.

10. TERM AND TERMINATION

10.01 Term and Cancellation; Automatic Renewal. The term of this Agreement ("Original Term") shall commence on the Effective Date and shall continue during the length of the Cloud Storage Plan selected by Customer, unless earlier terminated pursuant to this Agreement. THE CLOUD STORAGE PLAN YOU SELECT, AND THIS AGREEMENT, WILL AUTOMATICALLY RENEW AND WILL CONTINUE FOR THE SAME TERM OF YEARS AS THE EXPIRING CLOUD STORAGE PLAN (EACH AUTOMATIC RENEWAL, A "RENEWAL TERM"), UNLESS TERMINATED BY EITHER PARTY IN ACCORDANCE WITH THIS AGREEMENT. UPON AUTOMATIC RENEWAL, THE THEN CURRENT FEES AND PROVISIONS OF THIS AGREEMENT SHALL APPLY AND YOU AUTHORIZE US WITHOUT NOTICE TO COLLECT THE THEN APPLICABLE FEE AND TAXES FOR THE RENEWAL TERM, USING ANY CREDIT CARD WE HAVE ON RECORD FOR YOU. If your credit card expires or you have arranged another method of payment that has not been made in advance of the renewal date, your subscription or product will not automatically be terminated. You will remain responsible for payment of all charges for the Renewal Term. As used in this Agreement, "Term" shall include the Original Term and all Renewal Terms.

10.02 Cancellation Of Automatic Renewal. Either party may cancel this Agreement by giving written notice to the other party sixty (60) days prior to the end of a Term, and this Agreement and the Services will terminate at the end of that Term.

10.03 Suspension of Services. If you have not paid all applicable fees for the Services in accordance with this Agreement, or the Units in accordance with the terms of a Digital Ally purchase order, Digital Ally may provide you with written notice of such breach. If you do not make all outstanding payments then due within fifteen (15) days of such notice, Digital Ally may suspend your (including your Authorized Users') access to your Website Account and to the Services, until all fees are paid in full. If you are in breach of any other material provision of this Agreement, Digital Ally may, in its sole discretion, immediately temporarily suspend access to, and use of, the Website and Services by Customer (including your Authorized Users) until, in Digital Ally's reasonable discretion, the material breach or the threat to the security or functionality of the Services or the Website are cured, and upon such cure, Digital Ally will use reasonable efforts to re-establish the affected Services promptly. The exercise of Digital Ally's rights under this Section 10.03 shall not be deemed to waive Digital Ally's right to terminate this Agreement based upon any such breaches, and Digital Ally may further exercise all of its additional legal and equitable rights.

10.04 Immediate Termination By Digital Ally. If Digital Ally learns: (i) that the Services or Units are being used by anyone without authorization; (ii) that the Services or Units are being used for any unauthorized purpose; (iii) if Customer breaches its obligation to protect Digital Ally's Confidential Information or engages in an act prohibited under this Agreement, or (iv) if use of the Services or Units violates applicable law, Digital Ally may immediately and without notice of any kind, at its option, immediately terminate this Agreement, and may exercise all of its additional legal and equitable rights.

10.05 Termination for Cause. Subject to Digital Ally's rights under Section 10.03 and Section 10.04, this Agreement may be terminated: (i) by either party on thirty (30) days written notice to the other party following a material breach of the Agreement if the other party fails to cure such breach with reasonable promptness in light

of all surrounding circumstances.

10.06 Termination for Convenience. Digital Ally, by written notice, may terminate this Agreement any time, in whole or in part, without cause and/or for its convenience, and such termination shall not constitute a default. In such event, Digital Ally shall be entitled to payment for the Services rendered to Customer up to the time of said termination, and Digital Ally shall return to Customer any advance payments made by it for the Services that will not be provided by Digital Ally under this Agreement going forward. Customer may terminate this Agreement any time, in whole or in part, without cause and/or for its convenience, and such termination shall not constitute a default, so long as Customer makes complete payment under this Agreement, including for the Term of its then current Cloud Storage Plan and Services, and also fulfills its surviving obligations hereunder, including those in Sections 10.07 and 10.08.

10.07 Return of Digital Ally Assets. Upon termination of this Agreement, Customer shall immediately cease use of the License and the Services, and at its expense, return to Digital Ally all Confidential Information (including all copies thereof) then in Customer's possession or custody or control, and certify in writing as to such action.

10.08 Survival. Termination or expiration of this Agreement shall not relieve either party of obligations that by their nature or term survive termination or expiration; such as, by way of example and without limitation, the obligation to make all payments that have or will become due under this Agreement, and the confidentiality obligations in Section 9.

11. DEFINITIONS

11.01 "Cloud Storage" means data storage where the digital data is stored in logical pools, the physical storage spans across multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.

11.02 "Confidential Information" means non-public information that a party to this Agreement provides and reasonably considers to be of a confidential, proprietary or trade secret nature, including trade secrets, know how, inventions, techniques, research, designs, methods, compilations, processes, plans, programs, procedures, schematics, software source documents, data, customer lists, customer and supplier information, financial statements, projections and other financial information, and engineering, sales and marketing plans, whether in tangible or intangible form, and whether or not stored, compiled or memorialized physically, electronically, graphically, photographically, or in writing. Confidential Information shall not include Non-Confidential Information as defined below.

11.03 "Internet" means the global computer network comprised of interconnected networks using standard protocols including TCP/IP.

11.04 "Non-Confidential Information" means information which: (i) is, as of the time of its disclosure or thereafter becomes part of the public domain through no fault of the receiving party; (ii) can be demonstrated by credible evidence: (a) as rightfully known to the receiving party prior to the time of its disclosure, or (b) to have been independently developed by the receiving party; (iii) is subsequently learned from a third party not under a confidentiality obligation to the disclosing party; or, (iv) is required to be disclosed pursuant to a duly authorized subpoena, court order, or government authority, provided that the receiving party has provided prompt written notice and assistance to the disclosing party prior to such disclosure so that the disclosing party may seek a protective order or other appropriate remedy to protect against disclosure.

11. 05 "Server" means the Cloud server or servers as designated by Digital Ally from time to time

through which Digital Ally provides the VuVault program Services in accordance with this Agreement.

12. GENERAL

12.01 **Amendment**. WE MAY AMEND, CHANGE, OR MODIFY THIS AGREEMENT AT ANY TIME IN OUR SOLE DISCRETION BY POSTING THE REVISED TERMS ON THE WEBSITE OR BY OTHERWISE DELIVERING NOTICE TO YOU, BUT ANY INCREASE IN FEES WILL NOT AFFECT THE COST OF YOUR CLOUD STORAGE PLAN DURING THE TERM. YOUR CONTINUED USE OF THE SERVICES AFTER ANY AMENDMENT EVIDENCES YOUR AGREEMENT TO BE BOUND BY THE TERMS OF EACH AMENDMENT.

12.02 Notices. All notices, requests, demand or other communications shall be given in writing and shall be effective when received, which receipt shall be established as follows:(i) on the date of delivery when delivered personally or by a courier service (as conclusively evidenced by a report from such service) (ii) on the date actually delivered if deposited in U.S. certified mail, return receipt requested, or (iii) on the date of telecopy if successfully telecopied (as conclusively evidenced by a transmission report from the sender's telecopy machine indicating error-free transmission), to the Parties at the addresses set forth above, unless a party requests in writing that another address or facsimile number be used for notice purposes.

12.03 Assignment and Delegation. You may not assign, transfer, or sell any of your rights, or delegate any of your responsibilities under this Agreement without Digital Ally's prior written consent. All assignments of rights by Customer are prohibited by this Section 12.03, whether they are voluntary or involuntary, by merger, consolidation, dissolution, operation of law, or any other manner. Digital Ally may assign this Agreement, and any or all of its rights, interests, or obligations hereunder, to its affiliates, its successors in connection with the transfer or sale of all or substantially all of its business related to this Agreement, or in the event of its merger, consolidation, change in control, corporate reorganization, or similar transaction (each, a "Permitted Assign" and collectively, "Permitted Assigns"), provided, however, that any Permitted Assigns shall assume all obligations of Digital Ally under this Agreement. Any purported assignment of rights or delegation of performance in violation of this Section 12.03 is void. Subject to the preceding provisions, this Agreement shall be binding upon and inure to the benefit of the parties, their successors and assigns.

12.04 Governing Law; Forum. This Agreement shall be governed by and construed in accordance with the laws of the State of Kansas without regard to its choice of law principles. Any action arising from or relating to this Agreement must be brought in Kansas state or federal courts, located in or serving Johnson County, Kansas, and the parties hereby irrevocably consent to the exclusive jurisdiction of, and venue in such courts.

12.05 Waiver, Remedies, and Severability. If any provision of this Agreement is deemed illegal or otherwise unenforceable, that provision shall be severed and the remainder of this Agreement shall remain in full force and effect if the essential provisions of this Agreement for each party remain valid, legal and enforceable. The waiver of any breach, right, or election of any remedy in one instance, by either party, shall not affect, nor constitute a waiver of, any breach, rights or remedies in another instance. A waiver shall be effective only if made in writing and signed by an authorized representative of the party against whom the waiver is sought to be enforced. No failure or delay in exercising any right or remedy or requiring the satisfaction of any condition under this Agreement, and no act, omission or course of dealing between the parties operates as a waiver or estoppel of any right, remedy or condition.

12.06 Compliance with Laws. Customer and Digital Ally shall comply with all applicable federal, state,

and local laws and regulations.

12.07 Force Majeure. Neither party shall be liable for any delay in performance or failure to perform, in whole or in part when due to labor dispute, strike, war or act of war (whether an actual declaration is made or not), insurrection, riot civil commotion, act of public enemy, accident, fire, flood, or other act of God, act of any governmental authority, judicial action, or similar causes beyond the reasonable control of that party. If an event of force majeure occurs, the party so affected shall promptly notify the other party.

12.08 Independent Contractor. Customer and Digital Ally are and shall be independent contractors to one another, and nothing herein shall be deemed to cause this agreement to create an agency, partnership, or joint venture between the parties.

12.09 Signatures. This Agreement may be executed in several counterparts, all of which together shall constitute one agreement binding on all parties hereto, notwithstanding that all the parties have not signed the same counterpart. A signature provided by facsimile transmission shall constitute a valid signature for the purpose of this Agreement.

12. 10 Interpretation. Any pronoun used in this Agreement shall include the corresponding masculine, feminine and neutered forms. The words "include," "includes," and "including" shall be deemed to be followed by the phrase "without limitation." The words "herein," "hereof," "hereto," "hereunder," and similar terms shall refer to this Agreement, unless the context otherwise requires. The references to Exhibits, Sections, Subsections, or Articles are references to the Exhibits, Sections, Subsections or Articles of this Agreement, unless the context otherwise requires. This Agreement shall be deemed to be drafted equally by both Parties and shall not be subject to any rule requiring that it be construed against any drafter.

12.11 Captions and Section Heading and Section Numbers. The captions, section headings, and section numbers appearing in this Agreement are inserted only as a matter of convenience and in no way define, limit, construe or describe the scope or intent of such sections of this Agreement.

12.12 Survival of Obligations. The obligations of the parties hereunder, which by their terms might apply after the completion or termination of this Agreement shall survive such completion or termination.

12.13 Electronic Information. You are capable of printing or storing a copy of any electronic records of transactions into which you enter including, without limitation, any amendments to this Agreement; and, you agree to receive electronically information about the Services and other electronic records from Digital Ally that are necessary and appropriate to this Agreement. If you wish to withdraw this consent, please contact us at the customer service number set forth on the Website, in which case Digital Ally shall have the right to terminate your use of the Services.

12.14 Authority. You represent to us that you are lawfully able to enter into contracts, including that you are not a minor. If you are entering into this Agreement for an entity, including the law enforcement agency you represent, you represent to us that you have legal authority to bind that entity.

12.15 Entire Agreement. This Agreement, along with the exhibits and policies referenced herein, constitutes the entire agreement between the Parties concerning the subject matter hereof, superseding all previous agreements, proposals, representations, or understandings, whether oral or written.

IN WITNESS WHEREOF, the parties have duly executed this Agreement as of the Effective Date first

above written.

DIGITAL ALLY, INC.

BY:_____

NAME:

TITLE:

CUSTOMER: _____

BY:_____

NAME:

TITLE:

SECRETARY OF STATE

STATE OF NEVADA

CERTIFICATE OF EXISTENCE
WITH STATUS IN GOOD STANDING

I, BARBARA K. CEGAVSKE, the duly elected and qualified Nevada Secretary of State, do hereby certify that I am, by the laws of said State, the custodian of the records relating to filings by corporations, non-profit corporations, corporation soles, limited-liability companies, limited partnerships, limited-liability partnerships and business trusts pursuant to Title 7 of the Nevada Revised Statutes which are either presently in a status of good standing or were in good standing for a time period subsequent of 1976 and am the proper officer to execute this certificate.

I further certify that the records of the Nevada Secretary of State, at the date of this certificate, evidence, **DIGITAL ALLY, INC.**, as a corporation duly organized under the laws of Nevada and existing under and by virtue of the laws of the State of Nevada since December 13, 2000, and is in good standing in this state.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed the Great Seal of State, at my office on October 21, 2015.

Barbara K. Cegavske

BARBARA K. CEGAVSKE
Secretary of State

Electronic Certificate
Certificate Number: C20151021-1141
You may verify this electronic certificate online at **http://www.nvsos.gov/**

ATTACHMENT B – TECHNICAL PROPOSAL CERTIFICATION OF COMPLIANCE WITH TERMS AND CONDITIONS OF RFP

I have read, understand and agree to comply with ***all*** the terms and conditions specified in this Request for Proposal.

YES ***X*** I agree to comply with the terms and conditions specified in this RFP.

NO _____ I do not agree to comply with the terms and conditions specified in this RFP.

If the exception and/or assumption require a change in the terms in any section of the RFP, the contract, or any incorporated documents, vendors ***must*** provide the specific language that is being proposed in the tables below. If vendors do not specify in detail any exceptions and/or assumptions at time of proposal submission, the State will not consider any additional exceptions and/or assumptions during negotiations.

Digital Ally, Inc.
Company Name

Signature

Jessica Bishop — ***9/23/2016***
Print Name — Date

Vendors MUST use the following format. Attach additional sheets if necessary.

EXCEPTION SUMMARY FORM

EXCEPTION #	RFP SECTION NUMBER	RFP PAGE NUMBER	EXCEPTION (Complete detail regarding exceptions must be identified)
1	*3.11.3.19*	*20*	***The camera does not have a night vision enhancement feature; however it has a lux rating of 0.8 LUX for low light recording.***
2	*3.12.4.16*	*35*	***The DVM-800 is a replacement rear-view mirror was a front facing and passenger facing camera, eliminating the need for 360 degree rotation. The DVM-800 kit includes an external 12x camera that does have a 360 degree rotation.***

ASSUMPTION SUMMARY FORM

ASSUMPTION #	RFP SECTION NUMBER	RFP PAGE NUMBER	ASSUMPTION (Complete detail regarding assumptions must be identified)

This document must be submitted in Tab V of vendor's technical proposal

EXCEPTION #	RFP SECTION NUMBER	RFP PAGE NUMBER	EXCEPTION (Complete detail regarding exceptions must be identified)
3	*3.12.4.16*	*35*	***The DVM-800 is a replacement rear-view mirror was a front facing and passenger facing camera, eliminating the need for 360 degree rotation. The DVM-800 kit includes an external 12x camera that does have a 360 degree rotation.***
4	*3.12.3.3*	*36*	***The DVM-800 monitor has the capability to display date/time, user identification information, microphone activation indicator that is saved as metadata with the video file. It does not display emergency light indication, siren indication, latitude and longitude, speed, or braking indicator.***
5	*3.12.6.9*	*36*	***The DVM-800 is a replacement rear-view mirror, not allowing for mounting in multiple locations in the vehicle.***
6	*3.12.11.2*	*39*	***The FirstVu HD has the capability to be motorcycle mounted, however does not have a water resistant monitor. Viewing of video can be accomplished through the VuVault GO mobile application on an Android or iOS device.***

ATTACHMENT L BODY WORN SPECIFICATIONS

Vendors must respond check either yes or no to each section below: Where section asks to provide details or response, vendors must respond to the corresponding RFP section not in this document.

	Comply	
3.11.2 BWC Hardware Requirements	Yes	No
Cameras worn by officers shall be lightweight, preferably six ounces or less in total combined weight.	X	
Cameras shall have minimal wiring, not exceed two wires or cables and shall be designed to disengage to prevent the wearer from becoming entangled.	X	
Cameras shall have recording capability of at least ten continuous (10) hours (the State would prefer twelve (12) hours of continuous recording capability).	X	
Cameras must have a minimum stand-by battery life of ten (10) hours without recharging or additional batteries, with pre-record on.	X	
BWC Shall be user friendly that can be activated easily during times of stressful events.	X	
BWC should have automatic triggers, as a standalone system.	X	
Rechargeable battery must be able to reach full charge, from no power, in no more than six (6) hours.	X	
Cameras must have a minimum of thirty-two (32) GB internal/integrated memory and storage media not be removable.	X	
Rechargeable battery must be able to withstand at least three hundred (300) charging cycles, maintaining the 10 hour record time.	X	
BWC lens must have a field of view from 95 to 145 degrees.	X	
The recording speed shall be no less than 30 frames per second (fps).	X	
Camera shall record video images in full color with a minimum resolution of 640 pixels x 480 pixels. Adjustable resolution is preferable.	X	
Video compression shall be H.263 or higher.	X	
Cameras shall have multiple mounting options to accommodate varying uniformed officers, plain-clothed officers, and tactical field situations. Examples include, but are not limited to, lapel, shoulder, eyeglasses, cap, helmet, holster, button shirt, zipper shirt, utility belt, snow suit etc. Mounts shall not require modification to current in-service uniforms.	X	
Camera should allow for on scene (in the field) viewing? If so, describe the ability to playback or view video.	3.11.3.15 Page 45	
Camera shall provide feedback to user when activated, either via a visual indicator or audible tone.	X	
Camera shall have the ability to be set to stealth mode while in the field.	X	
Camera must have an indicator that shows current operating mode.	X	
If the camera offers night vision enhancement, the State shall have the ability to enable or disable it.		X

The System should provide automatic indexing functionality of video files and be capable of interfacing with existing computer-aided dispatch (CAD) vendor, Spillman technologies.		
Cameras shall automatically embed a time/date stamp in the recorded video.	X	
Cameras shall prevent users from deleting recorded files without authorization.	X	
Camera should have a method for adding desired metadata to video in the field prior to upload.	X	
Officers should have the ability to playback or view video in the field on mobile cameras and/or MDC's (Panasonic FZ-G1 Tablet) wirelessly (i.e. Bluetooth).	X	
Camera shall have a pre-event record feature (BWC should capture at least thirty (30) seconds of video prior to officer initiating the recording). Adjustable times are preferable.	X	
Camera will export in a standard, open format, such that it can be replayed in freely available software without processing or conversion. Proprietary data formats shall not be accepted.	X	
The Vendor must offer a multi-dock station capable of uploading digital evidence from multiple cameras simultaneously and have the capability to upload video via Wi-Fi and/or cellular LTE connectivity. If via cellular, product should be compatible with Fenny Wireless Skyus X modem.	X	
The multi-dock station must charge the camera batteries, securely transfer files without loss of quality or metadata, and delete the files from the camera once transferred to the evidence management system.	X	
The multi-dock station should not require a department computer to operate, connect or interface with the Internet (e.g. the multi-dock station should be a standalone device that connects to the cloud storage solution or server via an Ethernet connection).	X	
The camera should not cause electromagnetic interference with nearby airwave radios (and other electronic equipment and radio communication systems).	X	
Loss of power to the camera must not cause data to be lost/corrupted.	X	
Cameras will be ruggedized. Cameras shall be able to survive a six-foot drop test. Cameras shall be able to operate at minimum temperature of -12 degrees Fahrenheit and a maximum temperature of 130 degrees Fahrenheit.	X	
Vendor will state camera's Ingress Protection (IP) rating. The State prefers an IP rating of IP67.	X	
Describe what features devices have in place to prevent accidental activations of camera by the user (without the need for accessories or alteration of equipment by user).	3.11. 3.34 Page 48	
Vendor shall define the required time for automated indexing (specific time frame after upload of video evidence) and any expected error rate percentage upon indexing, if applicable.	3.11. 3.35 Page 48	
The Vendor must state the transfer rate of video from the multi-dock station to the cloud in sixty or thirty-minute increments. Vendors shall break down transfer rates by video quality (i.e. Hi Def).	3.11. 3.36 Page 49	

Describe device wireless activation features (e.g. device is automatically activated with the activation of patrol vehicle's light bar), if applicable.	3.11.3.37 Page 49	

	Comply	
3.11.4 VIDEO MANAGEMENT SYSTEM (VMS)	Yes	No
VMS shall either be an externally hosted cloud-based data storage solution with the capability of organizing/managing video/digital evidence, server based or consist of a hybrid solution and be accessible via the internet to multiple users simultaneously. The State prefers the Cloud or Hybrid solution.	X	
VMS shall allow for remote access with complete functionality (review, enter metadata and send video) with NHP mobile devices and/or computers.	X	
VMS shall provide an automatic audit trail for when files and videos are accessed.	X	
VMS shall allow officers to enter additional metadata to recorded files, such as notes or comments.	X	
Solution must support all major digital file types (avi, jpeg, mpeg, etc.).	X	
VMS shall provide remote viewing of the stored video based on the permissions granted by the System Administrator.	X	
VMS shall allow users to search video files by name, date of recording, date of upload, case number (CAD-generated), device number, as well as categorize and add notes to each file within the solution.	X	
VMS must allow System Administrators the ability to grant access of specific files to specified persons for a specific period of time.	X	
VMS shall have the ability to share files internally and externally via secure links over the Internet.	X	
When videos are exported to a portable media device , all metadata shall transfer over without compromising its authenticity.	X	
VMS shall grant System Administrators the ability to set variable retention rules per DPS/HPD preferences.	X	
VMS shall have the ability to set time tables for automatic deletions of files.	X	
VMS should have the ability to recover deleted evidence within a minimum of seven (7) days of deletion. The State would prefer a recovery period of 30 days.	X	
The VMS will maintain a log/audit trail illustrating users who have viewed and copied video to an external source (e.g. DVD/ long term storage).	X	
VMS must have the ability to preserve the raw file without editing.	X	
VMS must securely store all videos and recordings in a way that only State-authorized users and users authorized by DPS/HPD can view.	X	
VMS must provide redundant, security back-up of all data.	X	
VMS should offer redaction capabilities.	X	
VMS must be compatible with at least Windows 7 Professional Operating System or more recent versions) and Internet Explorer Version 11 web browser or more recent version(s).	X	
Provide the minimum required memory (RAM), if applicable.	N/A	

	Comply	
3.11.4 VIDEO MANAGEMENT SYSTEM (VMS)	Yes	No
Provide the minimum required processor speed, if applicable.	N/A	
Provide the minimum network speed to upload videos, if cloud based.	N/A	
Upload times to the VMS will be defined in per hour or thirty-minute increments of video files.	3.11.5.25 Page 53	
Any required or expected 'buffering' times before video files are accessible in cloud storage (for view or adding metadata) will be clearly defined.	3.11.5.26 Page 53	
Describe System compatibility with mobile devices (iPhones and Android).	3.11.5.27 Page 53	
Vendor shall indicate the number of searchable fields in storage system and any 'wild card' searches that can be done to locate stored data.	3.11.5.28 Page 53	
Preferences:		
Users should have the ability to send email messages from hosted solution interface to end users.	X	
VMS should send System Administrators administrative notifications when evidence files are about to be deleted.	X	
VMS should send System Administrators administrative notifications when users need their credentials reset due to failed log on attempts.	X	
VMS should offer auto-redaction capabilities, to include high-movement and low light video; preferred to minimize the amount of time to redact 30 fps for the entire length of video.	X	
VMS should have the ability to capture data, report on video statistics and provide custom reports.	X	

	Comply	
3.11.5 VIDEO STORAGE	Yes	No
If cloud based, the storage facility must be located within the continental United States.	X	
Does your storage solution have the ability to upload video from multiple camera units simultaneously?	X	
Storage solution should have the ability to view multiple linked videos simultaneously.	X	
Solution should have two tier storage capacity for active video and long term storage needs as defined by the State.	X	
Does proposed solution offer storage options for 'unlimited storage' of body camera video evidence?	X	

	Comply	
3.11.5 VIDEO STORAGE	Yes	No
Does your system provide a method to upload videos, via an access point? Please describe your process.	3.11.6.5 Page 54	
Is your system compatible with an EnGenius ENS500EXT access point?	3.11.6.6 Page 55	
Does solution have the ability to maintain and export audit trail along with video?	X	
Define maximum storage capacity, if any.	3.11.6.8 Page 55	
Describe the capability of proposed solution to provide the State with the ability to export/download and migrate original recordings with all metadata to other storage media or, local storage inclusive of all metadata and chain of custody information.	3.11.6.9 Page 55	
Describe archival, hot and cold cloud storage solutions.	3.11.6.10 Page 55	
Describe archival solutions for server storage, if applicable.	N/A	
Discuss different cost savings as defined by various storage solutions (active vs. long-term storage of files).	Attachment H.	
Describe capability to respond to requests to pull video from 'cold cloud storage', including time required to download video from storage.	3.11.6.13 Page 55	
Describe your solution to upload video in the rural areas that only have a maximum broadband speed of 1.5 Mbps	3.11.6.14 Page 56	

	Comply	
3.11.6 SYSTEM SECURITY	Yes	No
The VMS shall meet the minimal security requirements for the Criminal Justice Information Services (CJIS) Policy. In particular, the VMS shall comply with Policy Areas 2 through 13 in Section 5 of the CJIS Policy. The CJIS Policy can be viewed by accessing the following link: https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center	X	
Will access to Criminal Justice Information (CJI) within a cloud environment fall	X	

	Comply	
3.11.6 SYSTEM SECURITY	Yes	No
within the category of remote access? (5.5.6 Remote Access)		
Will advanced authentication (AA) be required for access to CJI within a cloud environment (5.6.2.2 Advanced Authentication, 5.5.2.2.1 Advanced Authentication Policy and Rationale)	X	
Does your cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physical Secure Location)	X	
Are the encryption requirements being met? (5.10.1.2 Encryption)	X	
Who will be providing the encryption as required in the CJIS Security Policy? (Client or cloud service provider)	3.11.7.5 Page 56	
Is the data encrypted while at rest and in transit?	X	
What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)	3.11.7.7 Page 57	
Will the cloud subscriber be notified of any incident?	X	
If CJI is compromised, what are the notification and response procedures?	3.11.7.9 Page 57	
Is the cloud service provider a private Vendor/vendor?	X	
If so, they are subject to the same screening and agreement requirements as any other private Vendors hired to handle CJI. (5.1.1.5 Private Vendor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Vendors and Vendors)	X	
Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)	X	
The State may verify that Vendor is in compliance with CJIS by requesting a compliance audit of Vendor's technology deployment through the CJIS Systems Agency to the Federal Bureau of Investigation (FBI). The FBI CJIS Division shall perform the requested audit to verify compliance. 140-2.	X	
System shall provide full conformance to Federal Information Processing Standards (FIPS) Publication	X	
VMS shall provide user authentication with a unique username and password.	X	
VMS will allow for authorized users to be established based on various roles and permissions by the System Administrator.	X	
VMS will offer optional IP access restriction and security challenge questions upon access from an unknown or previously used location.	X	
Any access to stored video shall be maintained in an automatic log or audit trail showing users that have viewed, shared or copied video to an external source (e.g. CD/DVD, local storage, etc.), and the audit trail should be capable of being exported	X	

	Comply	
3.11.6 SYSTEM SECURITY	Yes	No
Log activities performed by specific user ID, IP address and time/date stamp all activities.	X	
System Administrators shall have the ability to administratively manage accounts and assign rights and permissions to system users.	X	
VMS shall provide ability to set an unsuccessful access attempt limit and suspend IDs after reaching the unsuccessful access threshold.	X	
VMS shall provide ability to send alerts to System Administrators for unauthorized access attempts.	X	
VMS shall enable automatic logoff of ID after a defined period of session inactivity, and perform subsequent re-log-on password authentication.	X	
VMS shall provide ability to configure password parameters such as password lengths, user access to expiration settings and other behaviors, enabling alphanumeric characters, etc.	X	
VMS shall provide ability to lock out user or group ID.	X	
Vendor will provide a detailed explanation of data security standards, to include but not limited to: defining the physical environment, location of all host servers; protections against natural and man-made disasters; encryption; transfer; storage; redundancy and recovery of files.	3.11.7.26 Page 59-60	
Describe security standards for hardware (cameras) in place to prevent data from being accessed in the event a camera is lost or stolen.	3.11.7.27 Page 60	
Vendor will describe any previous loss of data occurring from criminal actions, as well as other issues that impact data integrity, such as unauthorized data access by contract personnel.	3.11.7.28 Page 59	
Provide a non-technical means for field personnel to remotely view stored video without altering original file (other than applying metadata to file).	3.11.7.29 Page 60	
Describe ability of system to enforce password expiration.	3.11.7.30 Page 60	
Describe ability of system to limit concurrent sessions.	3.11.7.31 Page 61	
Describe ability of system to log changes to administrative functions.	3.11.7.32 Page 61	

	Comply	
3.11.7 INFORMATION SECURITY	Yes	No
Vendor shall encrypt transmission of confidential data when transferred through publicly accessible networks such as the Internet.	X	
Vendor shall ensure all transmission of information data files are transferred through a Secure Socket Layer (SSL), which creates a 128 bit encrypted connection which is password protected. All data files that are on Vendor's servers are encrypted once they have completed the upload and pre-process procedures.	X	
All input data transmitted across public networks (all networks other than the State's) shall be encrypted during transit and decrypted electronically during processing to produce non-confidential output data. The decrypted data shall not be accessible by Vendor's employees unless otherwise limited on a "need to know" basis as determined by the Nevada Highway Patrol's designee.	X	
The System shall have a host-based firewall technology preventing inappropriate/ unauthorized access. Vendor shall provide the following:	X	
All intrusion detection system monitoring for unauthorized access attempts.	X	
Must run anti-virus software.	X	
Monitor daily logs for potential intrusions, file integrity.	X	
Only allow access by uniquely assigned and auditable IDs.	X	
All data transfers and administrative access must be in an encrypted format.	X	

	Comply	
3.11.8 In-CAR VIDEO INTEGRATION	Yes	No
BWC must have the ability to record audio for the In-car video system.	X	
BWC must have the ability to activate recording off the In-Car video systems automatic triggers.	X	

IN-CAR VIDEO COMPLY CHECK LIST

The In-Car Video portion of this RFP is contingent upon funding anticipated to be approximately one (1) year from contract award. Vendors proposing In-Car Video must be compatible with proposed Body Worn Cameras.

Vendors must respond check either yes or no to each section below: Where section asks to provide details or response, vendors must respond to the corresponding RFP section not in this document.

	Comply	
3.12 STANDARD SPECIFICATIONS	**Yes**	**No**
All mobile video systems and related audio equipment must conform to the applicable minimum standards as set by the following: Electronic Industries Association (EIA); Federal Communications Commission (FCC) rules/ regulations; Institute of Electrical and Electronic Engineers (IEEE); International Electro-technical Commission (IEC); International Organization for Standardization (ISO); National Fire Protection International (NFPA); National Highway Transportation Safety Administration (NHTSA); Society of Automotive Engineers (SAE); Underwriters Laboratories Inc. (UL); and	X	
Vendors must provide documentation that validates that their systems adhere to the minimum specifications in the International Association of Chief of Police (IACP) Specifications for In-Car Video (dated 11/21/2008), and that the technology used is generally accepted in the relevant field.	3.12.1.10 Page 63, 133	

	Comply	
3.12.2 VIDEO SYSTEM SPECIFICATIONS	**Yes**	**No**
The minimum acceptable components consist of the following parts: o Front camera o Back seat camera o Color LED monitor with audio o Body worn camera must act as a wireless transmitter for audio with in-car & home charger. o Covert secondary hard-wired microphone o Digital Video Recorder- DVR o Integrated GPS receiver and antenna; o Collision sensor o Controller center o Means to transfer media data from In-car to storage solution o Video viewer capability o Hardware/software necessary to submit videos as evidence o All mounts and cables for power, interfaces, cameras, and antennas o Documentation, o Warranty and maintenance, o Training o Shipping and handling	X	
3.12.3 DIGITAL VIDEO RECORDER (DVR)		
The digital video recorder (DVR) offered shall be in full commercial production. Prototypes will not be considered.	X	
Programming of the in-car recording system shall be restricted to authorized personnel only.	X	
All controls and indicators shall have adjustable backlighting.	X	
The officer shall have the option of recording primary, rear-facing, or both cameras simultaneously.	X	
A collision sensor covering 360 degrees, to trigger recordings, without requiring connection to the vehicles airbag system, shall be included. If a collision is detected, the video recorder (including pre-event memory) shall be automatically activated so the collision and video leading up to the collision is recorded.	X	
The in-car digital video system shall be provided with all necessary cables and hardware (e.g. fuse holders, mounting brackets) required for installation.	X	
Each digital video recording system shall be supplied with a comprehensive installation/ programming/ operations manual. The manual shall specify all brackets, hardware and mounting locations for installing camera systems.	X	

	Comply	
3.12.4 DIGITAL VIDEO RECORDER (DVR)	**Yes**	**No**
The DVR shall mount in standard equipment consoles between the seats, or overhead.	X	
No permanent modifications shall be required to install the DVR system.	X	
The DVR system shall be capable of being installed as to not hinder the operation of the police unit.	X	
The DVR shall be capable of recording two video inputs from a powerful zoom, forward-facing camera, and a wide-angle rear-facing camera.	X	
The DVR shall provide a choice of at least one of the following upload options. ○ **Wireless Ethernet**- provided 802.11n base station includes encryption, supports multiple simultaneous uploads and is upwardly scalable. The system should be capable of comfortably uploading from multiple vehicles in the regional command centers (depicted in the scope of work section of this RFP) simultaneously. In addition, a backup upload system must be provided, should the wireless transfer system fail. ○ **Removable Hard Disc Drive (HDD)** with provided hard drive docking stations that support plug and play hard drive insertion. ○ **Removable Compact Flash Device**-Device with provided docking stations that support plug-and-play flash card insertion. ○ **Cellular** - Upload media via LTE connectivity that is compatible with the Feeney Wireless Skyus-X modem.	X	
The DVR shall have the ability to record up to 8 hours of video before reaching the capacity of the storage media at maximum resolution. For the recording media available, specify the recording and playback times, resolution, and MB per second.	X	
Video resolution, frame rates, and quality on the DVR shall be preset but can be changed by an administrator. These settings shall be independently configurable for recording modes of both video cameras. Please specify levels for: video resolution video frame rate video quality	X	
The DVR shall require a security feature (key, admin software rights) to prevent unauthorized users from accessing the on-screen menus to adjust video settings and perform file management functions.	X	

The DVR shall include a GPS receiver to provide vehicle position, course and speed information. The GPS receiver shall also be used to set the internal DVR clock to the proper time and date so that all vehicles display and record proper time.	X	
The DVR shall include indicators visible outside of the vehicle to confirm that the system is recording and that the wireless audio transmitter is activated. This indicator does not need to be visible to occupants inside the vehicle.	X	
The DVR shall be capable of initiating a recording by both automatic and manual means. The DVR shall begin recording automatically when any of the following are activated:. ▪ Vehicle's emergency/pursuit lights; ▪ Siren, and ▪ The systems integrated crash sensor. (This activation shall include capturing the "look back" buffer memory to video-record the collision, should it be in view of the active camera	X	
The audio input associated with the forward-facing camera shall record audio using the internal microphone inside the vehicle. When the wireless audio transmitter/BWC is activated, the audio input shall be automatically switched to the wireless audio transmitter's microphone. The system shall automatically revert to the internal microphone when the wireless audio transmitter/BWC is deactivated.	X	
The DVR shall include a programmable pre-event recording mode allowing it to capture images a minimum of 30 seconds prior to the activation of the RECORD mode. Please specify pre-event recording capability of proposed DVR.	X	
The DVR shall be capable of capturing date/time, user identification information, emergency light indication, siren indication, speed indication (w/ radar interface), braking indication, and whether the microphone is activated. The information shall not be overlaid on the recorded video, and should be stored as secured metadata.	X	
The DVR shall allow video to be played back in the vehicle. When the DVR PLAY button is pressed a list of all prior recordings shall appear on the display screen provided.	X	
The DVR shall record video in a format that allows playback on multiple devices.	X	
The DVR shall provide a means to ensure the integrity of the recorded video has not been compromised. The video must be able to be authenticated at any time, including when it is played back outside of the police vehicle	X	
The DVR shall provide a means to ensure the integrity of the recorded video has not been compromised. The video must be able to be authenticated at any time, including when it is played back outside of the police vehicle.	X	
The Control Center/DVR firmware shall allow in-system programming for future updates. Please describe how updates are made.	X	
The DVR or related display (Mobile Data Computer, tablet etc.) shall have backlit controls for record; stop; play/pause; forward/reverse, fast forward/ reverse; trace, and lighted indicators for power on; record; and play.	X	

The power control switch shall allow the DVR to automatically power on after the vehicle's ignition is switched on	X	
The DVR shall automatically power down after the vehicle's ignition is turned off provided the DVR is not in "Record" and is not in the process of downloading files or other type of file save.	X	
The DVR should provide a means to tag an incident at the time it is recorded with a priority designation. Once a recording is stopped, the DVR should automatically prompt the officer to select from the pre-defined drop-down list(s).	X	
The DVR shall be capable of operating within the range of interior temperatures found within a law enforcement vehicle in Nevada without the need for supplemental heating or cooling. Specify your DVR's operating range and acceptability for the extreme temperature range in Nevada	X	

	Comply	
3.12.4 **COMPACT CCD COLOR CAMERA**	**Yes**	**No**
The low-light CCD color camera shall use a Sony EXview® HAD CCD or equivalent image sensor to provide high quality nighttime images while minimizing blooming and glaring from bright sources of light. Proof of "equal" shall be the responsibility of the bidder and shall be submitted with the bid if not using the Sony EX VIEW chipset.	3.12.4.1 Page 71-72	
The forward-facing camera shall be a solid state imaging system that is not subject to burn in, or interference by magnetic fields.	X	
The forward-facing camera shall operate within the range of temperatures from 0 to 120 degrees Fahrenheit or between -17.8 and 48.9 degrees Celsius	X	
The camera shall be compact so as not to obstruct the driver's forward or peripheral view thru the windshield, or provide any obstruction of factory installed airbags or mirrors.	X	
The camera shall be a single unit, including power lens, mounted on the windshield or roof of the vehicle and operate on 12 VDC power source.	X	
The camera shall provide a minimum field of view of 24 feet width at distance of 35 feet (40 degrees).	X	
The camera shall have manual and automatic focus capabilities, which are user selectable.	X	
The front camera should have a minimum 120X zoom (10x optical zoom with 12x digital zoom). Please specify _automatic/manual_ mode.	X	
The minimum LUX rating of the forward facing camera shall be rated at less than 1 LUX at full shutter speeds and 0.05 LUX in night view mode.	X	
The camera shall automatically adjust for varying light levels from day to night. The camera and lens will be equipped with auto focus, automatic exposure, and automatic white balance.	X	
The camera shall have a minimum color resolution of 450 horizontal lines	X	
All cameras shall default to auto focus. An override system should be configurable to prevent operation while the vehicle is in motion.	X	
The camera shall offer a signal-to-noise ratio of at least 46db.	X	

	Comply	
3.12.4 **COMPACT CCD COLOR CAMERA**	**Yes**	**No**
The camera shall have backlight compensation setting.	X	
The camera shall be compact. List the size and weight of the proposed CCD camera.	X	
The camera shall mount with a heavy-duty controlled pivot mount that does not obstruct the driver's field of view. Camera shall be able to be rotated 360 degrees and can pan and tilt to +/- 90 degrees. Adjustment shall require no tools.		X
An optional rear view camera shall be available.	X	

	Comply	
3.12.5 **BACK SEAT CAMERA SPECIFICATIONS**	**Yes**	**No**
The back-seat camera shall utilize a micro compact with wide angle 1/3" Super HAD image device (or equivalent) with approximately 420 lines of resolution. Proof of "equal" shall be the responsibility of the bidder and shall be submitted with the bid. This must be included in the system at no charge.	X	
The rear-facing camera shall be capable of being mounted covertly in the cab.	X	
The rear facing camera shall be capable of recording the entire rear seat area of the police vehicle.	X	
The rear-facing camera shall have a minimum lux rating of .03. Please specify the rating	X	
The rear-facing camera shall utilize infrared illumination to capture video in no-light conditions.	X	

	Comply	
3.12.6 **COMPACT COLOR LCD MONITOR**	**Yes**	**No**
The monitor shall be a full color high quality LCD, active matrix (TFT) screen that measures at least 3.0" measured diagonally.	X	
The monitor shall be capable of displaying a live picture from the camera when powered, even if recording is not in progress.	X	
The monitor shall operate between 32 and 120 degrees Fahrenheit.	X	
The monitor shall include a system speaker, with volume control, to provide monitoring of live audio or playback from all system microphones.	X	
The monitor shall have controls/indicators that mimic the DVR and include record; stop; play/pause; forward/reverse; brightness; volume; and power. The monitor should also include a button for disabling the monitor when the system in standby, and accessing a menu for programming.	X	
The monitor should have the capability to display: date/time, user identification information, emergency light indication, siren indication, latitude and longitude, speed (w/ radar interface), braking indicator and microphone activation indicator. The information shall not be overlaid on the recorded video; rather, it should be stored as external secure meta-data (or equivalent) in the video file.		X
The monitor should support a full-screen video mode (without the auxiliary data) using a single key press on the control center	X	
The monitor shall operate independently from the recording device. For covert	X	

	Comply	
3.12.6 **COMPACT COLOR LCD MONITOR**	**Yes**	**No**
operation it should possible to operate the DVR in RECORD mode with the monitor turned off.		
The monitor shall be provided with an adjustable mounting bracket that will allow it to be mounted in a variety of locations within the law enforcement vehicle.		X
The monitor shall have the capability to display the approximate amount of storage remaining on the media in an HH:MM format. An audible beep or other form of tone shall warn operator prior to or when there is 10%, or less, time remaining on the media.	X	

	Comply	
3.12.7 **MICROPHONES**	**Yes**	**No**
The system shall come equipped with a digital wireless microphone that is incorporated into the BWC and an in-car microphone. The in-car microphone shall be mountable anywhere within the vehicle.	X	
Audio from the interior microphone and the wireless microphone/BWC shall record on separate audio channels.	X	
The wireless microphone/BWC shall be self-contained and include a re-chargeable battery; mountable charger/docking station; internal microphone; internal antenna. Transmitters that rely on the microphone cable for an antenna, or which utilize an external antenna shall not be permitted.	X	
The wireless microphone/BWC system shall be FCC type accepted.	X	
The wireless microphone/BWC shall have a minimum effective operating range 1,000 feet under line-of-sight conditions.	X	
The wireless microphone/BWC must have a minimum stand-by battery life of ten (10) hours without recharging or additional batteries, with pre-record on.	X	
The wireless microphone/BWC should be capable of automatically activating the DVR system; additionally, the wireless audio transmitter/BWC shall be capable of being activated by the DVR system when a recording is started.	X	

	Comply	
3.12.8 **CONTROL CENTER SPECIFICATIONS**	**Yes**	**No**
The control center shall be compact in design and mounted overhead, or in the equipment console between the seats. .	X	
The control center shall not obstruct the driver's forward or peripheral view or provide any obstruction of factory installed airbags or mirrors.	X	
The control center shall not require any permanent modifications to the police vehicle.	X	
The control center shall accommodate the mounting of the front and rear-facing cameras, the monitor and keypad.	X	

	Comply	
3.12.9 **VIDEO VIEWING SOFTWARE/HARDWARE**	**Yes**	**No**
A video viewer/software shall be provided to allow recorded video files to be played on any computer and display date/time, user identification, emergency light indication, siren indication, latitude and longitude, speed (w/ radar interface), braking indication and the microphone activation indicator. This information shall not be overlaid on the recorded video; it shall be displayed outside the video frame.	X	
Support for this software shall include version updates provided free of charge for the lifetime of the system.	X	
Vendors shall provide all hardware (media readers/drives) and software necessary duplicate, share and present digital video in a court acceptable format. Please describe transfer steps needed to convert captured video to court acceptable evidence without the need for a server based infrastructure.	X	
The video management software should be capable of converting a video from the proprietary format to the standard DVD Video format, and authoring a DVD capable of being played in a standard DVD player.	X	

	Comply	
3.12.10 **SERVER BASED VIDEO MANAGEMENT SYSTEM (VMS) Backend (Optional)** Vendors may propose systems with a server based digital evidence management, but are not obligated to do so. If a server based Video Management Software System (VMS) component is proposed the following specifications apply.	**Yes**	**No**
The server based VMS should include server infrastructure in our Northern, Southern, and Central regional command offices and assume manual downloading of all rural substations into the regional command centers to which they report (see Table 1.2.A).	X	
The server based VMS shall be a turn-key component and fully installed, serviced, warranted, and maintained by the vendor.	X	
The server based VMS should include RAID-5 video storage servers or equivalent for all regional offices to capture video information, workstation(s) for managing and viewing stored video, equipment racks to mount equipment, and uninterruptible power supplies (UPS).	N/A	
The server based VMS should provide a configurable DVD archive unit that can automatically archive video copies based on set parameters, and copy video files to a DVD-Video or equivalent court acceptable format.	X	
Pricing for the server based VMS shall be provided on the Pricing Schedule in the vendor's response. Pricing must be included for all proposed hardware (workstations, servers, archiving hardware, video back up systems, access points), wiring, software, installation, configuration, and training.	X	
If a server based video management back office component is proposed, a schematic of the back end infrastructure shall be included with responses to the RFP.	N/A	
The server based VMS file storage shall be equipped with sufficient storage	N/A	

	Comply	
3.12.10 **SERVER BASED VIDEO MANAGEMENT SYSTEM (VMS) Backend (Optional)** Vendors may propose systems with a server based digital evidence management, but are not obligated to do so. If a server based Video Management Software System (VMS) component is proposed the following specifications apply.	**Yes**	**No**
to comfortably manage video that would be generated from cars depicted in the scope of work in this RFP. Please list and itemize the size of proposed storage for each regional command center identified.		
If wireless downloading capability is proposed for vehicles assigned to each regional office, provide download times for video captured based on the video compression and resolution capabilities of proposed cameras, the proposed number of access points, and the proposed servers/wiring infrastructure.	3.12.10.9 Page 80	
The server based VMS shall include a database that contains a record for each recorded video file. The database shall store sufficient information to support the search capabilities and provide chain-of-evidence documentation.	X	
The server based VMS shall be capable of searching stored video files by: department ID, time, date, officer ID, vehicle ID, camera, recording mode, and status (online or archived).	X	
The server based VMS shall be capable of providing custom fields that may be used to store department-defined information (e.g. suspect's name, license plate number, etc.)	X	
The server based VMS should allow videos to be categorized using department-defined drop-down lists. This classification shall be used for searching and to define how long each category of video is to be kept before it is automatically deleted.	X	
The server based VMS shall provide a means to ensure the integrity of the recorded video. Video integrity must be checked when the video is uploaded, anytime it is played back or archived, and shall be verifiable on demand.	X	
The server based VMS shall provide the capability to duplicate, share and present digital video in a court acceptable format. Describe the transfer steps, if any, needed provide video to the courts as acceptable evidence. Describe the way and format the proposed system archives recorded video files, and how these files will be stored and backed up for safeguarding.	3.12.10.15 Page 81	
When a video file is copied or archived to digital media, the Video Management Software shall store a unique archive ID and maintain a virtual directory to recall the archived video file(s).	X	
The Video Management Software shall be capable of converting a video from the proprietary format to the standard DVD Video format, and authoring a DVD capable of being played in a standard DVD player.	X	
The support for this software shall include version updates and be provided free of charge to the agency for the lifetime of the system.	X	

	Comply	
3.12.11 **CONTROL CENTER SPECIFICATIONS**	**Yes**	**No**
An optional radar interface shall integrate directly with the Agency Bee III radar equipment. Collected information shall include speed of the target, the "locked" target speed, and the patrol vehicle.		
The State is interested in a system that can be configured for motorcycle use. All of the specifications described for the DVR and wireless microphone shall be applicable. Is a motorcycle option available for your solution? If so, does the configuration utilize a weatherproofed monitor and camera? Please explain.		X

	Comply	
3.12.12 **OFFICER SAFETY**	**Yes**	**No**
All equipment shall be capable of installation in the following vehicles while still meeting the other requirements stated herein: Chevrolet Tahoe, Dodge Charger, Ford Interceptor Utility/Sedan and Ford F150 Pick-up.	X	
Describe dimensions and vehicle mounting options for your camera, recorder, wireless microphone, transmitter/ receiver and any other required equipment.	3.12.12.1 Page 82	
Equipment must not be installed in such as manner as to interfere with a passenger in the front passenger seat.	X	
No part of the system shall interfere in any way with the driver's field of view. The camera shall be a single unit, including power lens, mounted on the windshield or roof of the vehicle and operate on 12 VDC power source All connections to the camera, for power and video, shall be made by a single cable that attaches using a quick release connector.	X	
The in-car system shall be protected from damage due to input of voltage, reverse polarity, and electrical transients that may be encountered.	X	
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.	X	
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 as referenced in the In-Car Video Camera Systems Performance Specifications - Digital Video Systems provided by the International Association of Chiefs of Police. (11/21/2008).	X	
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.	X	
System components shall be capable of being illuminated for ready identification during periods of darkness. The illumination level shall be capable of being controlled over a range from bright to dark.	X	
All wiring shall meet industry standards applicable to the wire application including Underwriters Laboratory (UL) as well as the Society of Automotive Engineers (SAE).	X	
Manufacturers shall provide information in their installer's guide or owner's manual that specifies the proper wiring, fuses, connectors, connection points	X	

	Comply	
3.12.12 **OFFICER SAFETY**	**Yes**	**No**
with the vehicle electrical system and grounding points.		
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	X	
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.	X	
The In Car Video System shall operate on a power source that is filtered, regulated, and short-circuit protected. The voltage supplied to the In Car Video System components shall meet the manufacturer's specifications and shall not vary with fluctuations of the vehicle's electrical system of between 9 and 18 volts.	X	

	Comply	
3.12.13 **RELIABILITY**	**Yes**	**No**
The video systems shall maintain consistent audio/visual recording quality. The in-car recording system shall not be affected by transmissions from the police communication or interference from the following sources: high-powered television stations; other radio frequency interference (e.g. UHF, VHF & HF); automobile alternator, ignition, electrical systems; automobile heaters / air conditioner fan motors; or other patrol vehicle electrical systems.	X	
All equipment shall have a lifecycle of at least 3 years under law enforcement agency usage, or have replacement coverage under warranty and maintenance. Please provide expected lifecycle for all video system components.	X	
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	X	
Loss of power to the system shall not cause loss of any recorded data or result in the unit requiring reprogramming, reloading of software or operating system software.	X	
The video system shall be able to return to a "ready to record" mode after sudden loss of power without requiring user intervention.	X	
The system's timekeeping device and the vehicle's identifier shall be protected by a system battery backup to prevent loss of information in the event the vehicle battery is disconnected for up to a minimum of fourteen (14) days.	X	
Date and time within video system shall be self-adjusting for daylight savings time and leap years.	X	
The video system shall have self-charging backup battery that continues recording upon loss of power, and should gracefully shutdown prior to available power being exhausted. The battery backup that shall power the system for at least 2 minutes following loss of the vehicle's battery power.	X	

	Comply

3.12.14 **TRAINING/DOCUMENTATION**	**Yes**	**No**
The vendor shall offer and provide, at no additional cost, training to all end users on the use of the video system and video viewing software	X	
The vendor shall offer and provide, at no additional cost, training to electronic technicians at their Reno, Elko, and Las Vegas shop locations. This training will ensure proper operation, repair, and maintenance of the manufacturer's video system.	X	
A system administrator class covering all aspects of the system shall be given at all the DPS/HPD Regional Command sites (Reno, Elko, and Las Vegas) upon award.	X	
Trainers must be experienced instructors who are thoroughly familiar with all technical aspects of the system.	X	
Provide a course syllabus for training classes to be provided with your RFP response.	X	
Vendor shall include documentation for procedures on regular maintenance of video system components.	X	
Vendor shall provide complete service manuals and service bulletins on all electronic components.	X	
Vendor shall provide documentation of system that includes identification of all vehicle equipment and the physical configuration; all configurable system parameters; written installation instructions, user manuals; and system administrator manuals instructions covering the change of all configuration settings.	X	

3.11 Scope of Work Body Worn Camera (BWC)

3.11.1 The State of Nevada is seeking a qualified vendor that can provide at a minimum, the following

3.11.1.1 A Video Management System (VMS) that is either an externally hosted cloud-based data storage solution with the capability of organizing/managing video/digital evidence, server based or consist of a hybrid solution and be accessible via the internet to multiple users simultaneously. The State prefers the Cloud or Hybrid solution. The system must meet the State's geographical needs as described in this RFP.
Digital Ally is proposing VuVault.com, an externally hosted cloud-based Video Management System and data storage solution.

3.11.1.2 Up to 489 high quality Body Worn Cameras necessary to outfit 465 sworn (Lieutenants and below) with 5% spares.
Digital Ally can provide at a minimum up to 489 high quality Body Worn Cameras necessary to outfit 465 sworn with 5% spares.

3.11.1.3 The VMS shall have the ability to convert video to a portable media device i.e.: (DVD, external hard drive) without compromising its authenticity to include all metadata and chain of custody requirements.
Video exported from VuVault.com to a rewritable portable media device there is not a way to ensure the chain of custody requirements past the video being exported. All Chain of Custody reports will include who exported the video and metadata to the media device.

3.11.1.4 Full service vendor support including installation, maintenance/support, warranty, training, documentation, and project management throughout the contract period.

Digital Ally provides full service vendor support including installation, maintenance/support, warranty, training, documentation, and project management throughout the contract period.

3.11.1.5 All-inclusive pricing for all hardware (body worn cameras, workstations, servers, archiving hardware, video back-up systems, access points, automatic triggering devices, connectivity (Ethernet wiring), and software (system, database, and video management) installation, configuration, and training).
Digital Ally has provided all these costs in Attachment H.

3.11.1.6 Proposed systems that consist of server based video evidence management must be turn-key and provide warranties and full service maintenance and support on all hardware, wiring infrastructure, and software for a period of five (5) years.

Digital Ally is not proposing a server based video evidence management.

3.11.2 Body Worn Cameras

Specifications are provided by area including BWC Hardware Requirements, Evidence Managements System, Video Storage, System Security, Information Security, In-car Video Integration, Training and warranty.

3.11.3 BWC Hardware Requirements

3.11.3.1 Cameras worn by officers shall be lightweight, preferably six ounces or less in total combined weight.
The FirstVu HD has a total weight of 3.9oz.

3.11.3.2 Cameras shall have minimal wiring, not exceed two wires or cables and shall be designed to disengage to prevent the wearer from becoming entangled.
The FirstVu HD camera module and DVR/battery are connected via a USB cable designed to break away if forcibly removed from the operator's person to prevent the wearer from becoming entangled.

3.11.3.3 Cameras shall have recording capability of at least ten continuous (10) hours (the State would prefer twelve (12) hours of continuous recording capability).
Each FirstVu HD includes 32 GB of solid state storage space capacity. The maximum recording storage time is 25 hours if set in high definition and 54 hours if set in standard definition.

3.11.3.4 Cameras must have a minimum stand-by battery life of ten (10) hours without recharging or additional batteries, with pre-record on.
Each standard battery has up to 4.5 hours of continuous record time with pre-event enabled. The optional extended battery has up to 8 hours of continuous record time with pre-event enabled.

3.11.3.5 BWC Shall be user friendly that can be activated easily during times of stressful events.

The FirstVu HD can be activated by pressing the start/stop record button on the camera module. It can also automatically activate from external trigger events, such as car door opening, siren activation, etc. with the hands-free body camera activation system, VuLink. VuLink can automatically or manually start recordings on the FirstVu HD from customizable vehicle recording triggers allowing for easy activation during times of stressful events.

3.11.3.6 BWC should have automatic triggers, as a standalone system.

The FirstVu HD and VuLink work as a standalone system for automatic triggering of video recording. Recordings can be triggered by siren activation, light bar activation, speeding and more.

3.11.3.7 Rechargeable battery must be able to reach full charge, from no power, in no more than six (6) hours.

The FirstVu HD takes approximately 4 hours to reach a full charge from no power to full power after the initial 8-10 hour charge.

3.11.3.8 Cameras must have a minimum of thirty-two (32) GB internal/integrated memory and storage media not be removable.
The FirstVu HD has 32 GB of secure, internal, non-removable, solid state memory.

3.11.3.9 Rechargeable battery must be able to withstand at least three hundred (300) charging cycles, maintaining the 10 hour record time.
The FirstVu HD battery will typically perform 3-5 years before needing replacement.

3.11.3.10 BWC lens must have a field of view from 95 to 145 degrees.
The FirstVu HD has a field of view of 130 degrees.

3.11.3.11 The recording speed shall be no less than 30 frames per second (fps).
The FirstVu HD records in a maximum of 30 frames per second.

3.11.3.12 Camera shall record video images in full color with a minimum resolution of 640 pixels x 480 pixels. Adjustable resolution is preferable.
The FirstVu HD records in 720p (1280x720) or VGA (640x480) with configurable quality settings.

3.11.3.13 Video compression shall be H.263 or higher
The FirstVu HD's compression is H. 264 with configurable quality settings.

3.11.3.14 Cameras shall have multiple mounting options to accommodate varying uniformed officers, plain-clothed officers, and tactical field situations. Examples include, but are not limited to, lapel, shoulder, eyeglasses, cap, helmet, holster, button shirt, zipper shirt, utility belt, snow suit etc. Mounts shall not require modification to current in-service uniforms.
The FirstVu HD kit includes the following mounting options: Velcro mount, fabric clip, and button mount. There is an optional helmet mount.

3.11.3.15 Camera should allow for on scene (in the field) viewing? If so, describe the ability to playback or view video.
On scene viewing with the FirstVu HD can be accomplished through Digital Ally's VuVault GO mobile application for Android and iOS. The app allows for full system control including the ability to live view the video feed as well as the ability to view the remaining storage space and battery life. Connection to the FirstVu HD is done via WiFi tethering.

3.11.3.16 Camera shall provide feedback to user when activated, either via a visual indicator or audible tone.

The FirstVu HD has a Red Record LED light. This light will illuminate when recording has started.

3.11.3.17 Camera shall have the ability to be set to stealth mode while in the field.
The FirstVu HD has a red LED indicator that visually indicates recording. Stealth mode will disable the LED indicator and only send one vibration pulse every 15 seconds to indicate recording.

3.11.3.18 Camera must have an indicator that shows current operating mode.
The FirstVu HD has LED lights that indicate the operating mode. The red LED indicates the camera is in recording mode. The orange LED light indicates that the camera is in data upload mode. The blue LED indicates that the camera is in charging mode.

3.11.3.19 If the camera offers night vision enhancement, the State shall have the ability to enable or disable it.
The FirstVu HD does not have a night vision enhancement option; however it is have a 0.08 Lux Low light sensitivity for better night time operation.

3.11.3.20 The System should provide automatic indexing functionality of video files and be capable of interfacing with existing computer-aided dispatch (CAD) vendor.
Digital Ally has an Application Program Interface (API) that can be utilized to connect to other vendor software. We would have to create a service contract and determine the development time needed to integrate our system with the State's existing CAD system. Digital Ally will work with the State to determine exactly which features and information need to integrate with our systems. This level of integration will determine what the final cost will be.

3.11.3.21 Cameras shall automatically embed a time/date stamp in the recorded video.
All videos taken with the FirstVu HD will automatically be embedded with a time/date stamp.

3.11.3.22 Cameras shall prevent users from deleting recorded files without authorization.
The System Administrator can set security permissions for all users in VuVault.com and can prevent users from editing or deleting recordings both before and after they have been uploaded in VuVault.com.

3.11.3.23 Camera should have a method for adding desired metadata to video in the field prior to upload.
Digital Ally's VuVault GO mobile application can be utilized to view and tag video with desired metadata in the field prior to upload.

3.11.3.24 Officers should have the ability to playback or view video in the field on mobile cameras and/or MDC's (Panasonic FZ-G1 Tablet) wirelessly (i.e. Bluetooth).
Officers have the ability to playback or view video from the FirstVu HD in the field wirelessly via WiFi tethering to Android or iOS devices. The VuVault Go mobile application is not compatible with Windows devices at this time.

3.11.3.25 Camera shall have a pre-event record feature (BWC should capture at least thirty (30) seconds of video prior to officer initiating the recording). Adjustable times are preferable.
The FirstVu HD has a pre-event record feature of up to 60 seconds of video prior to an officer initiating a recording. This is adjustable from 0-60 seconds.

3.11.3.26 Camera will export in a standard, open format, such that it can be replayed in freely available software without processing or conversion. Proprietary data formats shall not be accepted.
FirstVu HD video is recorded in AVI format.

3.11.3.27 The vendor must offer a multi-dock station capable of uploading digital evidence from multiple cameras simultaneously and have the capability to upload video via Wi-Fi and/or cellular LTE connectivity. If via cellular, product should be compatible with Fenny Wireless Skyus X modem.
Digital Ally's Docking Station comes standard with a wired connection, but can work with the Fenney Wireless Skyus-X modem, provided there is an open connection directly to it, or a switch port available.

3.11.3.28 The multi-dock station must charge the camera batteries, securely transfer files without loss of quality or metadata, and delete the files from the camera once transferred to the evidence management system.
The Docking Station provides automated, simultaneous uploading and charging for up to 12 FirstVu HD devices plus 12 external batteries. All video and metadata files are transferred from the FirstVu HD devices and deleted from the FirstVu HDs, and then an integrity check is done to authenticate the SHA hash of each file. Once it has been verified that all files are uploaded in their full quality, the videos will be deleted from the Docking Station.

3.11.3.29 The multi-dock station should not require a department computer to operate, connect or interface with the Internet (e.g. the multi-dock station should be a standalone device that connects to the cloud storage solution or server via an Ethernet connection).
The Digital Ally Docking Station is a standalone device that connects to the cloud storage solution via an Ethernet connection.

3.11.3.30 The camera should not cause electromagnetic interference with nearby airwave radios (and other electronic equipment and radio communication systems).
The FirstVu HD does not cause electromagnetic interference with nearby airwave radios and other electronic equipment and radio communication systems.

3.11.3.31 Loss of power to the camera must not cause data to be lost/corrupted.
Loss of power on the FirstVu HD will not cause data to be lost/corrupted.

3.11.3.32 Cameras will be ruggedized. Cameras shall be able to survive a six-foot drop test. Cameras shall be able to operate at minimum temperature of -12 degrees Fahrenheit and a maximum temperature of 130 degrees Fahrenheit.
The FirstVu HD has been drop tested onto a hard surface from 6 feet and has an operating temperature of -4 degrees to +158 degrees Fahrenheit and a storage temperature of -40 degrees to +176 degrees Fahrenheit.

3.11.3.33 Vendor will state camera's Ingress Protection (IP) rating. The State prefers an IP rating of IP67.
The FirstVu HD has an IP rating of IPX5.

3.11.3.34 Describe what features devices have in place to prevent accidental activations of camera by the user (without the need for accessories or alteration of equipment by user).
The FirstVu HD's record button is on the side of the camera module and must be pushed in to begin recording, making for it difficult for accidental activation to occur.

3.11.3.35 Vendor shall define the required time for automated indexing (specific time frame after upload of video evidence) and any expected error rate percentage upon indexing, if applicable.

Once videos are uploaded to VuVault.com they are immediately ready to be viewed, searched, tagged, etc. there is no buffer time. The expected error rate percentage upon indexing is 0%.

3.11.3.36 The vendor must state the transfer rate of video from the multi-dock station to the cloud in sixty or thirty-minute increments. Vendors shall break down transfer rates by video quality (i.e. Hi Def).
Transfer rate of video from the multi-dock station to the cloud is directly dependent on the speed of the State's network.

3.11.3.37 Describe device wireless activation features (e.g. device is automatically activated with the activation of patrol vehicle's light bar), if applicable.

Digital Ally's VuLink is the first patented product on the market that can link multiple body cameras, in-car video systems, or activate off of triggers with a body camera. With the VuLink an officer can simultaneously start their FirstVu HD and their In-Car Video system, or simultaneously activate their body worn camera with the light bar, siren, microphone, etc.

3.11.4 Maintenance & Repairs (Hardware)

3.11.4.1 Vendor shall propose and provide a detailed description of the maintenance services that are available once the one-year warranty has expired.
Digital Ally provides a 1-year warranty/maintenance agreement on the FirstVu HD body worn camera. The warranty includes any defects in materials or workmanship on all system components as well as all software upgrades not requiring hardware revisions. Extended 1 and 5 year warranties are available for additional purchase. The FirstVu HD is a completely solid state device that does not require any scheduled maintenance. The warranty/maintenance period will begin from the date of installation.

3.11.4.2 Vendor shall provide on-site repair services as required.
Digital Ally will provide on-site repair services as required.

3.11.5 Video Management System

3.11.5.1 Vendors must be able to provide documentation establishing that their technology has undergone rigorous field testing by an independent and relevant scientific body. This documentation must be provided with the vendor's proposal response.
The documentation of the field testing by an independent and relevant scientific body has been provided on page 123.

3.11.5.2 Vendors shall be willing to provide an expert witness to testify in a court of law, to support court cases utilizing video from their BWC System, at a reasonable fee. Vendors must specify hourly rate for expert witness testimony within ***Attachment H ~ Cost***.
Digital Ally can provide testimonial support in legal proceedings only regarding the technical specifications of our equipment.

3.11.5.3 VMS shall either be an externally hosted cloud-based data storage solution with the capability of organizing/managing video/digital evidence, server based or consist of a hybrid solution and be accessible via the internet to multiple users simultaneously. The State prefers the Cloud or Hybrid solution.
The VMS that Digital Ally is proposing VuVault.com, a cloud solution hosted by Amazon Web Services (AWS). VuVault.com is capable of organizing/managing video and digital evidence.

3.11.5.4 VMS shall allow for remote access with complete functionality (review, enter metadata and send video) with NHP mobile devices and/or computers.
VuVault.com is a cloud based solution that can be accessed with valid sign in credentials from any device with a supported browser.

3.11.5.5 VMS shall provide an automatic audit trail for when files and videos are accessed.
VuVault.com will generate a log of all recordings, deletions, edits, and every action associated with a recorded event. A chain of custody report can be generated showing a log for each recording.

3.11.5.6 VMS shall allow officers to enter additional metadata to recorded files, such as notes or comments.
VuVault.com allows users with appropriate permissions to enter additional metadata to recorded files, such as notes or comments.

3.11.5.7 Solution must support all major digital file types (avi, jpeg, mpeg, etc.).
Any file type on a PC or a Mac can be uploaded into a case file in VuVault.com.

3.11.5.8 VMS shall provide remote viewing of the stored video based on the permissions granted by the System Administrator.
At this time live viewing of video on the FirstVu HD is only available through the VuVault GO mobile application.

3.11.5.9 VMS shall allow users to search video files by name, date of recording, date of upload, case number (CAD-generated), device number, as well as categorize and add notes to each file within the solution.
VuVault.com allows users to search video files by name, date of recording, date of upload, case number, device number, as well as categorize and add notes to each file within VuVault.com.

3.11.5.10 VMS must allow System Administrators the ability to grant access of specific files to specified persons for a specific period of time.
VuVault.com allows System Administrators to grant access of specific files to specified persons which can be changed at any time.

3.11.5.11 VMS shall have the ability to share files internally and externally via secure links over the Internet.

VuVault.com includes an extensive, secure and flexible share portal to facilitate convenient sharing of video evidence and case files with designated and credentialed third parties. This functionality can be used on a one off basis by the issuance of one time credentials or can be configured to allow regular and continued access by known and trusted third parties i.e. the prosecutor and staff. These third parties will have the option, if given privileges per share, to review and/or download files in native format to solid state memory. No proprietary player is needed to review video and audio post download.

3.11.5.12 When videos are exported to a portable media device, all metadata shall transfer over without compromising its authenticity.
Data can be exported from VuVault.com in a MP4 non-proprietary format. Exporting video also exports the metadata as well, without compromising its authenticity.

3.11.5.13 VMS shall grant System Administrators the ability to set variable retention rules per DPS/HPD preferences.
The retention period for a video can be set to begin with a date or event stored in the VuVault.com cloud system. The date or event can be utilized to calculate the date on which the video will become eligible for destruction. Triggers and other metadata cannot be utilized to set retention at this time.

3.11.5.14 VMS shall have the ability to set time tables for automatic deletions of files.
VuVault.com gives the system administrator the ability to set time tables for automatic deletions for files.

3.11.5.15 VMS should have the ability to recover deleted evidence within a minimum of seven (7) days of deletion. The State would prefer a recovery period of 30 days.
When video is deleted from VuVault.com, every copy, including the original unedited version, will be completely expunged from the system. VuVault.com has the option to set a recovery time for deleted videos. The recovery time period is configurable and allows the option to recover any video that has been deleted. After the recovery time period has expired, deleted video cannot be recovered by Digital Ally or Amazon Web Services.

3.11.5.16 The VMS will maintain a log/audit trail illustrating users who have viewed and copied video to an external source (e.g. DVD/ long term storage).
VuVault.com will maintain a log/audit trail illustrating users who have viewed and copied video to an external source.

3.11.5.17 VMS must have the ability to preserve the raw file without editing.

In VuVault.com users with appropriate permissions can edit videos. When edits have been made to a video, a new file is created under the event of the original video, never altering the original file.

3.11.5.18 VMS must securely store all videos and recordings in a way that only State-authorized users and users authorized by DPS/HPD can view.
VuVault.com can be accessed virtually anywhere with an internet connection only with the proper login credentials.

3.11.5.19 VMS must provide redundant, security back-up of all data.
Ensuring your data will always be protected and accessible is our number one priority; that is why we have built VuVault.com on the most trusted web service around. Amazon Web Services supplies three locations separated on the east and west coasts where all of your data will be copied and 100% secured. If one of the locations is wiped out by a natural disaster, your information will still be secured in two alternate locations states away. Any and all of the information that was flowing to that particular location will be directed to substitute locations.

3.11.5.20 VMS should offer redaction capabilities.

VuVault.com features a nearly automated redaction feature. This feature allows the user to redact faces and facial features so that the video can be released as needed by the user. VuVault.com also features an intuitive manual redaction tool as well, which allows for the redaction of other items such as license plates, addresses, t-shirts, and other items as needed.

3.11.5.21 VMS must be compatible with at least Windows 7 Professional Operating System or more recent versions) and Internet Explorer Version 11 web browser or more recent version(s).
VuVault.com is compatible with these.

3.11.5.22 Provide the minimum required memory (RAM), if applicable.
VuVault.com is a hosted solution and does not have a minimum required memory.

3.11.5.23 Provide the minimum required processor speed, if applicable.
VuVault.com is a hosted solution and does not have a required processor speed.

3.11.5.24 Provide the minimum network speed to upload videos, if cloud based.
The FirstVu HD docking station and the DVM-800 in-car system does not have a minimum network speed to upload videos.

3.11.5.25 Upload times to the VMS will be defined in per hour or thirty-minute increments of video files.
Upload times to the VMS is directly dependent on the State's network speeds and video file sizes.

3.11.5.26 Any required or expected ‘buffering’ times before video files are accessible in cloud storage (for view or adding metadata) will be clearly defined.
There is no buffering time before video files are accessible in cloud storage; once the video is uploaded to the cloud it is available for tagging, editing, etc.

3.11.5.27 Describe System compatibility with mobile devices (iPhones and Android).
Digital Ally's mobile application is compatible with Android and iOS mobile devices.

3.11.5.28 Vendor shall indicate the number of searchable fields in storage system and any ‘wild card’ searches that can be done to locate stored data.
There are several standard search criteria already implemented into VuVault.com such as date/time, event id, user id, event type, along with an unlimited customizable metadata fields to make finding recordings fast and easy.

3.11.5.29 Users should have the ability to send email messages from hosted solution interface to end users.
VuVault.com has a built in messing system that allows interface to end users.

3.11.5.30 VMS should send System Administrators administrative notifications when evidence files are about to be deleted.
VuVault.com will send System Administrators administrative notifications when evidence files are about to be deleted.

3.11.5.31 VMS should send System Administrators administrative notifications when users need their credentials reset due to failed log on attempts.
VuVault.com will send System Administrators administrative notifications when users need their credentials reset due to failed log on attempts.

3.11.5.32 VMS should offer auto-redaction capabilities, to include high-movement and low light video; preferred to minimize the amount of time to redact 30 fps for the entire length of video.
VuVault.com's redaction feature is highly automated with face suggestion and includes intuitive, manual redaction tools. With these manual redaction tools, signs, shirts, license plates, etc. can be redacted. VuVault.com also provides the ability to download or share your redacted video online. Redaction capabilities include high-movement and low light video, and will redact 30 fps for the entire length of video.

3.11.5.33 VMS should have the ability to capture data, report on video statistics and provide custom reports.
VuVault.com has the ability to capture data, report on video statistics and provide custom reports.

3.11.6 Video Storage

If cloud based, the storage facility must be located within the continental United States.

3.11.6.1 Does your storage solution have the ability to upload video from multiple camera units simultaneously?
Yes, VuVault.com has the ability to upload videos from multiple cameras units simultaneously.

3.11.6.2 Storage solution should have the ability to view multiple linked videos simultaneously.
Simultaneously recorded videos and their audio will be assembled and can be displayed in a dual-view layout in VuVault.com.

3.11.6.3 Solution should have two tier storage capacity for active video and long term storage needs as defined by the State.
VuVault.com does offer two tier storage capacity for active video and long term storage needs as defined by the State.

3.11.6.4 Does proposed solution offer storage options for ‘unlimited storage’ of body camera video evidence?
Digital Ally can provide the State a quote for unlimited storage at the State's request.

3.11.6.5 Does your system provide a method to upload videos, via an access point? Please describe your process.
The DVM-800 in-car video system allows the State to upload videos via an access point. When officers pull into the access point's range the DVM-800 will automatically connect and wirelessly upload videos. The FirstVu HD body worn cameras do not have the ability to upload videos via an access point at this time.

3.11.6.6 Is your system compatible with an EnGenius ENS500EXT access point?

Yes, the hardware and software of the proposed system is compatible with an EnGenius ENS500EXT access point.

3.11.6.7 Does solution have the ability to maintain and export audit trail along with video?

Yes, VuVault.com has the ability to maintain and export audit trail along with video.

3.11.6.8 Define maximum storage capacity, if any.

VuVault.com's storage capacity limit is directly dependent on the storage plan option the State chooses.

3.11.6.9 Describe the capability of proposed solution to provide the State with the ability to export/download and migrate original recordings with all metadata to other storage media or, local storage inclusive of all metadata and chain of custody information.

Videos in VuVault.com can be shared through the share portal. VuVault.com includes an extensive, secure and flexible share portal to facilitate convenient sharing of video evidence and case files with designated and credential third parties. All metadata and chain of custody information is available through this exportation option.

3.11.6.10 Describe archival, hot and cold cloud storage solutions.

Videos in hot storage are kept in AWS's "active" storage and are available for immediate playback. Cold storage acts as archival storage. After the primary Active or "hot" retention period of 30 days, the videos are automatically moved to the cold storage, unless specifically marked by the end user. Videos in cold storage are available within 2 hours upon request.

3.11.6.11 Describe archival solutions for server storage if applicable.

Digital Ally is not proposing a server solution. Not applicable.

3.11.6.12 Discuss different cost savings as defined by various storage solutions (active vs. long-term storage of files).

Various storage solutions are shown in Attachment H.

3.11.6.13 Describe capability to respond to requests to pull video from 'cold cloud storage', including time required to download video from storage.

Videos can be pulled from cold cloud storage in a period of 4-24 hours.

3.11.6.14 Describe your solution to upload video in the rural areas that only have a maximum broadband speed of 1.5 Mbps
Digital Ally's solution to upload video in the rural areas that only have a maximum broadband speed of 1.5 Mbps remains the same as in places with faster broadband speeds.

3.11.7 System Security

3.11.7.1 The VMS shall meet the minimal security requirements for the Criminal Justice Information Services (CJIS) Policy. In particular, the VMS shall comply with Policy Areas 2 through 13 in Section 5 of the CJIS Policy. The CJIS Policy can be viewed by accessing the following link: https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center
VuVault.com is completely CJIS compliant through Amazon Web Services.

A. Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (section 5.5.6 Remote Access found in the above link)
VuVault.com is completely CJIS compliant through Amazon Web Services.

3.11.7.2 Will advanced authentication (AA) be required for access to CJI within a cloud environment (Section 5.6.2.2 Advanced Authentication, 5.5.2.2.1 Advanced Authentication Policy and Rationale found in the link under 3.11.7.1)
VuVault.com requires advanced authentication for access to CJI within the cloud environment.

3.11.7.3 Does your cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (Section5.9.1 Physical Secure Location found in the link under 3.11.7.1)
VuVault.com's cloud service provider's, Amazon Web Services, datacenter(s) used in the transmission and storage of CJI meet all the requirements of a physically secure location as specified in section 5.9.1 Physical Secure Locations found in the link under 3.11.7.1.

3.11.7.4 Are the encryption requirements being met? (Section 5.10.1.2 Encryption found in the link under 3.11.7.1)
VuVault.com meets the encryption requirements in section 5.10.1.2 Encryption find in the link under 3.11.7.1.

3.11.7.5 Who will be providing the encryption as required in the CJIS Security Policy? (Client or cloud service provider)
Amazon Web Services cloud service provider will be providing the encryption as required in the CJIS Security Policy.

3.11.7.6 Is the data encrypted while at rest and in transit?

Yes, VuVault.com provides, at a minimum, encryption in transit of Secure Socket Layer (SSL) 1024 bit key or better and at rest Advanced Encryption Standard (AES) 265 bit or better.

3.11.7.7 What are the cloud service provider's incident response procedures? (Section 5.3 Policy Area 3: Incident Response found in the link under 3.11.7.1)

Amazon's Web Services (AWS) data centers utilize innovative architectural and engineering approaches. Each data center is equipped with fire detection and suppression, power failure back-ups climate and temperature controls, and electrical and mechanical management. When a storage device reaches its end of life security measures are taken by Amazon to ensure that data is not exposed to unauthorized individuals. Amazon security platforms also host around the clock surveillance to ensure data locations are secure. In case of failure, automated processes move data traffic away from the affected area to an alternate secure location. AWS is designed to tolerate system or hardware failures with minimal to no impact to users.

3.11.7.8 Will the cloud subscriber be notified of any incident?

Yes, the cloud subscriber will be notified of any incident.

3.11.7.9 If CJI is compromised, what are the notification and response procedures?

Once aware of the compromise Digital Ally will notify all clients via email.

3.11.7.10 Is the cloud service provider a private contractor/vendor?

Yes, Amazon Web Services is a private contractor/vendor.

3.11.7.11 If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI. (Section 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors found in the link under 3.11.7.1)

Yes, Amazon Web Services is subject to the same screening and agreement requirements as any other private contractors hired to handle CJI.

3.11.7.12 Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? (Section 5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA found in the link under 3.11.7.1)

Yes, Amazon Web Services will allow the CSA and FBI to conduct compliance and security audit. Any past audits can be found on their website.

3.11.7.13 The State may verify that Contractor is in compliance with CJIS by requesting a compliance audit of Contractor's technology deployment through the CJIS Systems Agency to the Federal Bureau of Investigation (FBI). The FBI CJIS Division shall perform the requested audit to verify compliance. 140-2.
Amazon Web Services (AWS) is compliant and undergoes regular audits to verify compliance.

3.11.7.14 System shall provide full conformance to Federal Information Processing Standards (FIPS) Publication.
Amazon Web Services fully conforms to Federal Information Processing Standards (FIPS) Publication.

3.11.7.15 VMS shall provide user authentication with a unique username and password.
Yes, VuVault.com will assign each user a personal username and password to access the system.

3.11.7.16 VMS will allow for authorized users to be established based on various roles and permissions by the System Administrator.
Yes, VuVault.com allows the System Administrators to give or revoke permissions to users based on various roles and permissions. These settings can be changed at any time by the System Administrator.

3.11.7.17 VMS will offer optional IP access restriction and security challenge questions upon access from an unknown or previously used location.
VuVault.com allows for the System Administrator to restrict access based on the IP address and security challenge question upon access from an unknown or previously used location.

3.11.7.18 Any access to stored video shall be maintained in an automatic log or audit trail showing users that have viewed, shared or copied video to an external source (e.g. CD/DVD, local storage, etc.), and the audit trail should be capable of being exported.
Yes. VuVault.com will create a Chain of Custody report reflecting these things.

3.11.7.19 Log activities performed by specific user ID, IP address and time/date stamp all activities.
Yes, VuVault.com will keep logs of activities performed by specific user ID, IP address and time/date stamps all activities.

3.11.7.20 System Administrators shall have the ability to administratively manage accounts and assign rights and permissions to system users.
VuVault.com gives System Administrators the ability to manage accounts and assign rights and permissions to system users.

3.11.7.21 VMS shall provide ability to set an unsuccessful access attempt limit and suspend IDs after reaching the unsuccessful access threshold.
Yes, VuVault.com has the ability to set an unsuccessful access attempt limit and suspend ID's after reaching a set unsuccessful access threshold.

3.11.7.22 VMS shall provide ability to send alerts to System Administrators for unauthorized access attempts.
Yes, VuVault.com has the ability to send alerts to System Administrators for unauthorized access attempts.

3.11.7.23 VMS shall enable automatic logoff of ID after a defined period of session inactivity, and perform subsequent re-log-on password authentication.
Yes, VuVault.com enables automatic logoff of ID after a set period of session inactivity, and perform subsequent re-log-on password authentication.

3.11.7.24 VMS shall provide ability to configure password parameters such as password lengths, user access to expiration settings and other behaviors, enabling alphanumeric characters, etc.
Yes, VuVault.com has the ability to configure password parameters such as password lengths, user access to expiration settings and other behaviors, enabling alphanumeric characters, etc.

3.11.7.25 VMS shall provide ability to lock out user or group ID.
Yes, VuVault.com gives System Administrators the ability to lock out user or group IDs.

3.11.7.26 Vendor will provide a detailed explanation of data security standards, to include but not limited to: defining the physical environment, location of all host servers; protections against natural and man-made disasters; encryption; transfer; storage; redundancy and recovery of files.

VuVault.com is hosted by Amazon Web Services' (AWS) data centers utilize secure innovative architectural and engineering approaches. Each data center is equipped with fire detection and suppression, power failure backup's climate and temperature controls, and electrical and mechanical management. When a storage device reaches its end of life security measures are taken by Amazon to ensure that data is not exposed to unauthorized individuals. Amazon security platforms also host around the clock surveillance to ensure data locations are secure. In case of failure, automated processes move data traffic away from the affected area to an alternate secure location. AWS is designed to tolerate system or hardware failures with minimal to no impact to users. Amazon Web Services supplies three locations separated on the east and west coasts where all of your data will be copied and 100% secured. If one of the locations is wiped out by a natural disaster, your information will still be secured in two alternate locations states away. Any and all of the information that was flowing to that particular location will be directed to substitute locations.

3.11.7.27 Describe security standards for hardware (cameras) in place to prevent data from being accessed in the event a camera is lost or stolen.
The FirstVu HD can be set to secure USB mode to prevent files from being uploaded to any computer without a VuVault.com login and password. When Secure USB Port is enabled, it is impossible to view, edit, or delete files present on the FirstVu HD using a normal computer. A proprietary encryption key restricts access to the FirstVu HD files when in secure USB mode.

3.11.7.28 Vendor will describe any previous loss of data occurring from criminal actions, as well as other issues that impact data integrity, such as unauthorized data access by contract personnel.
Digital Ally does not have any history of previous loss of data occurring from criminal actions, or other issues that impact data integrity.

3.11.7.29 Provide a non-technical means for field personnel to remotely view stored video without altering original file (other than applying metadata to file).
Remote viewing of stored video for field personnel can be accomplished through the VuVault GO mobile application.

3.11.7.30 Describe ability of system to enforce password expiration.
VuVault.com allows the administrative user to set a set number of days before user passwords will expire.

3.11.7.31 Describe ability of system to limit concurrent sessions.
VuVault.com does not have limitations on the number of concurrent sessions.

3.11.7.32 Describe ability of system to log changes to administrative functions.
VuVault.com will keep a log of changes made to administrative functions.

3.11.8 Information Security

3.11.8.1 Vendor shall encrypt transmission of confidential data when transferred through publicly accessible networks such as the Internet.
VuVault.com has AES 256 bit encryption in tandem with Amazon Web Services Multi-part upload tools, as well as SSL connections are utilized with every file transfer. Stored data at rest is encrypted with AWS Server Side Encryption (SSE) using 256-bit Advanced Encryption Standard (AES-256).

3.11.8.2 Vendor shall ensure all transmission of information data files are transferred through a Secure Socket Layer (SSL), which creates a 128 bit encrypted connection which is password protected. All data files that are on Vendor's servers are encrypted once they have completed the upload and pre-process procedures.

VuVault.com has AES 256 bit encryption in tandem with Amazon Web Services Multi-part upload tools, as well as SSL connections are utilized with every file transfer. Stored data at rest is encrypted with AWS Server Side Encryption (SSE) using 256-bit Advanced Encryption Standard (AES-256).

3.11.8.3 All input data transmitted across public networks (all networks other than the State's) shall be encrypted during transit and decrypted electronically during processing to produce non-confidential output data. The decrypted data shall not be accessible by vendor's employees unless otherwise limited on a "need to know" basis as determined by the Nevada Highway Patrol's designee.
Digital Ally's proposed Video Management solution meets this specification.

3.11.8.4 The System shall have a host-based firewall technology preventing inappropriate/ unauthorized access. Vendor shall provide the following:
A. All intrusion detection system monitoring for unauthorized access attempts.
Alert Logic Threat Manager for Amazon Web Services (AWS) is a network intrusion detection service specifically designed for AWS.

B. Must run anti-virus software.
Amazon Web Services runs anti-virus software.

C. Monitor daily logs for potential intrusions, file integrity.
Amazon Web Services (AWS) monitors daily logs for potential intrusions, file integrity.

D. Only allow access by uniquely assigned and auditable IDs.
VuVault.com only allows access by uniquely assigned and auditable IDs.

E. All data transfers and administrative access must be in an encrypted format.
VuVault.com has AES 256 bit encryption in tandem with Amazon Web Services Multi-part upload tools, as well as SSL connections are utilized with every file transfer. Stored data at rest is encrypted with AWS Server Side Encryption (SSE) using 256-bit Advanced Encryption Standard (AES-256).

3.11.9 In-Car Video Integration

3.11.9.1 BWC must have the ability to record audio for the In-car video system.
When the FirstVu HD is connected to the DVM-800 through the VuLink, the FirstVu HD can act as a microphone for the DVM-800.

3.11.9.2 BWC must have the ability to activate recording off the In-Car video systems automatic triggers.
When the FirstVu HD is connected to the DVM-800 through the VuLink, the FirstVu HD has the ability to activate recording off the In-Car video system's automatic triggers such as siren, accelerometer, light bar, etc.

3.12 In-Car Video

The In-Car Video portion of this RFP is contingent upon funding anticipated to be approximately one (1) year from contract award. Vendors proposing In-Car Video must be compatible with proposed Body Worn Cameras.

3.12.1 Standard Specifications

3.12.1.1 All mobile video systems and related audio equipment must conform to the applicable minimum standards as set by the following: Electronic Industries Association (EIA);
The DVM-800 and FirstVu HD meet these standards.

3.12.1.2 Federal Communications Commission (FCC) rules/ regulations;
The DVM-800 and FirstVu HD meet these standards
.

3.12.1.3 Institute of Electrical and Electronic Engineers (IEEE);

The DVM-800 and FirstVu HD meet these standards.

3.12.1.4 International Electro-technical Commission (IEC);
The DVM-800 and FirstVu HD meet these standards.

3.12.1.5 International Organization for Standardization (ISO);
The DVM-800 and FirstVu HD meet these standards.

3.12.1.6 National Fire Protection International (NFPA);
The DVM-800 and FirstVu HD meet these standards.

3.12.1.7 National Highway Transportation Safety Administration (NHTSA);
The DVM-800 and FirstVu HD meet these standards.

3.12.1.8 Society of Automotive Engineers (SAE);
The DVM-800 and FirstVu HD meet these standards.

3.12.1.9 Underwriters Laboratories Inc. (UL); and
The DVM-800 and FirstVu HD meet these standards.

3.12.1.10 Vendors must provide documentation that validates that their systems adhere to the minimum specifications in the International Association of Chief of Police (IACP) Specifications for In-Car Video (dated 11/21/2008), and that the technology used is generally accepted in the relevant field.
Documentation validating the system's compliance with the minimum specifications in the International Association of Chief of Police (IACP) is on page 123.

3.12.2 Video System Specifications

3.12.2.1 The minimum acceptable components consist of the following parts:

A. Front Camera
The DVM-800 has an internal front facing camera, as well as an external 12x front facing camera.

B. Back Seat Camera
The DVM-800 has an internal passenger facing camera and has the option of an external rear seat camera or a license plate backup camera.

C. Color LED monitor with audio
The DVM-800 has a 3.5" Color Ultra Bright monitor with built in audio.

D. Body worn camera must act as a wireless transmitter for audio with in-car & home charger;
When the FirstVu HD is connected to the DVM-800 through the VuLink the body worn camera will act as a wireless transmitter for auto with in-car and home charger.

E. Covert secondary hard-wired microphone;
The DVM-800 has a microphone built into the DVM unit as well as a covert back seat microphone.

F. Digital Video Recorder - DVR
The DVM-800 unit is a complete digital in-car video recording system integrated into a replacement vehicle rear-view mirror. The DVR is built into the replacement rear view mirror.

G. Integrated GPS receiver and antenna
The DVM-800 has an integrated GPS receiver and antenna.

H. Collision sensor
The DVM-800 includes a built-in accelerometer that can be used to trigger an event record when the set G-force levels are exceeded on any of the 3 axis of the vehicle. G-force levels are configured by a system administrator and include acceleration, braking, cornering, collisions, and vertical movements.

I. Controller center
The DVM-800 has a built in controller center in the rear-view mirror DVM unit.

J. Means to transfer media data from In-car to storage solution
The DVM-800 has multiple solutions for transferring media data including Wi-Fi automatic upload, removable SD card for manual upload, and USB in-car access to the DVM-800's internal memory to access ECA recordings.

K. Video view capability
The DVM-800 has the capability to view video with the LCD display.

L. Hardware/software necessary to submit videos as evidence
Yes, the DVM-800 will include hardware and software necessary to submit videos as evidence.

M. All mounts and cables for power, interfaces, cameras, and antennas
The DVM-800 will include all mounts and cables for power, interfaces, cameras, and antennas.

N. Documentation
All system documentation will be included with the DVM-800.

O. Warranty and maintenance
The DVM-800 comes with either a 2 or 5 year warranty.

P. Training and
Training is included in the professional services pricing. This pricing includes the states specified train the trainer program.

Q. Shipping and handling
Digital Ally has included the shipping and handling costs in Attachment H.

3.12.2.2 The digital video recorder (DVR) offered shall be in full commercial production. Prototypes will not be considered.
The DVM-800 is in full commercial production and is not a prototype.

3.12.2.3 Programming of the in-car recording system shall be restricted to authorized personnel only.
Yes, programming of the DVM-800 shall be restricted to authorized personnel only.

3.12.2.4 All controls and indicators shall have adjustable backlighting.
The DVM-800 controls and indicators have adjustable backlighting.

3.12.2.5 The officer shall have the option of recording primary, rear-facing, or both cameras simultaneously.
The DVM allows the officer to have the option of recording primary, rear-facing, or 2 cameras simultaneously.

3.12.2.6 A collision sensor covering 360 degrees, to trigger recordings, without requiring connection to the vehicles airbag system, shall be included. If a collision is detected, the video recorder (including pre-event memory) shall be automatically activated so the collision and video leading up to the collision is recorded.

The DVM-800 includes a built-in accelerometer that can be used to trigger an event record when the set G-force levels are exceeded on any of the 3 axis of the vehicle. G-force levels are configured by a system administrator and include acceleration, braking, cornering, collisions, and vertical movements.

3.12.2.7 The in-car digital video system shall be provided with all necessary cables and hardware (e.g. fuse holders, mounting brackets) required for installation.
The DVM-800 will be provided with all necessary cables and hardware required for installation.

3.12.2.8 Each digital video recording system shall be supplied with a comprehensive installation/ programming/ operations manual. The manual shall specify all brackets, hardware and mounting locations for installing camera systems.
The DVM-800 will include a comprehensive installation/ programming/ operations manual. The manual shall specify all brackets, hardware and mounting locations for installing camera systems.

3.12.3 Digital Video Recorder (DVR)

3.12.3.1 The DVR shall mount in standard equipment consoles between the seats, or overhead.
The DVM-800 is a complete digital in-car video recording system integrated into a replacement vehicle rear-view mirror. The DVR is built into the DVM unit.

3.12.3.2 No permanent modifications shall be required to install the DVR system.
The DVM-800 is a complete digital in-car video recording system integrated into a replacement vehicle rear-view mirror.

3.12.3.3 The DVR system shall be capable of being installed as to not hinder the operation of the police unit.
The DVM-800 is capable of being installed as to not hinder the operation of the police unit.

3.12.3.4 The DVR shall be capable of recording two video inputs from a powerful zoom, forward-facing camera, and a wide-angle rear-facing camera.
The DVM-800 is capable of recording two video inputs from a powerful zoom, forward-facing camera, and a wide-angle rear-facing camera.

3.12.3.5 The DVR shall provide a choice of at least one of the following upload options.

A. Wireless Ethernet- provided 802.11n base station includes encryption, supports multiple simultaneous uploads and is upwardly scalable. The system should be capable of comfortably uploading from multiple vehicles in the regional command centers (depicted in the scope of work section of this RFP) simultaneously. In addition, a backup upload system must be provided, should the wireless transfer system fail.
The DVM-800 offers this as an upload system.

B. Removable Hard Disc Drive (HDD) with provided hard drive docking stations that support plug and play hard drive insertion.
The DVM-800 does not have removable HDD, however it does have a removable SD card.

C. Removable Compact Flash Device-Device with provided docking stations that support plug-and-play flash card insertion.
The DVM-800 offers this as an upload system.

D. Cellular - Upload media via LTE connectivity that is compatible with the Feeney Wireless Skyus-X modem.
The DVM-800 offers this as an upload system.

E. If necessary, itemize and include the cost of media needed to allow officers the ability to rotate media between their vehicles and evidence technicians.
The cost of extra SD cards is included in the cost proposal.

3.12.3.6 The DVR shall have the ability to record up to 8 hours of video before reaching the capacity of the storage media at maximum resolution. For the recording media available, specify the recording and playback times, resolution, and MB per second.
The DVM-800 can record 8-82 hours of video depending on the quality and length of video. The DVM-800 includes 32GB of Solid State internal memory that retains continuous loop and a 32GB SD card for recording individual incidents. The record quality and frames per second can be configured by a System Administrator to control file size and available hours of recorded video.

3.12.3.7 Video resolution, frame rates, and quality on the DVR shall be preset but can be changed by an administrator. These settings shall be independently configurable for recording modes of both video cameras. Please specify levels for:

A. video resolution
The DVM-800 records the video data in three levels of resolution (High, Medium, and Standard) with a maximum resolution of 720 x 480.

B. video frame
rate
The DVM-800 can record up to 30 frames per second.

C. video quality
The DVM-800 records High – 4Mbps, Medium – 2Mbps, and Standard – 1Mbps.

3.12.3.8 The DVR shall require a security feature (key, admin software rights) to prevent unauthorized users from accessing the on-screen menus to adjust video settings and perform file management functions.
The System Administrator has the ability to require a user login before being able to use the DVM-800 menu to prevent unauthorized users from accessing the on-screen menus. All settings are configurable via VuVault.com and pushed to the DVM-800 wirelessly or manually.

3.12.3.9 The DVR shall include a GPS receiver to provide vehicle position, course and speed information. The GPS receiver shall also be used to set the internal DVR clock to the proper time and date so that all vehicles display and record proper time.
The DVM-800 includes a GPS receiver to provide vehicle position, course and speed information. The GPS receiver may also be used to set the internal DVR clock to the proper time and date so that all vehicles display and record proper time.

3.12.3.10 The DVR shall include indicators visible outside of the vehicle to confirm that the system is recording and that the wireless audio transmitter is activated. This indicator does not need to be visible to occupants inside the vehicle.
The DVM-800 indicates that it is in record mode with a red LED light on the rear-view mirror there is also a LED light to indicate that the wireless audio transmitter is activated.

3.12.3.11 The DVR shall be capable of initiating a recording by both automatic and manual means. The DVR shall begin recording automatically when any of the following are activated:

A. Vehicle's emergency/pursuit
lights;

The DVM-800 can trigger the activation of the recording function through the following programmable parameters: REC button on DVM unit, REC button on the wireless microphone, emergency light activation, siren activation, activation through auxiliary input, exceeding accelerometer (crash sensor), exceeding GPS speed limit, exceeding radar speed, exceeding speedometer speed limit, and vehicle breaks.

B. Siren, and

The DVM-800 can trigger the activation of the recording function through the following programmable parameters: REC button on DVM unit, REC button on the wireless microphone, emergency light activation, siren activation, activation through auxiliary input, exceeding accelerometer (crash sensor), exceeding GPS speed limit, exceeding radar speed, exceeding speedometer speed limit, and vehicle breaks.

C. The systems integrated crash sensor. (This activation shall include capturing the "look back" buffer memory to video-record the collision, should it be in view of the active camera.

The DVM-800 can trigger the activation of the recording function through the following programmable parameters: REC button on DVM unit, REC button on the wireless microphone, emergency light activation, siren activation, activation through auxiliary input, exceeding accelerometer (crash sensor), exceeding GPS speed limit, exceeding radar speed, exceeding speedometer speed limit, and vehicle breaks.

3.12.3.12 The audio input associated with the forward-facing camera shall record audio using the internal microphone inside the vehicle. When the wireless audio transmitter/BWC is activated, the audio input shall be automatically switched to the wireless audio transmitter's microphone. The system shall automatically revert to the internal microphone when the wireless audio transmitter/BWC is deactivated.

The DVM-800's associated audio input with the forward-facing camera will record audio using the internal microphone inside the vehicle. When the FirstVu HD or the wireless audio transmitter's microphone is activated, input will automatically switch and will revert to the internal microphone when deactivated.

3.12.3.13 The DVR shall include a programmable pre-event recording mode allowing it to capture images a minimum of 30 seconds prior to the activation of the RECORD mode. Specify pre-event recording

capability of proposed DVR.

The DVM-800 has a pre-event recording mode of up to 30 seconds for each of the two recording channels, adjustable in 6 second increments.

3.12.3.14 The DVR shall be capable of capturing date/time, user identification information, emergency light indication, siren indication, speed indication (w/ radar interface), braking indication, and whether the microphone is activated. The information shall not be overlaid on the recorded video, and should be stored as secured metadata.
The DVM-800 will track all these metadata fields and add them to the event file.

3.12.3.15 The DVR shall allow video to be played back in the vehicle. When the DVR PLAY button is pressed a list of all prior recordings shall appear on the display screen provided.
The DVM-800 monitor allows for video playback in the vehicle. When the DVR PLAY button is pressed a list of all prior recordings will appear on the display screen for the officer to choose which video they want to view.

3.12.3.16 The DVR shall record video in a format that allows playback on multiple devices.
The DVM-800 records in AVI format and can be converted to MP4 for playback on multiple devices.

3.12.3.17 The DVR shall provide a means to ensure the integrity of the recorded video has not been compromised. The video must be able to be authenticated at any time, including when it is played back outside of the police vehicle.
The DVM-800 authenticates video by encrypting the connection with WAP2 encryption. This encryption method is more secure and up-to-date than 128-bit MD5 hash. An integrity check is done to verify video has not been tampered with. Additionally, all edited video is saved as a separate file, keeping the raw original untouched.

3.12.3.18 The DVR shall provide a means to ensure the integrity of the recorded video has not been compromised. The video must be able to be authenticated at any time, including when it is played back outside of the police vehicle.
The DVM-800 includes a built-in accelerometer that can be used to trigger an event record when the set G-force levels are exceeded on any of the 3 axis of the vehicle. G-force levels are configured by a system administrator and include acceleration, braking, cornering, collisions, and vertical movements.

Additionally, all edited video is saved as a separate file, keeping the raw original untouched.

3.12.3.19 The Control Center/DVR firmware shall allow in-system programming for future updates. Please describe how updates are made.
Digital Ally will send out periodic software updates through VuVault.com. These updates will be downloaded to the DVM-800 via its WiFi connection.

3.12.3.20 The DVR or related display (Mobile Data Computer, tablet etc.) shall have backlit controls for record; stop; play/pause; forward/reverse, fast forward/ reverse; trace, and lighted indicators for power on; record; and play.
The controls on the DVM-800 have backlit controls for record, stop, play/pause, forward/reverse, fast forward/reverse, trace and lighted indicators for power on, record, and play.

3.12.3.21 The power control switch shall allow the DVR to automatically power on after the vehicle's ignition is switched on.
The DVM-800 has a power control switch allowing it to automatically power on after the vehicle's ignition is switched on.

3.12.3.22 The DVR shall automatically power down after the vehicle's ignition is turned off provided the DVR is not in "Record" and is not in the process of downloading files or other type of file save.
If the DVM-800 is not recording when the vehicle is powered off it will power down after 60 seconds using the internal backup battery or when the DVM-800 is finished uploading video.

3.12.3.23 The DVR should provide a means to tag an incident at the time it is recorded with a priority designation. Once a recording is stopped, the DVR should automatically prompt the officer to select from the pro-defined drop-down list(s).
Once a recording has completed, the DVM-800 monitor will give the officer the option to tag the incident by utilizing pro-defined drop-down list(s).

3.12.3.24 The DVR shall be capable of operating within the range of interior temperatures found within a law enforcement vehicle in Nevada without the need for supplemental heating or cooling. Specify your DVR's operating range and acceptability for the extreme temperature range in Nevada
The DVM-800 has an operating temperature of -20 degrees to +70 degrees C and a storage temperature of -40 degrees to +80 degrees C.

3.12.4 Compact CCD Color Camera

3.12.4.1 The low-light CCD color camera shall use a Sony EXview® HAD CCD or equivalent image sensor to provide high quality nighttime images while minimizing blooming and glaring from bright sources of light. Proof of "equal" shall be the responsibility of the bidder and shall be submitted with the bid if not using the Sony EX VIEW chipset.

	Sony EXview HAD CCD	***Sony Super HAD CCD***
Image Size	Type 1/3	Type 1/4
Pixels	480k	480k
Effective Pixels	976(H) x 494(V)	976(H) x 494(V)
Unit Cell Size	5.0(H) x 7.4(V)	5.0(H) x 7.4(V)
Sensitivity [mV] (F5.6)	2800(mV)	2350(mV)
Smear [dB] (F5.6)	-110(dB)	-110(dB)
Supply Voltage [V]	+15/-7.5 (typ.)	12V

3.12.4.2 The forward-facing camera shall be a solid state imaging system that is not subject to burn in, or interference by magnetic fields.
The DVM-800 forward-facing camera is a solid state imaging system that is not subject to burn in, or interference by magnetic fields.

3.12.4.3 The forward-facing camera shall operate within the range of temperatures from 0 to 120 degrees Fahrenheit or between -17.8 and 48.9 degrees Celsius.
The DVM-800 forward-facing camera has an operating temperature of -20 to +80 degrees Celsius.

3.12.4.4 The camera shall be compact so as not to obstruct the driver's forward or peripheral view thru the windshield, or provide any obstruction of factory installed airbags or mirrors.
The DVM-800 is a complete in-car camera system built into a replacement rear-view mirror as to not obstruct the driver's forward or peripheral view through the windshield, or provide any obstruction of factory installed airbags or mirrors.

3.12.4.5 The camera shall be a single unit, including power lens, mounted on the windshield or roof of the vehicle and operate on 12 VDC power source.
The DVM-800 is a single unit with 2 cameras built in including power lens, mounted in place of the vehicle's stock rear-view mirror and operates on 12 VDC power source.

3.12.4.6 The camera shall provide a minimum field of view of 24 feet width at distance of 35 feet (40 degrees).
The DVM-800's internal road facing camera has a field of view of V: 57.9 degrees, H: 79.2 degrees, and D: 103.4 degrees.

3.12.4.7 The camera shall have manual and automatic focus capabilities, which are user selectable.
The DVM-800 cameras have manual and automatic focus capabilities that are user selectable.

3.12.4.8 The front camera should have a minimum 120X zoom (10x optical zoom with 12x digital zoom). Specify mode.
The DVM-800 road facing camera's zoom magnification is 12X [f=3.8 ~ 38.0mm(F2.8)], Practical H. angle 51.2° (Wide) ~ 5.58° (Tele)

3.12.4.9 The minimum LUX rating of the forward facing camera shall be rated at less than 1 LUX at full shutter speeds and 0.05 LUX in night view mode.
The DVM-800 built in cameras have a LUX rating of .5 LUX.

3.12.4.10 The camera shall automatically adjust for varying light levels from day to night. The camera and lens will be equipped with auto focus, automatic exposure, and automatic white balance.
The DVM-800 internal cameras have a low LUX rating of 0.5 LUX when the IR LEDs are turned off and 0.0 LUX when the IR LEDs are turned on.

3.12.4.11 The camera shall have a minimum color resolution of 450 horizontal lines.
The DVM-800 has a resolution of 720 x 480.

3.12.4.12 All cameras shall default to auto focus. An override system should be configurable to prevent operation while the vehicle is in motion.
The DVM-800 cameras default to auto focus with a configurable override system to prevent operation while the vehicle is in motion.

3.12.4.13 The camera shall offer a signal-to-noise ratio of at least 46db.
The DVM-800 has a signal to noise ratio of 52db.

3.12.4.14 The camera shall have backlight compensation setting.
The DVM-800 cameras have backlight compensation settings.

3.12.4.15 The camera shall be compact. List the size and weight of the proposed CCD camera.
The DVM-800 unit is 1.9in (D) x 11in (W) x 4.7in (H) and weighs 1.62lbs.

3.12.4.16 The camera shall mount with a heavy-duty controlled pivot mount that does not obstruct the driver's field of view. Camera shall be able to be rotated 360 degrees and can pan and tilt to +/- 90 degrees. Adjustment shall require no tools.
The DVM-800 has two cameras built into the DVM unit, one forward facing and one in-car eliminating the need for the cameras to rotate 360 degrees. The DVM-800 also includes an external 12x camera that does have the capability to rotate 360 degrees.

3.12.4.17 An optional rear view camera shall be available.
An optional rear view camera is available for the DVM-800.

3.12.5 Back Seat Cameras

3.12.5.1 The back-seat camera shall utilize a micro compact with wide angle 1/3" Super HAD image device (or equivalent) with approximately 420 lines of resolution. Proof of "equal" shall be the responsibility of the bidder and shall be submitted with the bid. This must be included in the system at no charge.
The DVM-800 external back-seat cameras utilizes a micro compact with wide angle 1/4" Super HAD CCD image.

3.12.5.2 The rear-facing camera shall be capable of being mounted covertly in the cab.
The DVM-800 rear-facing camera is built into the DVM unit keeping it covert.

3.12.5.3 The rear facing camera shall be capable of recording the entire rear seat area of the police vehicle.
The DVM-800 rear-facing camera has the capability to record the entire rear-seat area of the police vehicle.

3.12.5.4 The rear-facing camera shall have a minimum lux rating of .03. Specify the rating.
The rear-facing camera has a lux rating of 0.5 LUX with IF LEDs off and 0.0 LUX with IF LEDs on.

3.12.5.5 The rear-facing camera shall utilize infrared illumination to capture video in no-light conditions.
The rear-facing camera utilizes infrared illumination to capture video in no-light conditions.

3.12.6 Compact Color LCD Monitor

3.12.6.1 The monitor shall be a full color high quality LCD, active matrix (TFT) screen that measures at least 3.0” measured diagonally.
The DVM-800 has a 3.5" Color Ultra Bright LCD monitor with 640 x 480 resolution.

3.12.6.2 The monitor shall be capable of displaying a live picture from the camera when powered, even if recording is not in progress.
The DVM-800 monitor is capable of displaying a live picture from the camera when powered, even if a recording is not in progress.

3.12.6.3 The monitor shall operate between 32 and 120 degrees Fahrenheit
The DVM-800 unit has an operating temperature of -20 to +80 degrees Celsius.

3.12.6.4 The monitor shall include a system speaker, with volume control, to provide monitoring of live audio or playback from all system microphones.
The DVM-800 includes a system speaker, with volume control, that provides monitoring of live audio or playback from all system microphones.

3.12.6.5 The monitor shall have controls/indicators that mimic the DVR and include record; stop; play/pause; forward/reverse; brightness; volume; and power. The monitor should also include a button for disabling the monitor when the system in standby, and accessing a menu for programming.
The DVM-800 monitor is built into the DVR and includes controls/indicators such as stop, play/pause, forward/reverse, brightness, volume, and power. The monitor also includes a button for disabling the monitor when the system is in standby, and accessing a menu for programming.

3.12.6.6 The monitor should have the capability to display: date/time, user identification information, emergency light indication, siren indication, latitude and longitude, speed (w/ radar interface), braking indicator and microphone activation indicator. The information shall not be overlaid on the recorded video; rather, it should be stored as external secure meta-data (or equivalent) in the video file.

The DVM-800 has the capability to display date/time, user identification information, siren indicator, and microphone activation indicator.

3.12.6.7 The monitor should support a full-screen video mode (without the auxiliary data) using a single key press on the control center.
The DVM-800 supports a full-screen video mode (without the auxiliary data) using a single key press on the control center.

3.12.6.8 The monitor shall operate independently from the recording device. For covert operation it should possible to operate the DVR in RECORD mode with the monitor turned off.
The DVM-800 will allow the DVR to operate in Record mode with the monitor turned off.

3.12.6.9 The monitor shall be provided with an adjustable mounting bracket that will allow it to be mounted in a variety of locations within the law enforcement vehicle.
The DVM-800 monitor is built into the DVM rear-view mirror unit and therefore can only be mounted by replacing the factory mirror.

3.12.6.10 The monitor shall have the capability to display the approximate amount of storage remaining on the media in an HH:MM format. An audible beep or other form of tone shall warn operator prior to or when there is 10%, or less, time remaining on the media.
The DVM-800 monitor will display the approximate amount of storage remaining on the media in an HH:MM format in the lower right portion of the screen.

3.12.7 Microphones

3.12.7.1 The system shall come equipped with a digital wireless microphone that is incorporated into the BWC and an in-car microphone. The in-car microphone shall be mountable anywhere within the vehicle.
The DVM-800 comes with a digital wireless microphone and also has a microphone built into the DVM unit. An additional wireless microphone can be paired to the DVM unit, and can be mounted anywhere in the vehicle.

3.12.7.2 Audio from the interior microphone and the wireless microphone/BWC shall record on separate audio channels.
Audio recorded from the interior microphone and the wireless microphone will record on separate audio channels.

3.12.7.3 The wireless microphone/BWC shall be self-contained and include a re-chargeable battery; mountable charger/docking station; internal microphone; internal antenna. Transmitters that rely on the microphone cable for an antenna, or which utilize an external antenna shall not be permitted.
The DVM-800 wireless microphone is self-contained with a rechargeable battery and comes with a charging/docking station that can be mounted in the vehicle. The wireless microphone has an internal microphone and antenna and does not rely on the microphone cable for an antenna.

3.12.7.4 The wireless microphone/BWC system shall be FCC type accepted.
The DVM-800 wireless microphone is FCC type accepted.

3.12.7.5 The wireless microphone/BWC shall have a minimum effective operating range 1,000 feet under line-of-sight conditions.
The DVM-800 wireless microphone has a minimum effective operating range of 1,000 feet under line-of-sight conditions.

3.12.7.6 The wireless microphone/BWC must have a minimum stand-by battery life of ten (10) hours without recharging or additional batteries, with pre-record on.
The DVM-800 wireless microphone has approximately 20 hours in use with a full charge and 14 days of standby time.

3.12.7.7 The wireless microphone/BWC should be capable of automatically activating the DVR system; additionally, the wireless audio transmitter/BWC shall be capable of being activated by the DVR system when a recording is started.
The DVM-800 is capable of automatically activating from the wireless microphone and from the FirstVu HD when paired through the VuLink. The wireless microphone will activate when the DVM-800 starts a recording.

3.12.8 Control Center

3.12.8.1 The control center shall be compact in design and mounted overhead, or in the equipment console between the seats.
The DVM-800 is a complete digital in-vehicle video recording system integrated into a replacement vehicle rear-view mirror included the control center.

3.12.8.2 The control center shall not obstruct the driver's forward or peripheral view or provide any obstruction of factory installed airbags or mirrors.

The DVM-800 is a complete digital in-vehicle video recording system integrated into a replacement vehicle rear-view mirror. The control center is built into the DVM unit keeping from obstructing the driver's forward or peripheral view or any obstruction of factory installed airbags or mirrors.

3.12.8.3 The control center shall not require any permanent modifications to the police vehicle.
The DVM-800 is a complete digital in-vehicle video recording system integrated into a replacement vehicle rear-view mirror. This is not a permanent modification to the police vehicle.

3.12.8.4 The control center shall accommodate the mounting of the front and rear-facing cameras, the monitor and keypad.
The DVM-800 is a complete digital in-vehicle video recording system integrated into a replacement vehicle rear-view mirror. The front and rear-facing internal cameras are built into the DVM unit.

3.12.9 Video Viewing Software/Hardware

3.12.9.1 A video viewer/software shall be provided to allow recorded video files to be played on any computer and display date/time, user identification, emergency light indication, siren indication, latitude and longitude, speed (w/ radar interface), braking indication and the microphone activation indicator. This information shall not be overlaid on the recorded video; it shall be displayed outside the video frame.
VuVault.com is a hosted cloud solution allowing access to the system from any internet enabled device with the appropriate login information. VuVault.com allows for recorded video files to be played on any computer and display date/time, user identification, emergency light indication, siren indication, latitude and longitude, speed, braking indication and the microphone activation indicator. This information is included in the metadata portion of the video file and not as an overlay.

3.12.9.2 Support for this software shall include version updates provided free of charge for the lifetime of the system.
Digital Ally will provide support for this software including version updates free of charge for the lifetime of the system.

3.12.9.3 Vendors shall provide all hardware (media readers/drives) and software necessary duplicate, share and present digital video in a court acceptable format. Please describe transfer steps needed to convert captured video to court acceptable evidence without the need for a server based infrastructure.
VuVault.com includes and extensive, secure and flexible share portal to facilitate convenient sharing of video evidence and case files with designated and credentialed third parties.

3.12.9.4 The video management software should be capable of converting a video from the proprietary format to the standard DVD Video format, and authoring a DVD capable of being played in a standard DVD player.
VuVault.com allows for users with appropriate permissions to download video files to then burn to DVD's. These can be played in a standard DVD player.

3.12.10 Server Based Video Management System (VMS)

3.12.10.1 VMS shall either be an externally hosted cloud-based data storage solution with the capability of organizing/managing video/digital evidence, server based or consist of a hybrid solution and be accessible via the internet to multiple users simultaneously. The State prefers Cloud or a Hybrid solution.
VuVault.com is an externally hosted cloud-based data storage solution with the capability of organizing/managing video/digital evidence.

3.12.10.2 The VMS should include infrastructure in our Northern, Southern, and Central regional command offices to assure downloading of all rural substations into the regional command centers to which they report (see Table 3.8.A).
VuVault.com can be accessed by any internet capable computer with the proper logins.

3.12.10.3 The VMS shall be a turn-key component and fully installed, serviced, warranted, and maintained by the vendor.
VuVault.com is a hosted cloud solution.

3.12.10.4 The VMS should include video storage servers or equivalent for all regional offices to capture video information, workstation(s) for managing and viewing stored video, equipment racks to mount equipment, and uninterruptible power supplies (UPS).
VuVault.com is a hosted cloud solution.

3.12.10.5 The VMS should provide a configurable archive unit that can automatically archive video copies based on set parameters, and copy video files to a DVD-Video or equivalent court acceptable format.
VuVault.com allows users with appropriate login credentials can copy video files to a DVD-Video or equivalent court acceptable format.

3.12.10.6 Pricing for the VMS shall be provided on the In-Car Video Cost in the vendor's response. Pricing must be included for all proposed hardware (workstations, servers, archiving hardware, video backup systems, and access points), wiring, software, installation, configuration, and training. If proposing a cloud or Hybrid solution, provide this pricing in the ICV cost schedule.
Pricing for VuVault.com is provided in the In-Car Video Cost as well as all proposed hardware, wiring, software, installation, configuration, and training.

3.12.10.7 If a server based video management back office component is proposed, a schematic of the back end infrastructure shall be included with responses to the RFP.
VuVault.com is a hosted cloud solution.

3.12.10.8 The VMS file storage shall be equipped with sufficient storage to comfortably manage video that would be generated from cars depicted in the scope of work in this RFP. List and itemize the size of proposed storage for each regional command center identified.
Digital Ally has provided a quote for unlimited cloud storage in the Cost Proposal.

3.12.10.9 If wireless downloading capability is proposed for vehicles assigned to each regional office, provide download times for video captured based on the video compression and resolution capabilities of proposed cameras, the proposed number of access points, and the proposed servers/wiring infrastructure or cloud solutions.
Download times for wireless downloading for vehicles assigned to each regional office is directly affected by the office's network speed.

3.12.10.10 The VMS shall include a database that contains a record for each recorded video file. The database shall store sufficient information to support the search capabilities and provide chain-of-evidence documentation.
VuVault.com includes a databased hosted on Amazon Web Services' cloud that contains a record for each recorded video file, as well as all activities preformed on each video. The database stores all sufficient information to support the search capabilities (default and customized) and provide chain of custody activity report.

3.12.10.11 The VMS shall be capable of searching stored video files by: department ID, time, date, officer ID, vehicle ID, camera, recording mode, and status (online or archived).

There are several standard search criteria already implemented into VuVault.com such as date/time, event id, user id, event type, along with an unlimited customizable metadata fields to make finding recordings fast and easy.

3.12.10.12 The VMS shall be capable of providing custom fields that may be used to store department-defined information (e.g. suspect's name, license plate number, etc.).
VuVault.com has an unlimited amount of customizable metadata fields that can be used to store department-defined information.

3.12.10.13 The VMS should allow videos to be categorized using department-defined drop-down lists. This classification shall be used for searching and to define how long each category of video is to be kept before it is automatically deleted.
VuVault.com allows videos to be categorized using customizable department-defined drop-down lists. These categorizes can be used to search for video, as well as to set the retention time of videos.

3.12.10.14 The VMS shall provide a means to ensure the integrity of the recorded video. Video integrity must be checked when the video is uploaded, anytime it is played back or archived, and shall be verifiable on demand.
The DVM-800 utilizes Digital Ally's wireless transfer module which allows for automatic encrypted transmission of video with the included metadata whenever in range of a configured access point. During a wireless upload, a SHA-256 checksum is initiated to validate and ensure the integrity of the video file during the file transfer. The video file itself is recorded in a standard AVI format. The Digital Ally VuVault.com system has a "file integrity check" function and can identify if a file has been altered or is corrupted using this feature. An "integrity check report" can be quickly generated which will illustrate detailed information on the file(s) in question. With the electronic door lock access feature, and automated file transfer, chain of evidence is assured. Additionally a "chain of custody" report can be generated as an unalterable, encrypted PDF file which will illustrate all activity associated with the recorded event file.

3.12.10.15 The VMS shall provide the capability to duplicate, share and present digital video in a court acceptable format. Describe the transfer steps, if any, needed provide video to the courts as acceptable evidence. Describe the way and format the proposed system archives recorded video files, and how these files will be stored and backed up for safeguarding.

VuVault.com includes and extensive, secure and flexible share portal to facilitate convenient sharing of video evidence and case files with designated and credentialed third parties. This functionality can be used on a one off basis by the issuance of one time credentials or can be configured to allow regular and continued access by known and trusted third parties i.e. the prosecutor and staff. These third parties will have the option, if given privileges per share, to review and/or download files in native format to solid state memory. No proprietary player needed to review video and audio post download.

3.12.10.16 When a video file is copied or archived to digital media, the Video Management Software shall store a unique archive ID and maintain a virtual directory to recall the archived video file(s).
When a video file is copied or archived to digital media, VuVault.com will store an unique event number ID and maintains a virtual directory to recall the archived video file(s).

3.12.10.17 The Video Management Software shall be capable of converting a video from the proprietary format to the standard DVD Video format, and authoring a DVD capable of being played in a standard DVD player.
VuVault.com allows for users with appropriate permissions to download video files to then burn to DVD's. These can be played in a standard DVD player.

3.12.10.18 The support for this software shall include version updates and be provided free of charge to the agency for the lifetime of the system.
Digital Ally will provide all support for VuVault.com including version updates for the lifetime of the system.

3.12.11 Control Center Specifications

3.12.11.1 An optional radar interface shall integrate directly with the Agency Bee III radar equipment. Collected information shall include speed of the target, the "locked" target speed, and the patrol vehicle.
With the appropriate cable, the DVM-800 should be compatible with Agency Bee III radar equipment.

3.12.11.2 The State is interested in a system that can be configured for motorcycle use. All of the specifications described for the DVR and wireless microphone shall be applicable. Is a motorcycle option available for your solution? If so, does the configuration utilize a weatherproofed monitor and camera? Please explain.
The FirstVu HD has the capability to be motorcycle mounted, however does not have a water resistant monitor. Viewing of video can be accomplished through the VuVault GO mobile application on an Android or iOS device.

3.12.12 Officer Safety

3.12.12.1 All equipment shall be capable of installation in the following vehicles while still meeting the other requirements stated herein: Chevrolet Tahoe, Dodge Charger, Ford Interceptor Utility/Sedan and Ford F150 Pick-up.
The DVM-800 is capable of installing in all listed vehicles.

3.12.12.2 Describe dimensions and vehicle mounting options for your camera, recorder, wireless microphone, transmitter/ receiver and any other required equipment.
The DVM-800 has one mounting option; it is a replacement rear-view mirror. The dimensions are 1.9in (D) x 11in (W) x 4.7in (V).

3.12.12.3 Equipment must not be installed in such as manner as to interfere with a passenger in the front passenger seat.
The DVM-800 is a complete digital in-vehicle video recording system integrated into a replacement vehicle rear-view mirror allowing for no interference with a passenger in the front passenger seat.

3.12.12.4 No part of the system shall interfere in any way with the driver's field of view. The camera shall be a single unit, including power lens, mounted on the windshield or roof of the vehicle and operate on 12 VDC power source All connections to the camera, for power and video, shall be made by a single cable that attaches using a quick release connector.
The DVM-800 is a complete digital in-vehicle video recording system integrated into a replacement vehicle rear-view mirror allowing for no interference in any way with the driver's field of view. The external cameras are single units, including power lens, mountable on the roof of the vehicle while operating on 12 VDC power source. All connections from the DVM-800 unit and external cameras is made by a single cable that attaches using a quick release connector.

3.12.12.5 The in-car system shall be protected from damage due to input of voltage, reverse polarity, and electrical transients that may be encountered.
The DVM-800 is protected from damage due to input of voltage, reverse polarity, and electrical transients that may be encountered.

3.12.12.6 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.

No DVM-800 items installed in the interior of the passenger compartment will increase the risk of injury to occupants during events related to a vehicle crash.

3.12.12.7 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 as referenced in the In-Car Video Camera Systems Performance Specifications - Digital Video Systems provided by the International Association of Chiefs of Police. (11/21/2008).
All DVM-800 items installed in the interior of the vehicle shall meet the requirements stated in the Federal Motor Vehicle Safety Standard 201 Occupant Protection in Interior Impact as referenced in the In-Car Video Camera Systems Performance Specifications – Digital Video Systems provided by the International Association of Chiefs of Police.

3.12.12.8 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.
The DVM-800 has an easy accessible record button on the face of the DVM unit. The record button can be utilized by officers wearing gloves.

3.12.12.9 System components shall be capable of being illuminated for ready identification during periods of darkness. The illumination level shall be capable of being controlled over a range from bright to dark.
The DVM-800 system components are backlit allowing them to be illuminated for ready identification during periods of darkness. Backlight controls are included.

3.12.12.10 All wiring shall meet industry standards applicable to the wire application including Underwriters Laboratory (UL) as well as the Society of Automotive Engineers (SAE).
The DVM-800 wiring meets industry standards applicable to the wire application including Underwriters Laboratory as well as the Society of Automotive Engineers.

3.12.12.11 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.

The and DVM-800 will include information in their installer's guides and owner's manuals that specifies the proper wiring, fuses, connectors, and connection points with the vehicle electrical system and ground points.

3.12.12.12 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.
No parts of the FirstVu HD or DVM-800 that can come into contact with human skin will be allowed to reach a temperature capable of causing a burn injury.

3.12.12.13 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.
All system components of the FirstVu HD and DVM-800 units carried on the officer's person meets all Underwriters Laboratory Standards for shock/electrocution and burn prevention. All batteries used in the FirstVu HD and DVM-800 units meet Underwriters Laboratory Standards for safety.

3.12.12.14 The In-Car Video System shall operate on a power source that is filtered, regulated, and short-circuit protected. The voltage supplied to the In-Car Video System components shall meet the manufacturer's specifications and shall not vary with fluctuations of the vehicle's electrical system of between 9 and 18 volts.

The DVM-800 operates on a power source that is filtered, regulated, and short-circuit protected and will not vary with fluctuations of the vehicle's electrical system of between 9 and 18 volts. During an event recording, if vehicle power is completely lost to the DVM system, the unit will switch to the internal battery to end the event record, close any open files to prevent data corruption, and then power off after 60 seconds. If the DVM is not recording when vehicle power is completely lost, the DVM-800 will power down after 60 seconds using the internal backup battery.

3.12.13 Reliability

3.12.13.1 The video systems shall maintain consistent audio/visual recording quality. The in-car recording system shall not be affected by transmissions from the police communication or interference from the following sources: high-powered television stations; other radio frequency interference (e.g. UHF, VHF & HF); automobile alternator, ignition, electrical systems; automobile heaters / air conditioner fan motors; or other patrol vehicle electrical systems.

The FirstVu HD and DVM-800 maintain consistent audio/visual recording quality. The DVM-800 is not affected by transmissions from the police communication or interference from high-powered television stations, other radio frequency interference, automobile alternator, ignition, electrical systems, automobile heaters/air conditioner fan motors, or other patrol vehicle electrical systems.

3.12.13.2 All equipment shall have a lifecycle of at least 3 years under law enforcement agency usage, or have replacement coverage under warranty and maintenance. Please provide expected lifecycle for all video system components.
The FirstVu HD and DVM-800 have a lifecycle of three or four years under law enforcement agency usage, as well as battery replacement coverage under warranty and maintenance.

3.12.13.3 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.
The FirstVu HD and DVM-800 do not generate electromagnetic or radiation while in use that interferes with communications or other electronic equipment found within a police vehicle.

3.12.13.4 Loss of power to the system shall not cause loss of any recorded data or result in the unit requiring reprogramming, reloading of software or operating system software
During an event recording, if vehicle power is completely lost to the DVM system, the unit will switch to the internal battery to end the event record, close any open files to prevent data corruption, and then power off after 60 seconds. If the DVM is not recording when vehicle power is completely lost, the DVM-800 will power down after 60 seconds using the internal backup battery.

3.12.13.5 The video system shall be able to return to a "ready to record" mode after sudden loss of power without requiring user intervention.
Once the DVM-800 system boots back on, it will return to a "ready to record" mode after sudden loss of power without requiring user intervention.

3.12.13.6 The system's timekeeping device and the vehicle's identifier shall be protected by a system battery backup to prevent loss of information in the event the vehicle battery is disconnected for up to a minimum of fourteen (14) days.
The DVM-800's timekeeping device and the vehicle's identifier will be protected by a system battery backup to prevent loss of information in the event the vehicle battery is disconnected. The time frame for how long the unit remains on is customizable by

the System Administrator.

3.12.13.7 Date and time within video system shall be self-adjusting for daylight savings time and leap years.
The date and time within the FirstVu HD and DVM-800 are self-adjusting for daylight savings time and leap years.

3.12.13.8 The video system shall have self-charging backup battery that continues recording upon loss of power, and should gracefully shutdown prior to available power being exhausted. The battery backup should power the system for at least 2 minutes following loss of the vehicle's battery power.
The DVM-800 has a self-charging backup battery that will activate if vehicle power is completely lost to the DVM system during a recording, the unit will switch to the internal battery to end the event record, close any open files to prevent data corruption, and then power off after 60 seconds. If the DVM is not recording when vehicle power is completely lost, the DVM-800 will power down after a customizable interval of time (default 60 seconds) using the internal backup battery.

3.12.14 Training/Documentation

3.12.14.1 The vendor shall offer and provide, at no additional cost, training to all end users on the use of the video system and video viewing software.
Digital Ally will offer and provide training to all end users on the use of the video system and video viewing software.

3.12.14.2 The vendor shall offer and provide, at no additional cost, training to electronic technicians at their Reno, Elko, and Las Vegas shop locations. This training will ensure proper operation, repair, and maintenance of the manufacturer's video system.
Digital Ally will provide at no additional cost training to electronic technicians at their Reno, Elko, and Las Vegas shop location.

3.12.14.3 A system administrator class covering all aspects of the system shall be given at all the DPS/HPD Regional Command sites (Reno, Elko, and Las Vegas) upon award.
Digital Ally will provide a system administrator class covering all aspects of the system at all the DPS/HPD Regional Command sites upon award.

3.12.14.4 Trainers must be experienced instructors who are thoroughly familiar with all technical aspects of the system.

Digital Ally will provide trainers that are experienced instructors who are thoroughly familiar with all technical aspects of the system.

3.12.14.5 Provide a course syllabus for training classes to be provided with your RFP response.
Digital Ally has submitted a course syllabus for training classes with this response.

3.12.14.6 Vendor shall include documentation for procedures on regular maintenance of video system components.
Digital Ally has submitted documentation for procedures on regular maintenance of video system components.

3.12.14.7 Vendor shall provide complete service manuals and service bulletins on all electronic components.
Digital Ally will provide complete service manuals and service bulletins on all electronic components.

3.12.14.8 Vendor shall provide documentation of system that includes identification of all vehicle equipment and the physical configuration; all configurable system parameters; written installation instructions, user manuals; and system administrator manuals instructions covering the change of all configuration settings.
Digital Ally will provide documentation of system that includes identification of all vehicle equipment and the physical configuration; all configurable system parameters; written installation instructions, user manuals; and system administrator manuals instructions covering the change of all configuration settings.

3.12.15 Installation

3.12.15.1 Describe your approach for installing camera systems if this service is requested by the State. The State reserves the right to do such installations either through its fleet shops, or through an accessory installation contract.
Digital Ally will not utilize subcontractors for service requested by the state.

3.12.15.2 Provide an installation price per camera unit for each regional office.
Price can be found on Attachment H.

3.12.15.3 Specify the companies that will provide installation of camera systems in our Reno, Elko and Las Vegas regional offices if requested by the State.
N/A

Electromagnetic Compliance Engineering Test Report

To

EN 301 489-1/3 and EN 61000-6-1

For

Model: FirstVu HD

FOR

Digital Ally

9705 Loiret Blvd
Lenexa, KS 66219

Test Report Number: 140220A

ROGERS LABS, INC.
4405 West 259th Terrace
Louisburg, KS 66053
Phone / Fax (913) 837-3214

Engineering Test Report
For Verification to
EN 301 489-1/3 and EN 61000-6-1

For

Digital Ally

9705 Loiret Blvd
Lenexa, KS 66219

Model: FirstVu HD

Test Date: February 20, 2014

Certification Date: February 20, 2014

Certifying Engineer: Scot D Rogers

Scot D. Rogers
Rogers Labs, Inc.
4405 West 259th Terrace
Louisburg, KS 66053
Telephone/Facsimile: (913) 837-3214

This report shall not be reproduced except in full, without the written approval of the laboratory. This report must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government.

Certificate of Compliance

Digital Ally
9705 Loiret Blvd
Lenexa, KS 66219
Model: FirstVu HD

Test Performed	Results
Emissions	Complies
Immunity to Radio Frequency Electromagnetic Field	Complies
Immunity to Electrostatic Discharge	Complies

This Engineering Report has been prepared by Rogers Labs, Inc., for the product described above. This report has been construct in support of the requirements set forth in The International Standards, EN 301 489-1, EN 301 489-3, and EN 61000-6-1.

I, individually, and for Rogers Labs, Inc., certify that the statements made in this Engineering report are true, complete, and correct to the best of my knowledge and are made in good faith.

Scot D Rogers
Scot D. Rogers
Rogers Labs, Inc.
Dated: February 20, 2014

This report has been reviewed as presented and accepted by Digital Ally. The undersigned is responsible for ensuring the Digital Ally; Model FirstVu HD remains compliant with the applicable rules.

Digital Ally

Table of Contents

CERTIFICATE OF COMPLIANCE 3

TABLE OF CONTENTS 4

REVISIONS 5

EXECUTIVE SUMMARY 6

ENVIRONMENTAL CONDITIONS 6

INTRODUCTION 7

Purpose 7

Scope 7

References 7

Definitions 8

EQUIPMENT AND CABLE CONFIGURATION 8

Equipment Tested 8

Equipment Function 8

Equipment Configuration 9

EMISSIONS REQUIREMENTS 9

Summary 9

Radiated Emissions 10

Radiated Emissions Summary 10

Radiated Emissions Test Setup 10

Radiated Emissions Test Execution 11

Radiated Emissions Data 11

IMMUNITY COMPATIBILITY TESTING 12

Immunity to Radio-Frequency Electromagnetic Field 12

Radio-Frequency Electromagnetic Field Summary 12

Radio-Frequency Electromagnetic Field Test Setup 12

Radio-Frequency Electromagnetic Field Test Execution 13

Immunity to Electrostatic Discharge 14

Electrostatic Discharge Summary 14
Electrostatic Discharge Test Setup 14
Electrostatic Discharge Test Execution 15

ANNEX 16

A1 Test Plan 17
A1.1 Scope 17
A1.2 Reference Documents 17
A1.3 Operating/Functional Conditions 18
A1.4 EMI/EMC Product Compliance 18
A1.4.1 Radiated Emissions, EN 55022 18
A1.4.2 Immunity to Radiated Electromagnetic Fields 18
A1.4.3 Immunity to Electro Static Discharge 19
A2 Equipment and Configuration 20
A3 EN 301 489-1 International Standard-Table 5 20
A4 EN 55022 International Standard Tables 6 and 8 20
A5 IEC 61000-4-3 International Standard Figure 2 21
A6 IEC 61000-4-2 International Standard Figure 6 22
A7 IEC 61000-4-4 International Standard Figure 7 23
A8 IEC 61000-4-4 International Standard Figure 5 23
A9 Photographs of Equipment and Test Setups 24
A9.1 Photographs of Equipment Under Test 24
A9.2 Radiated Emissions Test set up Photograph 27
A9.3 Radiated Field Immunity Test set up Photograph 28
A9.4 Electrostatic Discharge Immunity Test set up Photograph 28
A10 Test Equipment List for Rogers Labs, Inc. 29
A11 Qualifications 30
A12 FCC Site Registration Letter 31
A13 Industry Canada Site Registration Letter 32

Revisions

Revision 1 Issued April 9, 2014

Executive Summary

The requested electromagnetic compatibility tests required for demonstration of compliance with the International Standards EN 301 489-1, EN 301 489-3 and EN 61000-6-1 have been conducted on the FirstVu HD. The results have been reviewed and found the equipment to demonstrate compliance with all requirements investigated. The EUT described in this report was tested for compliance of International Standards including the following:

EN 301 489-1 Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-3 Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz

EN 61000-6-1 Electromagnetic compatibility (EMC) – Generic standards – Immunity for residential, commercial, and light-industry environments

EN 61000-4-3 Testing and measurement techniques – Electromagnetic Compatibility Part 4: Testing and Measurement Techniques; Section 3: Radiated, Radio Frequency, Electromagnetic Field Immunity Test

Test Performed	Results
Emissions	Complies
Immunity to Electrostatic Discharge	Complies
Immunity to Radio Frequency Electromagnetic Field	Complies

Name of Applicant: Digital Ally
9705 Loiret Blvd
Lenexa, KS 66219

Model: FirstVu HD

Environmental Conditions

Ambient Temperature	20.6° C
Relative Humidity	35%
Atmospheric Pressure	1015.6 mb

Introduction

Purpose

The purpose of this report is to document the Electromagnetic Compatibility of FirstVu HD as outlined by EN 301 489-1, EN 301 489-3, and EN 55024, and EN 61000-6-1.

Scope

This report applies to the FirstVu HD manufactured by Digital Ally

References

ETSI EN 301 489-1 v1.9.1: Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-3 Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz

EN 55024:1998 Information technology equipment – Immunity characteristics – Limits and methods of measurement

EN 61000-6-1Electromagnetic Compatibility (EMC) Part 6-1: Generic standards – Immunity for residential, commercial and light-industrial environments

EN 61000-4-2 Electromagnetic Compatibility Part 4: Testing and Measurement Techniques – Section 2: Electrostatic Discharge Immunity Test

EN 61000-4-3 Electromagnetic Compatibility Part 4: Testing and Measurement Techniques – Section 3: Radiated, Radio Frequency, Electromagnetic Field Immunity Test

Definitions

EUT - Equipment Under Test

Immunity Criteria - The Immunity Criteria outlined in the EMI/EMC Test Plan as applied to all referenced tests.

Equipment and Cable Configuration

Equipment Tested

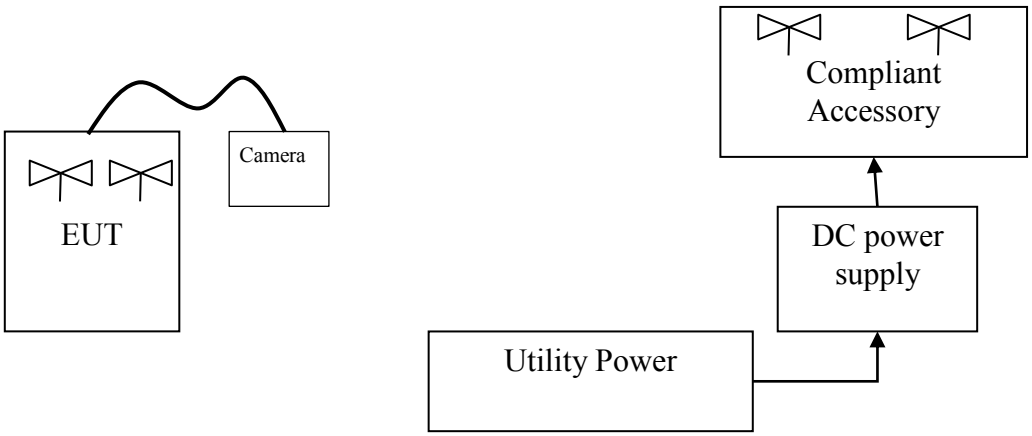
Equipment	Model	FCC I.D.
EUT	FirstVu HD	WPZ-FISTVU

Test results in this report relate only to the items tested.

Equipment Function

The EUT is a portable video recording device incorporating transceiver circuitry in the 2412-2462 MHz frequency band. The transceiver system provides switching ability for remote activation of compliant equipment. The design utilizes permanently attached PCB mounted chip antenna. For testing purposes, the FirstVu HD transceiver was paired with manufacturer provided equipment for frequency selection and activation. This configuration provided operational control of the EUT. The FirstVu HD offers two ports for connection with proprietary compliant USB equipment only and offers no other interface ports. For testing purposes, the FirstVu HD received powered from the rechargeable 3.7-volt battery and was configured to transmit in available modes. As requested by the manufacturer and required by regulations, the equipment was tested for emissions compliance using the available configurations with the worst-case data presented. Test results in this report relate only to the products described in this report.

Equipment Configuration



Emissions Requirements

Summary

The EUT was tested for demonstration compliance of emissions and immunity as defined in EN 301 489-1. Testing was performed for demonstration of compliance to the limits and methods of measurements per EN 55022, RSS-GEN, EN 61000-6-3, ICES-003, CFR 47 parts 15B and 15C and other relevant standards as presented in supporting documentation. The system tested demonstrated compliance with emissions requirements of EN 301 489-1 and EN 301 489-3.

Radiated Emissions

Radiated Emissions Summary

The product described in this report was tested for compliance with the EN55022 Class B Radio Disturbance Standard. The EUT was tested in accordance with the limits specified in the EN55022 Document. The test site and procedures follow the requirements set forth in Paragraph 10 of the EN55022 Document.

Radiated Electromagnetic Interference per Par. 6, Table 4, Class B Information and Technology Equipment

Frequency Range (MHz)	Limit (dBµV/m @10m)	Results
30 to 230	30 (Quasi Peak)	Complies
230 to 1000	37 (Quasi Peak)	Complies
1000 to 3000	50 / 70 (Ave / Peak)	Complies
3000 to 6000	54 / 74 (Ave / Peak)	Complies

Radiated Emissions Test Setup

Radiated emissions from the EUT were obtained on a validated test site using test procedures defined in the EN55022 Document. The EUT was configured as the test sample was provided and powered on during testing. The EUT was placed on a wooden table located in a screen room with the FSM (Field Strength Measuring) antenna located at a 1-meter distance. The frequency spectrum from 30 MHz to 12,000 MHz was scanned for initial screening. The worst-case configuration was then setup at the 3 meters open area test site (OATS) and the radiated emissions data then taken. The EUT was placed on a 1 x 1.5 meter rotating wooden bench 1.5 meters above the ground plane, positioned 3 meters from the FSM antenna, located at the open area test site. The radiated emission amplitudes were maximized by changing cable locations, rotating the turntable and varying the antenna height and polarization before final data was recorded. Data was taken at a 3 meters distance then conversion calculations were made for 3 meters field strength using the following formula:

FS = Received field strength, AF = Receive antenna factor, Amp Gain = Preamplifier gain stage

$$dB\mu V/m @ 3m = FS (dB\mu V) + AF (dB) - Amp\ Gain (dB)$$

Radiated Emissions Test Execution

Preliminary testing was performed in a screen room. Radiated emissions measurements were performed with the EUT positioned 1 meter from the receive antenna. The frequency spectrum from 30 MHz to 12,000 MHz was investigated to identify frequencies that produced the highest emissions. The EUT was arranged in with the test sample configuration and operated in a standard mode. The EUT, supporting equipment, and cable locations were noted and reconfigured at the final test site. The highest radiated emission was then maximized at the Open Area Test Site location before final radiated emissions measurements were performed. Final data was taken with the EUT located at the Open Area Test Site at a distance of 3 meters between the EUT and receiving antenna. The frequency spectrum from 30 MHz to 12,000 MHz was searched for radiated emissions. Emissions were maximized by EUT placement on the turntable, changing cable location, rotating the turntable, and varying the antenna height and polarization. Antennas used were Broadband Biconical from 30 to 200 MHz, Log Periodic from 200 MHz to 5 GHz, double ridge horn from 1 to 12 GHz, and/or a Biconilog from 30 MHz to 1200 MHz.

Radiated Emissions Data

Frequency (MHz)	FSM Hor. Peak (dBµV)	FSM Hor. Ave (dBµV)	FSM Vert. Peak (dBµV)	FSM Vert. Ave (dBµV)	CISPR 22 Limit (dBµV/m) @ 3m
2390.0	39.3	26.7	39.4	26.5	54.0
2400.0	51.7	27.4	44.6	26.6	54.0
2483.5	41.6	27.4	40.0	27.2	54.0

Other emissions present had amplitudes at least 20 dB below the limit.

Immunity Compatibility Testing

Immunity to Radio-Frequency Electromagnetic Field

Radio-Frequency Electromagnetic Field Summary

The EUT described in this report was tested for compliance with the International Standards ETSI EN 301 489-1, ETSI EN 301-489-3, EN55024, EN 61000-6-1, and EN 61000-4-3 Standards for Immunity to Radio-Frequency Electromagnetic Field Interference as described.

Immunity to Radio-Frequency Electromagnetic Field Interference 3 V/m (unmodulated) strength, Tested with 80% Amplitude Modulated 1 kHz Sine wave.

Frequency Range (MHz)	Amplitude	Results
80 - 1000	3 (v/m)	Complies
1000 – 2700	3 (v/m)	Complies

Radio-Frequency Electromagnetic Field Test Setup

The test procedure used conforms to the Guidelines set out in the International Standard EN 61000-4-3. The EUT was placed on a 0.8-meter high wooden table located in a shielded enclosure. The EUT was positioned a minimum of 0.8 meters from all surrounding walls. The ground plane in the shielded enclosure is connected to the protective earth ("ground" in U.S. terminology). The EUT was arranged as described by the manufacturer and connected such that all of its functional requirements were met. The EUT was communicating with compliant accessory equipment and monitored with a test system allowing verification of operational status of the unit at a distance according to the manufacturer's instructions. The EUT and supporting components of the system were positioned similar to the typical test setup as shown in EN 61000-4-3. All wiring between enclosures of the EUT was the manufacturers specified wiring type and connectors.

Radio-Frequency Electromagnetic Field Test Execution

The EUT and support equipment were subjected to a uniform electromagnetic field of strength 3 volts/meters (unmodulated) in the frequency band of 80 MHz to 2700 MHz. These tests were performed using Biconical and Log Periodic Antennas as described in the EN 61000-4-3 International Standard. Both horizontal and vertical polarizations were investigated for this test. The frequency range was swept using signal 80% amplitude modulated with a 1 kHz sine wave, pausing to adjust the signal level and antennas as necessary. The sweep rate did not exceed 1.5 X 10^{-3} decades/second, leaving enough dwell time at each frequency for the EUT to be exercised and able to respond. Performance criterion A was specified by the manufacturer and stated in the EN 61000-6-1 European Standard. This criterion specifies that the EUT shall continue to operate as intended. No degradation of performance or loss of function is allowed below a performance level specified by the manufacturer. The performance of the EUT was not degraded below the performance levels specified in the test plan. The equipment did not become unsafe or dangerous as a result of these tests.

Immunity to Electrostatic Discharge

Electrostatic Discharge Summary

The EUT described in this report was tested for compliance with ETSI EN 301 489-1, ETSI EN 301-489-3, EN55024, EN 61000-6-1, and EN 61000-4-2 Standard for Immunity to Electrostatic Discharge as described in Table 1 of that Document.

Immunity to Electrostatic Discharge 8 kV (charge voltage) Air Discharge Method

Test Voltage kV	Results
Air Discharge Level of 2 kV	Complies
Air Discharge Level of 4 kV	Complies
Air Discharge Level of 8 kV	Complies

Immunity to Electrostatic Discharge 4 kV (charge voltage) Contact Discharge Method

Test Voltage kV	Results
Contact Discharge Level of 1 kV	Complies
Contact Discharge Level of 2 kV	Complies
Contact Discharge Level of 4 kV	Complies

Electrostatic Discharge Test Setup

The test procedure used conforms to the Guidelines set out in the International Standard EN 61000-4-2. The EUT was placed above a metal plated wooden tabletop 0.8 meters above the ground plane located in a screen room. The ground plane in the screen room is connected to the protective earth ("ground" in U.S. terminology). The metal plated tabletop functions as the horizontal coupling plane (HCP) for indirect discharges. This plane is coupled to the ground plane through two 470KΩ resistors in series. A metal plate 0.5m X 0.5m was positioned above the copper plate (HCP) standing vertically as shown in the standard as the vertical coupling plane (VCP). This plate is also coupled to the ground plane through two 470KΩ resistors in series.

The EUT was connected to the earthing system as described by the manufacturer's installation specifications. The position of the signal and power lines were representative of those used in a typical installation.

Electrostatic Discharge Test Execution

The EUT was subjected to electrostatic discharges of voltages of 2.0, 4.0, 6.0 and 8.0 kV using the Air Discharge Test Method as described in EN 61000-4-2. Polarity of the test voltage was set to both positive and negative as described in the EN 61000-4-2 International Standard. Testing was performed using both direct and indirect application of the discharges to the EUT. The direct application static electricity discharges were applied to all surfaces and points of the EUT, which were accessible to an operator during normal usage. Evaluation of the immunity test was based on performance criterion B as specified by the manufacturer and the International Standard EN 61000-4-2. This criterion specifies that the EUT shall continue to operate as intended after the test. Temporary degradation or loss of function or performance, which is self-recoverable, is allowed as long as it is not degraded below a performance level specified by the manufacturer, when the EUT is used as intended. During the test, degradation of performance is however allowed. No change of actual operating state or stored data is allowed. The performance of the EUT was not affected or degraded below the manufacturers specified level during testing. The equipment did not become unsafe, dangerous or exhibit any damage to components as a result of these tests.

Annex

A1 EMI/EMC Test Plan

A2 Equipment & Configuration

A3 EN 301 489-1 International Standard Table 5

A4 EN 55022 International Standard Tables 6 and 8

A5 IEC 61000-4-3 International Standard Figure 2

A6 IEC 61000-4-2 International Standard Figure 6

A7 IEC 61000-4-4 International Standard Figure 7

A8 IEC 61000-4-4 International Standard Figure 5

A9 Photographs of Equipment and Test Setups

A10 Rogers Labs Test Equipment List

A11 Rogers Qualifications

A12 FCC Site Registration Letter

A13 Industry Canada Site Registration Letter

A1 Test Plan

A1.1 Scope

This document describes the current Electromagnetic Emissions and Immunity requirements necessary to demonstrate compliance with EN 301 489-3. In addition, this document describes how the compliance requirements are applied to Digital Ally, Model: FirstVu HD, and how conformance determined.

A1.2 Reference Documents

ETSI EN 301 489-1 v1.9.1: Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

ETSI EN 301 489-3 v1.5.1: Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz

EN 61000-6.1 Generic standards – Immunity for residential, commercial and light—industrial environments

EN 55022 (CISPR 22) - Limits and Methods of Measurements of Radio Disturbance Characteristics of Information Technology Equipment.

EN 55024 (CISPR 24) - Information technology equipment – Immunity characteristics – Limits and methods of measurement

IEC 61000-4-2 - Electromagnetic Compatibility Part 4: Testing and Measurement Techniques; Section 2: Electrostatic Discharge Immunity Test.

IEC 61000-4-3 - Electromagnetic Compatibility Part 4: Testing and Measurement Techniques, Section 3: Radiated, Radio Frequency, Electromagnetic Field Immunity Test

A1.3 Operating/Functional Conditions

Product's Function/Service/Use:

The FirstVu HD incorporates a low power transmitter with operation capability in the band of 2412-2462 MHz. The equipment offers wireless communication capability with compliant 2412-2462 MHz equipment. The unit operates from power received from the installation vehicle power. The EUT was arranged as a test system emulating typical user equipment configuration during testing.

Performance criteria:

The EUT when subjected to the requirements specified in each test shall continue to be operational. Operational is defined as no loss of function of the system. Any loss of function during a test must be repeatable within ten attempts. The system must not become hazardous to operate and must remain in a safe and stable state of operation. The system must not require repair, adjustment, or part replacement to restore operation.

A1.4 EMI/EMC Product Compliance

A1.4.1 Radiated Emissions, EN 55022

Specification/Conformance:

The FirstVu HD operating according to Section A1.1.3, must demonstrate compliance with EN 55022 Class B requirements for Radiated Electromagnetic Interference.

A1.4.2 Immunity to Radiated Electromagnetic Fields

Specification/Conformance:

The FirstVu HD must demonstrate compliance with the performance criteria according to Section A1.1.3. The FirstVu HD operated as per Section A1.1.3 must demonstrate compliance with the requirements of EN 61000-4-3. As outlined in the standards at severity level of field strength of 3 V/m for 80-2000 MHz and 3 V/m for 2000-2700 MHz. The unit shall function as described in Performance Criteria A as specified.

Definition of Performance Criteria A:

The equipment shall continue to operate as intended without operator intervention. No degradation of performance or loss of function is allowed below a performance level specified by the manufacturer when the equipment is used as intended. The performance level may be replaced by a permissible loss of performance. If the minimum performance level or the permissible performance loss is not specified by the manufacturer, then either of these may be derived from the product description and documentation, and by what the user may reasonably expect from the equipment if used as intended. The EUT when subjected to the requirements of the Radiated Electromagnetic Fields Test shall continue to be operational. Operational is defined as described in A1.1.3. The EUT must not become unsafe or dangerous because of these tests.

A1.4.3 Immunity to Electro Static Discharge

Specification/Conformance:

The FirstVu HD operated as per Section A1.1.3 shall demonstrate compliance with IEC 61000-4-2 requirements at severity level of 4 and 8 kV, and satisfy Performance Criteria B as specified.

Definition of Performance Criteria B:

After the test, the equipment shall continue to operate as intended without operator intervention. No degradation of performance or loss of function is allowed, after the application of the phenomena below a performance level specified by the manufacturer, when the equipment is used as intended. The performance level may be replaced by a permissible loss of performance. During the test, degradation of performance is however allowed. However, no change of actual operating state or stored data is allowed to persist after the test. If the minimum performance level (or the permissible performance loss) is not specified by the manufacturer, then either of these may be derived from the product description and documentation, and what the user may reasonably expect from the equipment if used as intended. Operational is defined as described in A1.1.3. The EUT must not become unsafe or dangerous because of these tests.

A2 Equipment and Configuration

The FirstVu HD shall be tested in the manufacturer-defined mode emulating typical worst-case operational conditions. Power will be supplied through the manufacturers supplied power cord. The test system provides for visual and support equipment monitoring of EUT activity and performance to identify EUT function.

A3 EN 301 489-1 International Standard-Table 5

Table 5: Limits for conducted emissions

Frequency range	Limit (quasi-peak) (dBµV)	Limit (average) (dBµV)
0,15 MHz to 0,5 MHz	66 to 56	56 to 46
> 0,5 MHz to 5 MHz	56	46
> 5 MHz to 30 MHz	60	50
NOTE: The limit decreases linearly with the logarithm of the frequency in the range 0,15 MHz to 0,50 MHz.		

A4 EN 55022 International Standard Tables 6 and 8

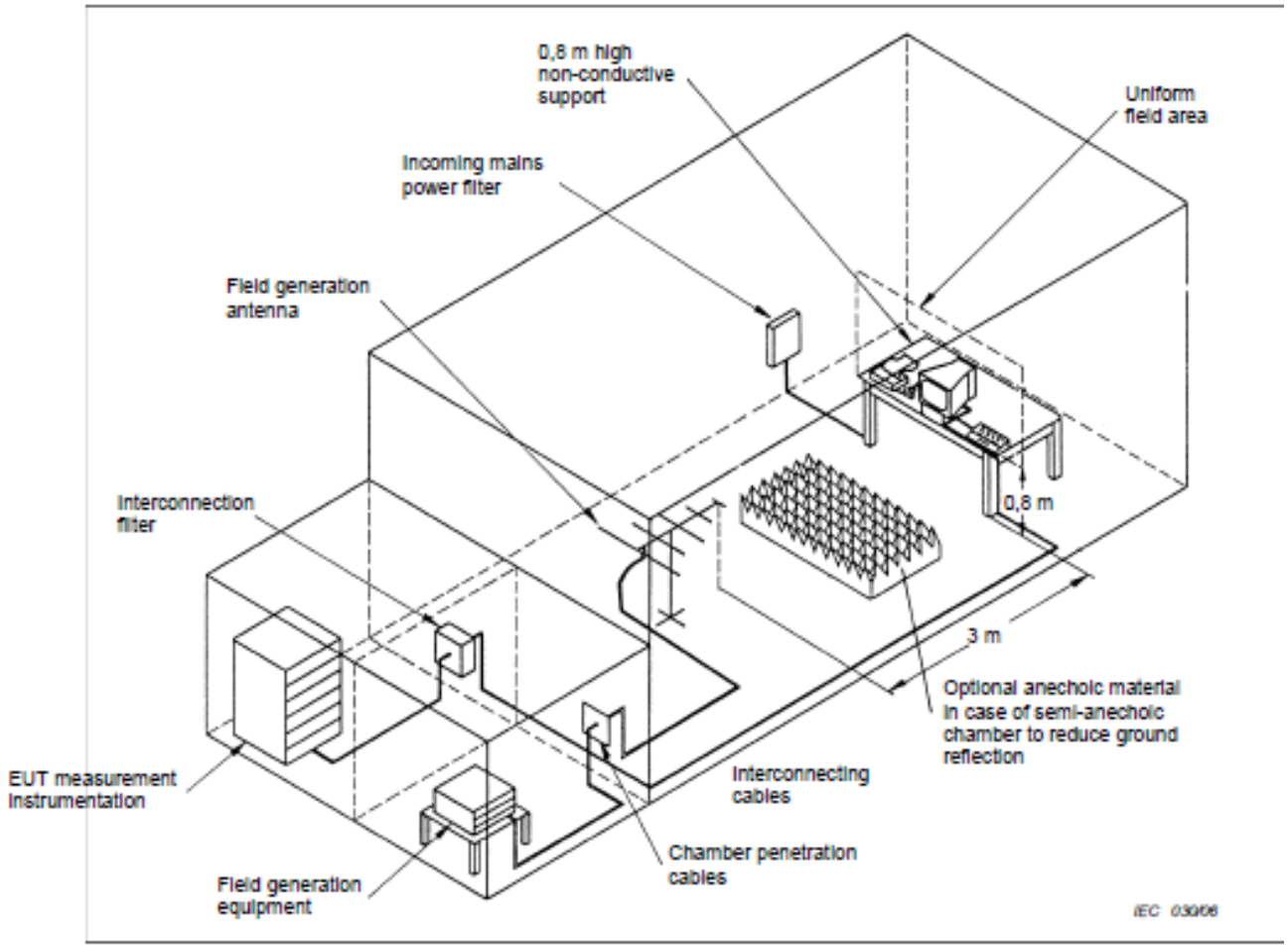
Table 6 – Limits for radiated disturbance of class B ITE at a measuring distance of 10 m

Frequency range MHz	Quasi-peak limits dB(µV/m)
30 to 230	30
230 to 1 000	37
NOTE 1 The lower limit shall apply at the transition frequency. NOTE 2 Additional provisions may be required for cases where interference occurs.	

Table 8 – Limits for radiated disturbance of Class B ITE at a measurement distance of 3 m

Frequency range GHz	Average limit dB(µV/m)	Peak limit dB(µV/m)
1 to 3	50	70
3 to 6	54	74
NOTE The lower limit applies at the transition frequency.		

A5 IEC 61000-4-3 International Standard Figure 2



NOTE Anechoic lining material on walls and ceiling has been omitted for clarity.

Figure 2 – Example of suitable test facility

A6 IEC 61000-4-2 International Standard Figure 6

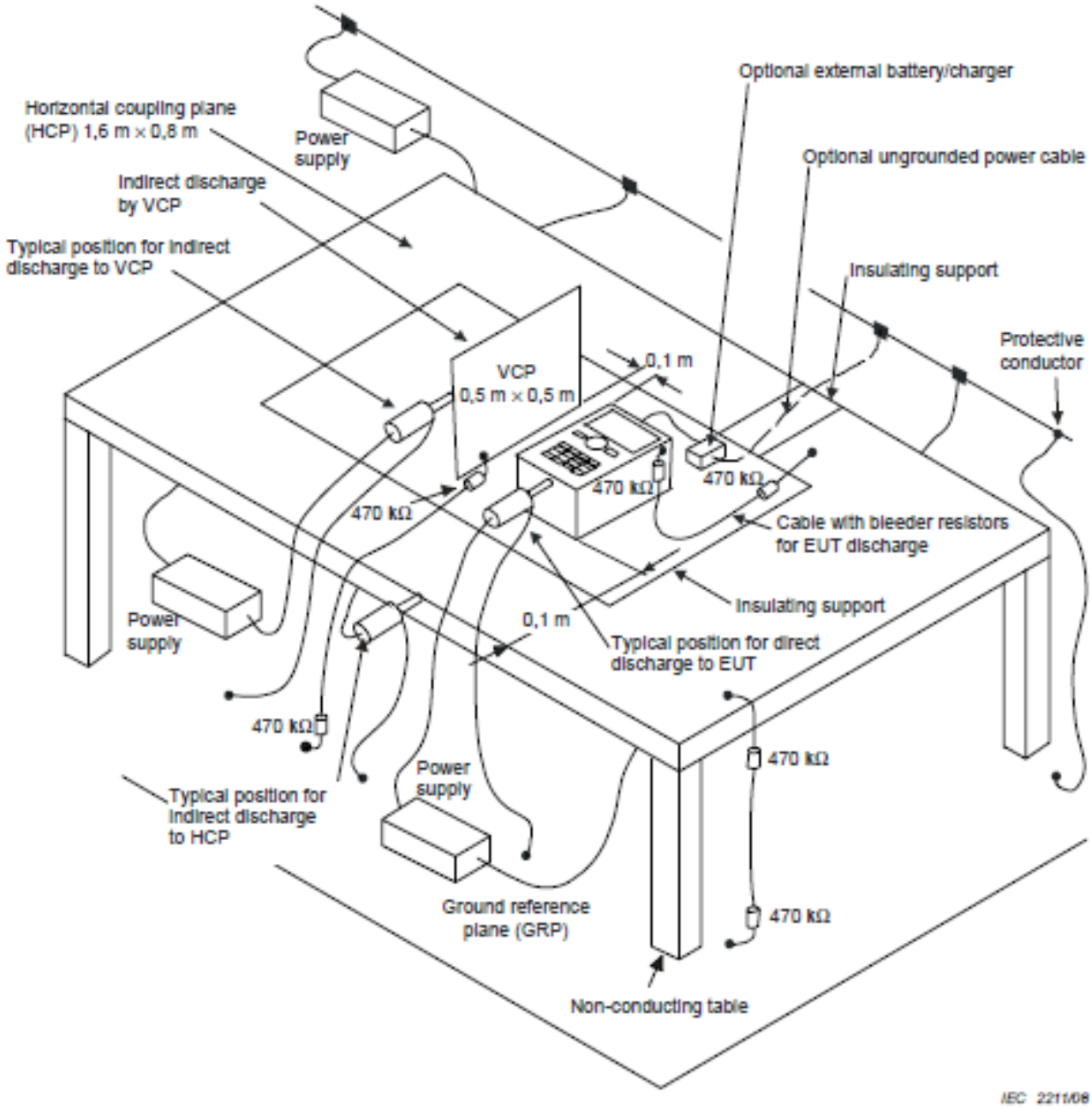
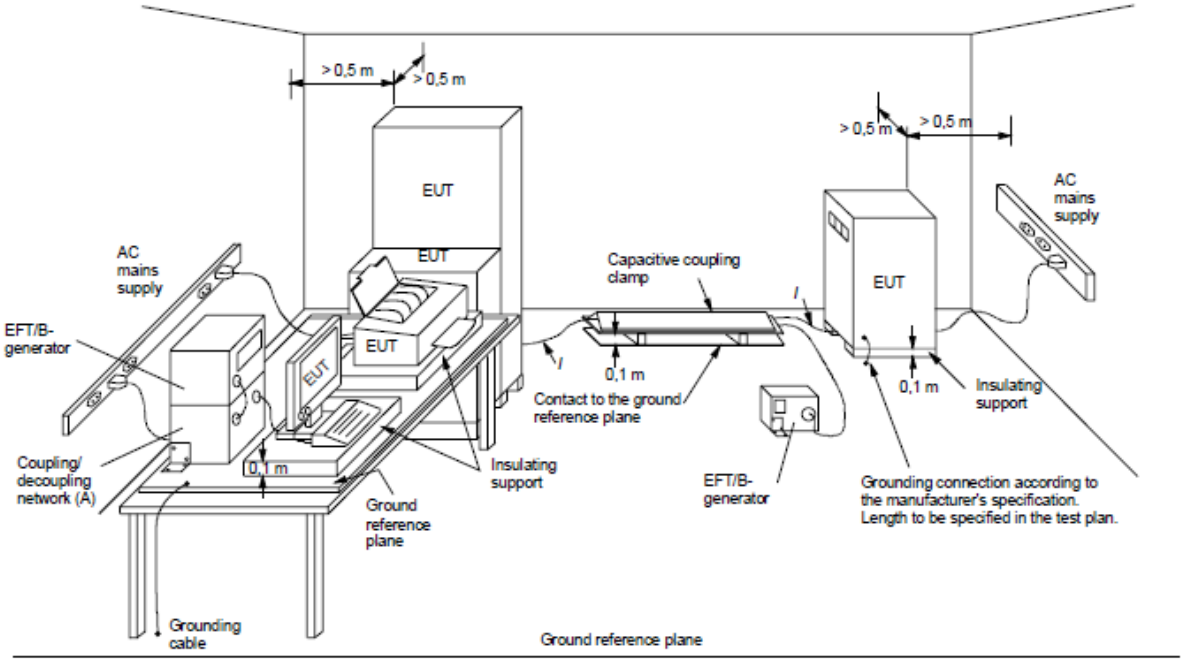


Figure 6 – Example of a test setup for ungrounded table-top equipment

A7 IEC 61000-4-4 International Standard Figure 7



Key

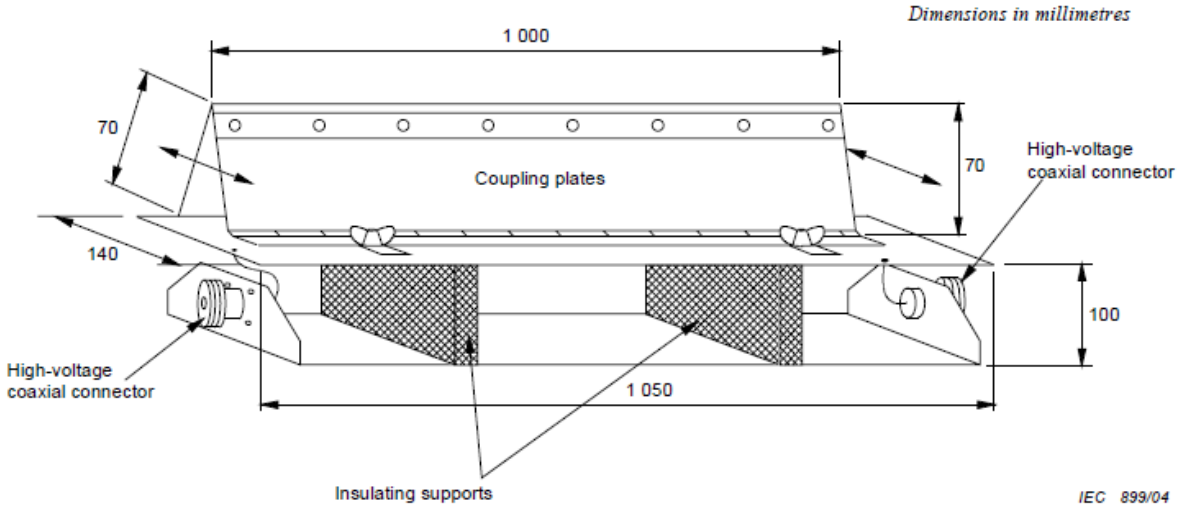
l length between clamp and the EUT to be tested (should be 0,5 m ± 0,05 m)

(A) location for supply line coupling

(B) location for signal lines coupling

Figure 7 – General test set-up for laboratory type tests

A8 IEC 61000-4-4 International Standard Figure 5

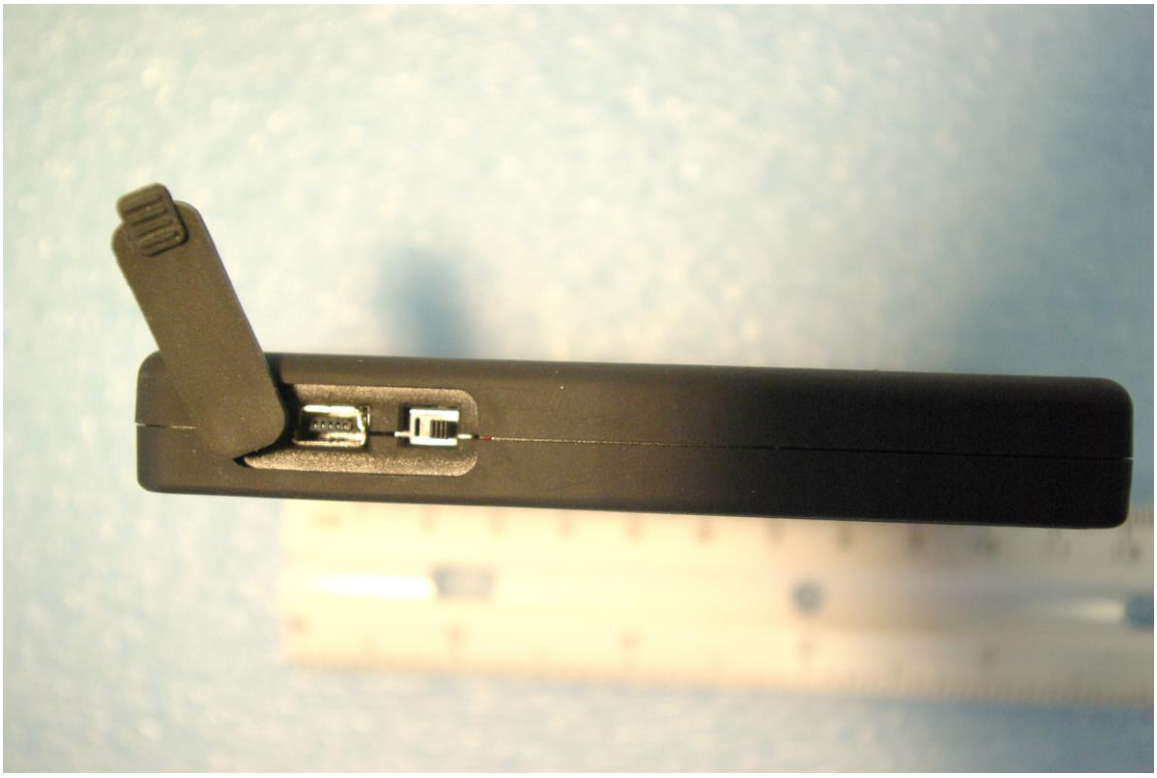


Warning The distance of the coupling section to all other conductive constructions except to the cable under test and the ground plane shall be more than 0,5 m.

Figure 5 – Construction of the capacitive coupling clamp

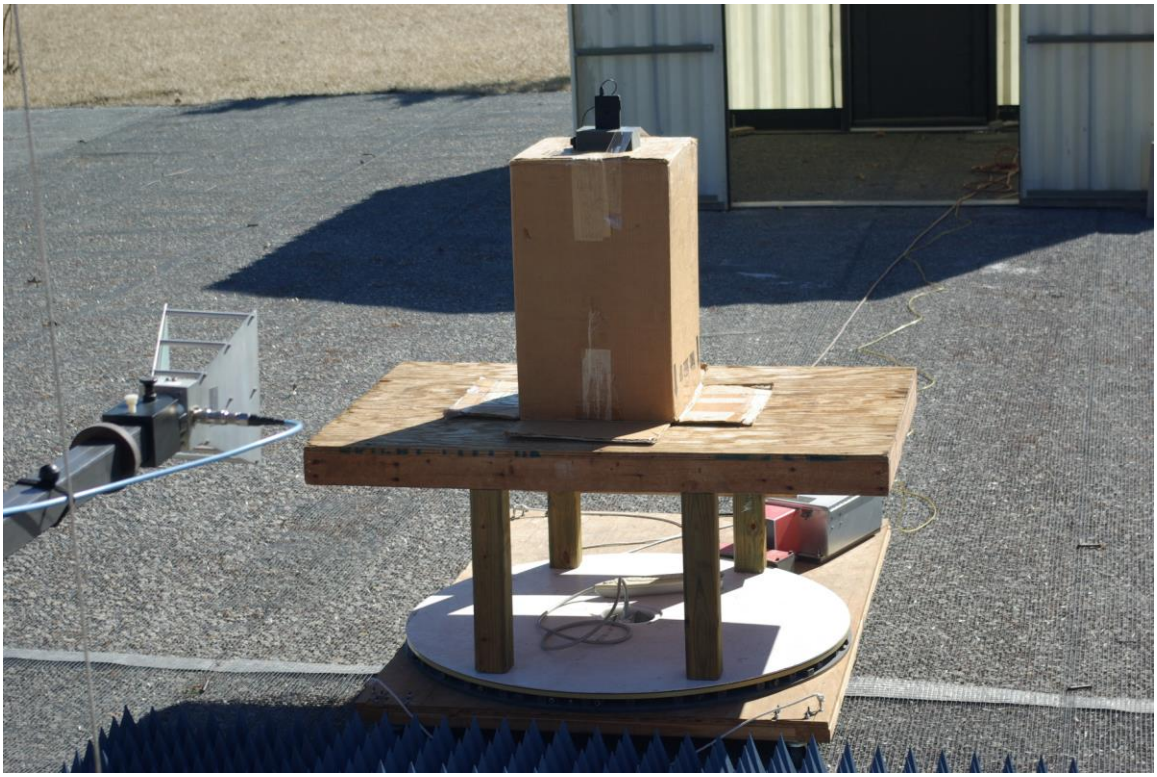
A9 Photographs of Equipment and Test Setups

A9.1 Photographs of Equipment Under Test

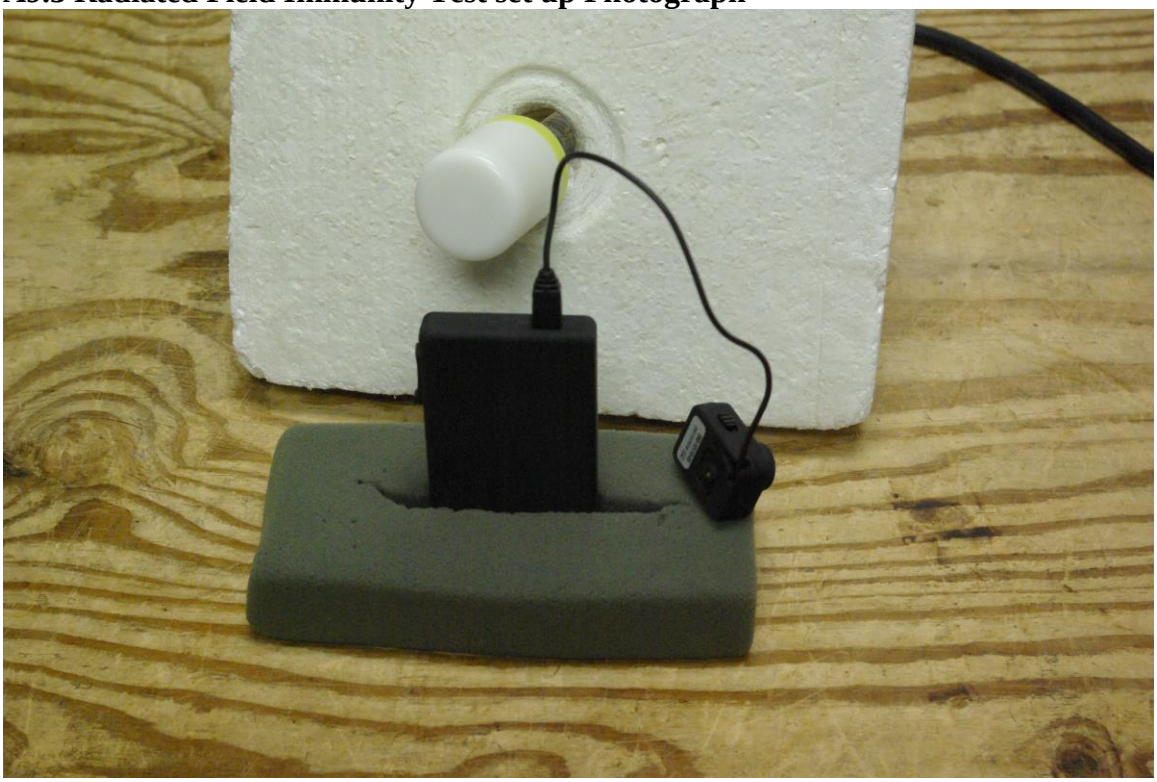


Digital·Ally
00-10-101-050

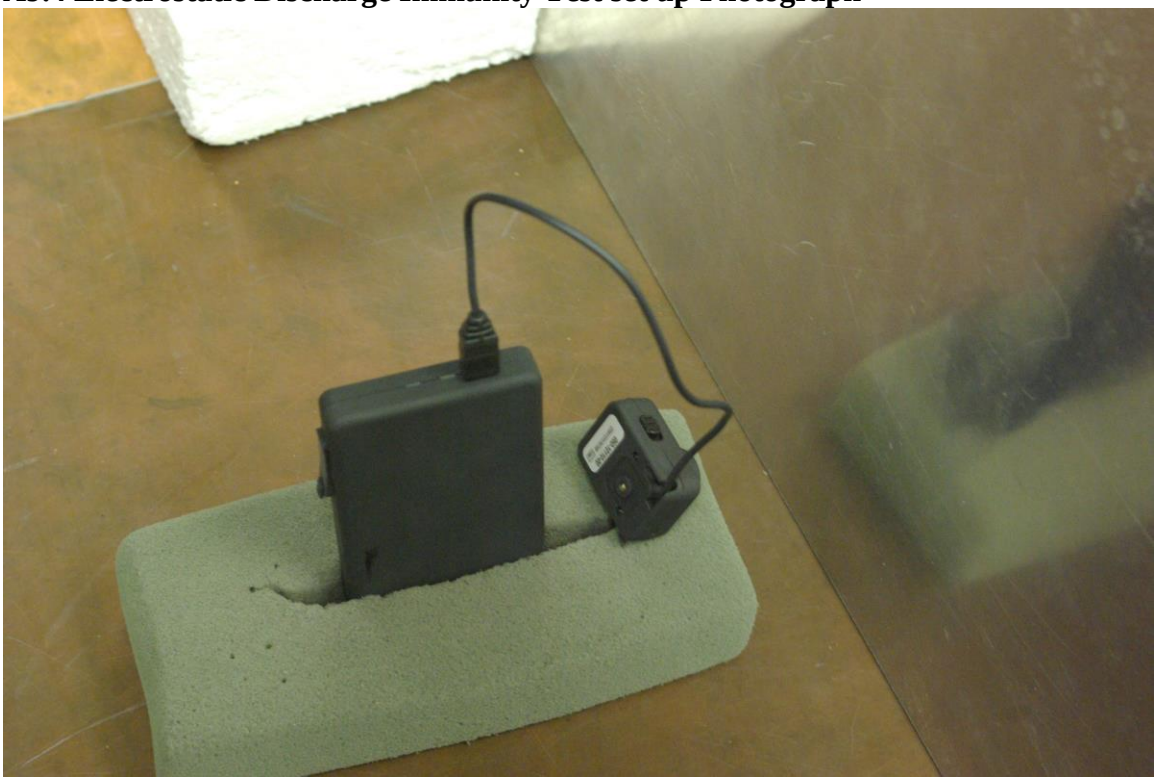
A9.2 Radiated Emissions Test set up Photograph



A9.3 Radiated Field Immunity Test set up Photograph



A9.4 Electrostatic Discharge Immunity Test set up Photograph



A10 Test Equipment List for Rogers Labs, Inc.

Equipment (Serial Number)	Calibration Due
Spectrum Analyzer: Rohde & Schwarz ESU40 (100108)	5/14
Spectrum Analyzer: HP 8562A, 11518, 11519, and 11520 (3051A05950)	5/14
Mixers: 11517A, 11970A, 11970K, 11970U, 11970V, 11970W	
Spectrum Analyzer: HP 8591EM (3628A00871)	5/14
Antenna: EMCO Biconilog Model: 3143 (9607-1277)	5/14
Antenna: Sunol Biconilog Model: JB6 (A100709)	10/14
Antenna: EMCO Log Periodic Model: 3147 (40582)	10/14
Antenna: Com Power Model: AH-118 (10110)	10/14
Antenna: Com Power Model: AH-840 (101046)	10/14
Antenna: Antenna Research Biconical Model: BCD 235 (169)	10/14
Antenna: EMCO 6509 (9502-1374)	10/14
LISN: Compliance Design Model: FCC-LISN-2.Mod.cd (126)	10/14
R.F. Preamp Com-Power Model: CPPA-102 (01254)	10/14
Cable: Belden RG-58 (L1-CAT3-11590)	10/14
Cable: Belden RG-58 (L2-CAT3-11590)	10/14
Cable: Belden 8268 (L3)	10/14
Cable: Time Microwave: 4M-750HF290-750 (L4M)	10/14
Cable: Time Microwave: 10M-750HF290-750 (L10M)	10/14
Frequency Counter: Leader LDC825	2/14
Oscilloscope Scope: Tektronix 2230	2/14
Wattmeter: Bird 43 with Load Bird 8085	2/14
Power Supplies: Sorensen SRL 20-25, SRL 40-25, DCR 150, DCR 140	2/14
R.F. Generators: HP 606A, HP 8614A, HP 8640B	2/14
R.F. Power Amp 65W Model: 470-A-1010	2/14
R.F. Power Amp 50W M185- 10-501	2/14
R.F. Power Amp A.R. Model: 10W 1010M7	2/14
R.F. Power Amp EIN Model: A301	2/14
LISN: Compliance Eng. Model 240/20	2/14
LISN: Fischer Custom Communications Model: FCC-LISN-50-16-2-08	2/14
Antenna: EMCO Dipole Set 3121C	2/14
Antenna: C.D. B-101	2/14
Antenna: Solar 9229-1 & 9230-1	2/14
Audio Oscillator: H.P. 201CD	2/14
AC Power Source: Ametek 3001IX-CTS-EOS1 (352A00713)	2/14
EMC Test System Transient Tester: EMC Specialists (TR-3000 F-S-D-V-1529)	2/14
ESD Test Set 2010i	2/14
Fast Transient Burst Generator Model: EFT/B-101	2/14
Field Intensity Meter: EFM-018	2/14
KEYTEK Ecat Surge Generator	2/14

A11 Qualifications

Scot D. Rogers, Engineer

Rogers Labs, Inc.

Mr. Rogers has approximately 17 years' experience in the field of electronics. Working experience includes six years working in the automated controls industry and 6 years working with the design, development and testing of radio communications and electronic equipment.

Positions Held:

Systems Engineer:	A/C Controls Mfg. Co., Inc.	6 Years
Electrical Engineer:	Rogers Consulting Labs, Inc.	5 Years
Electrical Engineer:	Rogers Labs, Inc.	Current

Educational Background:

Bachelor of Science Degree in Electrical Engineering from Kansas State University

Bachelor of Science Degree in Business Administration Kansas State University

Several Specialized Training courses and seminars pertaining to Microprocessors and Software programming

A12 FCC Site Registration Letter

FEDERAL COMMUNICATIONS COMMISSION

Laboratory Division
7435 Oakland Mills Road
Columbia, MD 21046

June 28, 2013

Registration Number: 90910

Rogers Labs, Inc.
4405 West 259th Terrace,
Louisburg, KS 66053

Attention: Scot Rogers,

Re: Measurement facility located at Louisburg
3 & 10 meter site
Date of Renewal: June 28, 2013

Dear Sir or Madam:

Your request for renewal of the registration of the subject measurement facility has been received. The information submitted has been placed in your file and the registration has been renewed. The name of your organization will remain on the list of facilities whose measurement data will be accepted in conjunction with applications for Certification under Parts 15 or 18 of the Commission's Rules. Please note that the file must be updated for any changes made to the facility and the registration must be renewed at least every three years.

Measurement facilities that have indicated that they are available to the public to perform measurement services on a fee basis may be found on the FCC website www.fcc.gov under E-Filing, OET Equipment Authorization Electronic Filing, Test Firms.

Sincerely,

Phyllis Parrish
Industry Analyst

A13 Industry Canada Site Registration Letter

Industry Canada Industrie Canada

June 19, 2013

OUR FILE: 46405-3041
Submission No: 168037

Rogers Labs Inc.
4405 West 259th Terrace
Louisburg
KS, USA
66053

Attention: Mr. Scot D. Rogers

Dear Sir:

The Bureau has received your application for the renewal of 3/10m OATS. Be advised that the information received was satisfactory to Industry Canada. The following number(s) is now associated to the site(s) for which registration / renewal was sought **(Site# 3041A-1).** Please reference the appropriate site number in the body of test reports containing measurements performed on the site. In addition, please keep for your records the following information;

- The company address code associated to the site(s) located at the above address is: **3041A**

Furthermore, to obtain or renew a unique site number, the applicant shall demonstrate that the site has been accredited to ANSI C63.4-2003 or later. A scope of accreditation indicating the accreditation by a recognized accreditation body to ANSI C63.4-2003 or later shall be accepted. Please indicate in a letter the previous assigned site number if applicable and the type of site (example: 3 metre OATS or 3 metre chamber). If the test facility is not accredited to ANSI C63.4-2003 or later, the test facility shall submit test data demonstrating full compliance with the ANSI standard. The Bureau will evaluate the filing to determine if recognition shall be granted.

The frequency for re-validation of the test site and the information that is required to be filed or retained by the testing party shall comply with the requirements established by the accrediting organization. However, in all cases, test site re-validation shall occur on an interval not to **exceed three years**. There is no fee or form associated with an OATS filing. OATS submissions are encouraged to be submitted electronically to the Bureau using the following URL;
http://strategis.ic.gc.ca/epic/internet/inceb-bhst.nsf/en/h_tt00052e.html.

If you have any questions, you may contact the Bureau by e-mail at certification.bureau@ic.gc.ca Please reference our file and submission number above for all correspondence.

Yours sincerely,

Bill Payn
For: Wireless Laboratory Manager
Certification and Engineering Bureau
3701 Carling Ave., Building 94
P.O. Box 11490, Station "H"
Ottawa, Ontario K2H 8S2
Email: Bill.Payn@ic.gc.ca
Tel. No. (613) 990-3639
Fax. No. (613) 990-4752

ROGERS LABS, INC.

4405 West 259th Terrace
Louisburg, KS 66053
Phone / Fax (913) 837-3214

May 13, 2013

Mr. Matt Andrews
Hardware Engineering Manager
Digital Ally Inc.
9705 Loiret Blvd
Lenexa, KS 66053

RE: FCC Class B Test Report and DoC for Model: First Vu HD

Mr. Andrews:

Enclosed please find the CISPR and FCC Class B Certification Data, Report, and Declaration of Conformity for your aforementioned equipment. The equipment tested demonstrated compliance with CFR 47 15B, CISPR, and ICES-003 requirements for Class B equipment.

Please complete the following to fulfill the requirements for Self-Authorization, additional compliance information is also attached below:

1) Complete the labeling requirements per Sections 2.954, 15.19, 15.21, and 15.105(b).
2) Add schematics and design drawings of the unit to the report.
3) Include a record of the procedures used for production, inspection and testing.
4) Add Owner's/Operator's Manual to report.
5) No FCC submittal is required. Keep a copy of the report and additions on file at Digital Ally Inc. for future reference.

If you have any questions, please do not hesitate to call. Thank you for the opportunity to be of service.

Best Regards,

Scot D Rogers

Scot D. Rogers
Rogers Labs, Inc.

For the Self-Authorization DoC procedures, the following applies:

Information to be included in the owners' manual and/or product label

Per 15.19(a)(5) the following statement shall be displayed in the manual or pamphlet supplied with the device:

> "This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

In addition, per 15.19(b)(3) the device shall also be labeled with one of the following with the text placed on the pamphlet:

First Vu HD

Tested to comply
With FCC Standards

FOR HOME OR OFFICE USE

§15.21 Information to User:

The users' manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

§15.105(b) Information to User:

For a Class B digital device or peripheral, the instructions furnished the user shall include the following or similar statement, placed in a prominent location in the text of the manual:

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Industry Canada compliance procedures, the following applies:

CAN ICES-3(B) / NMB-3(B)

ROGERS LABS, INC.

4405 West 259th Terrace
Louisburg, KS 66053
Phone / Fax (913) 837-3214

ENGINEERING TEST REPORT FORM
For
TESTING to EN 300 440-2 v1.4.1

For
Digital Ally
9705 Loiret Blvd
Lenexa, KS 66219

Model: FirstVu HD

Mobile Short Range Data transmitter
Frequency 2412-2462 MHz
Short Range Device Transmitter class 8

Test Date: February 20, 2014

Certification Date: February 20, 2014

Certifying Engineer: Scot D Rogers

Scot D. Rogers
Rogers Labs, Inc.
4405 West 259th Terrace
Louisburg, KS 66053
Telephone/Facsimile: (913) 837-3214

This report shall not be reproduced except in full, without the written approval of the laboratory. This report must not be used by the client to claim product certification, approval or endorsement by NVLAP, NIST, or any agency of the Federal Government.

Table Of Contents

TABLE OF CONTENTS 2

REVISIONS 2

LIST OF MEASUREMENTS 3

EQUIVALENT ISOTROPICALLY RADIATED POWER (E.I.R.P.) SUB CLAUSE 7.1 ... 4

Limit Sub Clause 7.1.3 4

OPERATING FREQUENCY SUB CLAUSE 7.2 5

TRANSMITTER SPURIOUS EMISSIONS SUB CLAUSE 7.3 6

Transmitter Spurious Emissions (Radiated) Sub Clause 7.3.4 & 7.3.5 6

Limit Sub Clause 7.3.7 6

TRANSMITTER DUTY CYCLE SUB CLAUSE 7.4 7

RECEIVER SPURIOUS EMISSIONS, SUB CLAUSE 8.3.5 7

TEST EQUIPMENT AND ANCILLARIES USED FOR TESTS 8

ADDITIONAL INFORMATION SUPPLEMENTARY TO TEST REPORT 8

PHOTOGRAPHS OF THE EQUIPMENT 9

External photograph front side 9

External photograph Back side 9

Photograph of Test Setup 10

Revisions

Revision 1 Issued April 9, 2014

List of Measurements

The following list of measurements represents the complete list of measurements tested for compliance with ETSI EN 300-440-1.

7.1 Equivalent Isotropically radiated power

7.2 Permitted range of operating frequencies

7.3 Spurious emissions

7.4 Duty cycle

8.3 Receiver Spurious Emissions

Equivalent Isotropically Radiated Power (e.i.r.p.) Sub Clause 7.1

Applicants declared operating frequency band 2402 - 2480 MHz

Lowest frequency 2,412 MHz Highest frequency 2,462 MHz

Rated output power (maximum) < 10 mW

Antenna: The device utilizes an integral antenna with 3-dBi gain.

Bandwidth of measurement receiver 1.0 MHz

Test Conditions		Transmitter peak power (dBm)		
		Lowest frequency	Middle frequency	Highest frequency
T_{nom} 21.1°C	V_{nom} 3.70 V_{dc}	-0.48	-0.42	-0.51
T_{min} -30 °C	V_{min} 3.14 V_{dc}	-0.70	-0.64	-0.73
	V_{max} 4.25 V_{dc}	-0.70	-0.64	-0.73
T_{max} 55 °C	V_{min} 3.14V_{dc}	-1.78	-1.72	-1.81
	V_{max} 4.25 V_{dc}	-1.78	-1.72	-1.81
Maximum deviation from rated output under normal conditions (dB)		0.5	0.5	0.5
Measurement uncertainty (dB)		1.5 dB		

Limit Sub Clause 7.1.3

Class	Radiated peak power (e.i.r.p.) W / dBm		
	1.0 ≤ f ≤ 5.0 GHz	5.0 < f ≤ 20.0 GHz	f < 20.0 GHz
I	10 mW / 10 dBm	210 mW / 14 dBm	100 mW / 20 dBm
II	500 mW / 27 dBm		
III	500 mW / 27 dBm	2 W / 33 dBm	

Reference Number(s) Of Test Equipment Used (for references see test equipment listing).
5, 6, 7, 9, 10, 11, 12, 13

Operating Frequency Sub Clause 7.2

Applicants declared operating frequency band 2402 - 2480 MHz

Lowest frequency 2,412 MHz Highest frequency 2,462 MHz

Rated output power (maximum) < 10 mW

Antenna: The device utilizes an integral antenna with 3-dBi gain.

Bandwidth of measurement receiver 1.0 MHz

Test conditions		Frequency (MHz)
T_{nom} 21.1°C	V_{nom} 12.0V	2402.0
		2473.0
Measurement uncertainty Hz		1000

Band edge limits

Fl = 2400.0 MHz Fh = 2483.5 MHz

Reference Number(s) Of Test Equipment Used (for references see test equipment listing)
5, 6, 7, 9, 10, 11, 12, 13

Transmitter Spurious Emissions Sub Clause 7.3

Transmitter Spurious Emissions (Radiated) Sub Clause 7.3.4 & 7.3.5

Applicants declared operating frequency band 2402 - 2480 MHz
Lowest frequency 2,412 MHz Highest frequency 2,462 MHz
Rated output power (maximum) < 10 mW
Antenna: The device utilizes an integral antenna with 3-dBi gain.
Bandwidth of measurement receiver 1.0 MHz
Transmitter operating Modulated, Frequency static

Frequency (MHz)	Measuring receiver bandwidth (MHz)	Spurious emissions level (µW)
4824.0	1	0.00058
7236.0	1	0.00111
9648.0	1	0.00104
12060.0	1	0.00144
14472.0	1	0.00125
4874.0	1	0.00055
7311.0	1	0.00106
9748.0	1	0.00109
12185.0	1	0.00194
14622.0	1	0.00131
4924.0	1	0.00040
7386.0	1	0.00099
9848.0	1	0.00111
12310.0	1	0.00140
14772.0	1	0.00165
Measurement uncertainty (dB) 4 dB		

Limit Sub Clause 7.3.7

State	47 to 74 MHz 87.5 to 118 MHz 174 to 230 MHz 470 to 862 MHz	Other frequencies ≥ 25 to ≤ 1000 MHz	Frequencies > 1000 MHz
Operating	4 nW	250 nW	1µW
Standby	2 nW	2 nW	20 nW

Reference Number(s) Of Test Equipment Used (for references see test equipment listing)
5, 6, 7, 9, 10, 11, 12, 13

Transmitter Duty Cycle Sub Clause 7.4

Worst-case duty cycle operation could reach Class 4.

Receiver Spurious emissions, Sub clause 8.3.5

Applicants declared operating frequency band 2402 - 2480 MHz

Spurious emissions receiver operating – conducted

Channel Frequency (MHz)	Spurious Emission Frequency (MHz)	Spurious Emission Level (dBm)	Measurement Bandwidth (kHz)
2437.00			1000
			1000
			1000
			1000
Measurement uncertainty 1.5 dB			

Note: No Emissions found less than 20 dB below limit

Limits

Frequency Range	Limit	Measurement Bandwidth
30 MHz to 1 GHz	-57 dBm	100 kHz
1 GHz to 12,75 GHz	-47 dBm	1 MHz

Receiver spurious emissions measurement was performed as defined in EN 300 440 – 8.3

Test Equipment and Ancillaries Used For Tests

To simplify the identification on each page of the test equipment used, on each page of the test report, each item of test equipment and ancillaries such as cables are identified (numbered) by the Test Laboratory, below.

Reference	Instrument/Ancillary	Type	Manufacturer	Serial Number
1	Spectrum Analyzer	HP 8562A	Hewlett Packard	3051A05950
2	Spectrum Analyzer	HP8591EM	Hewlett Packard	3628A00871
3	Receive Antenna	Biconilog/3143	EMCO	9607-1277
4	Receive Antenna	Log Periodic /3147	EMCO	40582
5	Receive Antenna	Double Ridge Horn	Com-Power	10110
6	Receive Antenna	Loop	EMCO 6509	9502-1379
7	Power supply	DC Power supply	BK Precision	N961313540
8	Temperature Chamber	Tenney Jr	Tenney	11504-72
9	Spectrum Analyzer	Rohde & Schwarz	ESU40	100108
10	Pre-Amplifier	Com-Power	PA-010	171003
11	Pre-Amplifier	Com-Power	CPPA-102	01254
12	Pre-Amplifier	Com-Power	PA-22	711923
13				
14				

Additional Information Supplementary To Test Report

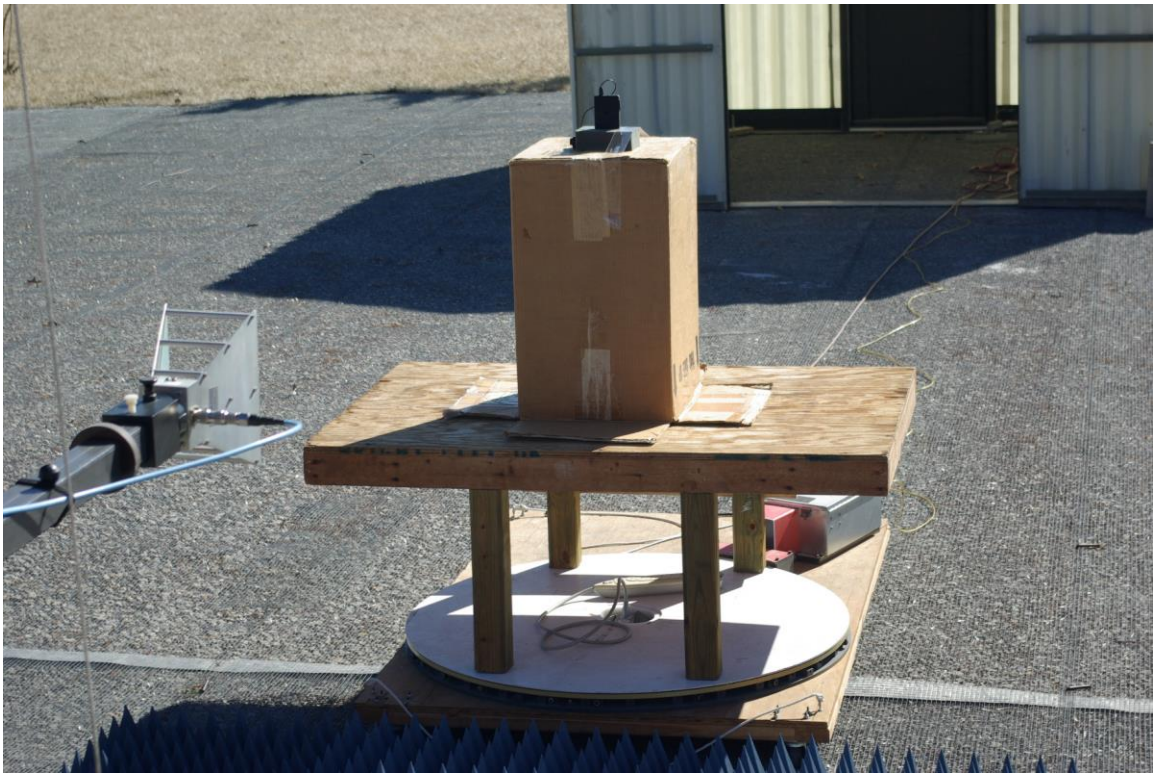
Page No. Remarks

Photographs of the equipment

External photograph front side

External photograph Back side

Photograph of Test Setup



International Association of Chiefs of Police

Digital Video Systems Minimum Performance Specifications Document

Version 14 – 11/21/2008

In-Car Video Camera Systems

Performance Specifications:

Digital Video Systems Module

Ronald C. Ruecker
President
International Association of Chiefs of Police
Director of Public Safety
City of Sherwood, OR

Daniel N. Rosenblatt
Executive Director
International Association of Chiefs of Police

James W. McMahon
Deputy Executive Director
International Association of Chiefs of Police

John Firman
Research Center Director
International Association of Chiefs of Police

David Hagy, Ph.D.
Director
National Institute of Justice

John Morgan, Ph.D.
Deputy Director for Science & Technology
National Institute of Justice

Frances Scott, Ph.D.
Senior Program Manager
Office of Science & Technology
National Institute of Justice

This project was supported under Award number 2007-MU-MU-K004 from the U.S. Department of Justice, National Institute of Justice (NIJ), Office of Justice Programs. Points of view or opinions contained in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Justice.

Welcome

For a number of years, the IACP has recognized the value of mobile video recorders for the protection of officers, their agencies, and the public they serve. As new digital technology rapidly began to replace existing analog systems, the IACP was concerned with the quality and reliability of the technology. To ensure the continued success of in-car camera programs, in 2005 the IACP Cutting Edge of Technology Project was tasked with establishing minimum performance specifications for digital in-car video systems.

The objective of this initiative was two-fold: 1) As law enforcement leadership recognized that those managing in-car video systems had little in terms of impartial information with which to evaluate, purchase, and manage systems, it became imperative that a document was needed to provide objective guidance and outline optimum system parameters that would promote officer safety and quality video for evidentiary purposes; and 2) It was necessary for manufacturers and system providers to better understand the overall needs of their law enforcement customers in the design and marketing of these digital in-car systems.

Through a grant from the U.S. Department of Justice, National Institute of Justice (NIJ) Office of Science and Technology, the IACP established a Digital Video Systems (DVS) Advisory Panel in March 2005 that included voluntary participation from law enforcement practitioners, video system manufacturers, and the scientific and technical community. Six task groups were formed to address specific components of the technical specifications document: quality measurement, data security, operational measurements, officer safety, interoperability, and testing and certification.

Over the next three years, the DVS Advisory Panel participants conducted field tests at various locales using multiple police agencies and vehicles in an effort to:

- Identify a standard "theater of operations" defined by the field-of-view of an in-car camera during a routine traffic stop. In doing so, the Panel sought to determine the relative sizes of critical objects (e.g. license plates, weapons) within the field-of-view.
- Examine the effects of operating conditions (e.g. inclement and extreme weather and light level) on the ability of standard systems to resolve critical objects.
- Measure the quality of video recordings produced by in-car systems as compared to known test criteria to develop parameters for performance of the in-car systems.

Following multiple field measurements, lengthy collaborative discussions, and a series of Advisory Panel meetings between 2005 and 2008, this document is the culmination of a great deal of effort and dedication from all parties involved in this initiative. Yet as with seemingly any technological innovations, digital in-car camera systems technology is certain to evolve. Thus, the IACP intends for this to be a living document, monitoring industry advancements and technology as it matures and advances.

Special Acknowledgements

The reader will find a complete list of participating agencies and IACP staff within Appendices F and G, but the International Association of Chiefs of Police wishes to first recognize a number of notable individuals and organizations for their dedication and tireless efforts towards the completion of this technical document:

Wm. Grady Baker
Herb Blitzer
Miles Brissette
Mike Burridge
Grant Fredericks
Steve Lisiewicz
Harlin McEwen
Christopher Miles
Patty Wolfhope

Delaware State Police
Fairfax County, VA Police Department
Farmington, NM Police Department
Indiana State Police
Institute for Forensic Imaging
Montgomery County, MD Police Department
Prince Georges County, MD Police Department
Tarrant County, TX Criminal District Attorney's Office

Foreword

Over a period of three years, 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 these minimum standards, specifications and accompanying documents adjust to technological and scientific advances as we move into the future of digital media and its adopted use in public safety..

Chief Mike Burridge (ret)
L3-Communications Mobile-Vision
"Digital Video Standards for Public Safety" Executive Committee Co-Chair

TABLE OF CONTENTS **PAGE**

Welcome Letter iii
Special Acknowledgements iv
Foreword v

Section 1 – General Information
1.1 Scope 1
1.2 Purpose 1
1.3 Application 1
1.4 Definitions 1
1.5 Acronyms 8
1.6 Units of Measure 9

Section 2 – Applicable Standards
2.1 Industry Standards 10
2.2 White Paper Requirement 10

Section 3 – Officer/Occupant Safety
3.1 Requirements for Any and All Physical Equipment Installed in Motor Vehicles for the Purpose of Collecting Digital Multimedia Evidence (DME) 11
3.2 Items Carried by the Officer 13
3.3 Record Indicators 14

Section 4 – General Mobile Video System Specifications
4.1 Mobile Video Systems Components 15
4.2 Vehicular Recording Front-facing Primary Camera System 15
4.3 Vehicular System Electric Conditions 18

Section 5 – Security Features
5.1 Restricted Access to Programming Functions 19
5.2 Erasure Prevention 19
5.3 Vehicle Recording System Integrity 19
5.4 Consistency 19
5.5 DME Verification 19
5.6 Transfer of Digital Assets 20
5.7 Vehicle Recording System Security 23

Section 6 – Digital Asset Recording
6.1 Video Systems Measurements 25

Section 7 – Interoperability
7.1 Active or Archival Storage Server 29
7.2 Active Storage and Archival Storage Interoperable Exchange 30

APPENDICES **PAGE**

Appendix A	Recommended Policies and Best Practices	31
Appendix B	Federal Motor Vehicle Safety Standards 201, "Occupant Protection in Interior Impact"	38
Appendix C	Federal Motor Vehicle Safety Standards 205, "Glazing Materials"	71
Appendix D	Interoperability Chart	75
Appendix E	Acknowledgements: DVS Executive Committee	76
Appendix F	Acknowledgements: Participating Agencies/Organizations	77
Appendix G	Acknowledgements: IACP Staff	79

Section 1 – General Information

1.1 Scope

The scope of this document is limited to vehicular video and audio recording systems used by law enforcement agencies for recording events occurring in and around the vehicle.

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.

The requirement to comply with these specifications applies to any mobile digital video equipment delivered to a law enforcement agency 18 months following the published date of the specifications. Said equipment must meet the minimum performance specifications and show proof of certification and compliance, as determined by the International Association of Chiefs of Police (IACP).

1.3 Application

This document applies to vehicle-mounted digital video recording systems that record at least one camera. This document also applies to vehicle-mounted digital video and audio recording systems that record at least one camera and at least one microphone.

The minimum electrical hazard and performance requirements outlined within this specifications document are based on limited international harmonized requirements that may not be all inclusive for the local country, i.e. normative body. Additional consideration should be given when evaluating products to such electrical hazard and performance requirements outlined within this specifications document as it relates to the local authorities having jurisdiction outside of the United States.

1.4 Definitions

"Will, Shall, Must;" denote mandatory key safety items that are crucial for officer safety and "shall" not be deviated from.

"Recommended, Should, May;" state preferred practices that agencies "may" deviate from.

1.4.1 **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 known standards to verify that the known standards can be processed within an acceptable range of results.

1.4.2 **Accuracy**: Refers 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 to be considered an accurate photographic reproduction? Also refers to the margin of error in measuring a value.

1.4.3 **Active Storage**: A storage location or device (i.e. server) which Digital Multimedia Evidence (DME) is transferred to from the in-vehicle recorder using any method. Active Storage shall provide ready access to recently recorded DME which has not been moved to Archival Storage due to elapsed time from the original recording creation date. Access to DME in Active Storage may or may not require administrator interaction based on departmental policy.

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

1.4.5 **Ambient Interference**: The conducted and/or radiated electromagnetic interference and/or mechanical motion interference, at a specific test location and time, which might be detrimental to the proper recording system or device performance.

1.4.6 **Amperage**: A measurement of electrical current

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

1.4.8 **Archival Storage**: A storage location or device to which DME is moved after a designated amount of time. Access to DME contained within Archival Storage may be limited and may require administrator authorization to review or move back to Active Storage.

1.4.9 **Archive**: Offline storage of DME intended for long-term storage and retrieval.

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

1.4.11 **Archive Image**: 1) any image placed on media that is suitable for long-term storage. 2) a bit stream duplicate of the DME placed on media that is suitable for long-term storage and retrieval.

1.4.12 **Archiving**: Long-term storage of data.

1.4.13 **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.

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

1.4.15 **Bundled**: Accessories or software that are included in the purchase of the main item such a computer or a major software application.

1.4.16 **Capture**: The process of producing the DME from a natural event.

1.4.17 **Capture Device**: A device used to record DME and associated metadata.

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

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

1.4.20 **Chain of Custody**: The chronological documentation of the movement, control, locations and possession of evidence.

1.4.21 **Codec**: A device/program capable of encoding and/or decoding digital data. Codecs encode a stream or signal for transmission, storage or encryption and decode it for viewing and listening.

1.4.22 **Compression**: The process of condensing the size of a video file (measured in bits per second for a stream, or bytes for a file/clip).

1.4.23 **Consistency**: The degree of uniformity, standardization, and freedom from contradiction among the video/data or parts of a system or component.

1.4.24 **Copy**: An accurate reproduction of information.

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

1.4.26 **DAT**: Digital Audio Tape

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

1.4.28 **Data File**: A set of binary information representing DME.

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

1.4.30 **Date Stamping**: A software feature that automatically inserts the current date into the data file.

1.4.31 **Digital Image**: A photographic image that is represented by discrete numerical values organized in a two-dimensional array or video stream. Each discrete block of the array is called a pixel.

1.4.32 **Digital Multimedia Evidence (DME)**: Data representing audio essence, video essence, metadata, and any other information attached to a digital file.

1.4.33 **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.

1.4.34 **Display**: A visual readout device.

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

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

1.4.37 **Encryption**: The process of coding data so that a specific code or key is required to restore the original data.

1.4.38 **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 in order for the data to be displayed.

1.4.39 **Format Conversion**: To transfer DME material from one media type to another and/or from one recording method to another.

1.4.40 **Hash**: A mathematical formula that generates a unique number used to verify the data's integrity.

1.4.41 **Image Authentication**: 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 the removal of elements in the image (e.g. adding bruises to a face).

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

1.4.43 **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.

1.4.44 **Integrity**: 1) the completeness of the digital multimedia 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.

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

1.4.46 **Internal Circuit Test**: A test function (whether manually or automatically initiated) that verifies that all device internal signal processing circuitry is working correctly.

1.4.47 **Locked File**: A file on which one or more of the usual types of manipulative operations cannot be performed – typically, one that cannot be altered by additions or deletions.

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

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

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

1.4.51 **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.

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

1.4.53 **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.

1.4.54 **Network Topology**: Graphical representation of a network.

1.4.55 **Nominal Value**: The numerical value of a device characteristic as specified by the manufacturer.

1.4.56 **Non-Removable Recording Media:** Any data storage that is housed within another device and cannot be removed from that device without disassembly of the device.

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

1.4.58 **Physical Image**: A bit stream duplicate of data contained on the physical device.

1.4.59 **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.

1.4.60 **Pixel**: A picture element.

1.4.61 **Power Density**: Power density per unit area or energy density flux per unit area.

1.4.62 **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.

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

1.4.64 **Proprietary**: A quality of a technique, technology, or other in which it is owned and controlled by a company or other party, and is thereby only usable or adaptable as allowed by that party.

1.4.65 **Proxy**: A compressed copy of the original DME. A proxy can be transmitted faster than the original data.

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

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

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

1.4.69 **Removable Media**: Any portable device that contains data. Storage media that can be removed from the recording device.

1.4.70 **Sample Rate**: The number of horizontal lines of video information and the number of samples on each line.

1.4.71 **Storage Media**: Any object on which DME is preserved.

1.4.72 **Transcoding**: The direct digital-to-digital conversion from one format to another. It involves decoding/decompressing the original data to an intermediate format and re-encoding.

1.4.73 **Validation**: The process of performing a set of experiments and/or tests which establishes the efficacy and reliability of a tool, function, or procedure or modification.

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

1.4.75 **Validity Check**: The process of analyzing data to determine whether it conforms to predetermined completeness and consistency parameters.

1.4.76 **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.

1.4.77 **Verification**: The process of confirming the accuracy of any copy of the DME to the original DME.

1.4.78 **Working Copy**: An accurate copy or duplicate of the original DME that can be used for subsequent processing and/or analysis.

1.5 Acronyms

ABA	American Bar Association
AFSC	United States Air Force Charts
ANSI	American National Standards Institute
ASCLD-LAB	American Society of Crime Lab Directors/Laboratory Accreditation Board
CPSC	Consumer Product Safety Commission
DSS	Digital Spread Spectrum
DVS	Digital Video System
DME	Digital Multimedia Evidence
EDD	Electronic Disruption Device
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 Standards 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 Inc.
ULC	Underwriters Laboratories of Canada
VHF	Very High Frequency
VVCS	Vehicle Video Capture System
WMV	Windows Media Format
WORM	Write Once, Read Many

1.6 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 following:

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 Traffic Safety Administration (NHTSA)
h) Society of Automotive Engineers (SAE)
i) Underwriters Laboratories Inc. (UL)
j) Underwriters Laboratories of Canada (ULC)

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

Section 3 – Officer/Occupant Safety

3.1 Requirements for any and all physical equipment installed in the motor vehicle for the purpose of collecting Digital Multimedia Evidence (DME).

3.1.1 Items installed or located in the interior of the vehicle per the manufacturers' installation instructions and supplied hardware 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 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.

3.1.1.1 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 B).

3.1.1.2 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. Note: This correlates to Federal Motor Vehicle Safety Standard 201 (5.4) [October 1, 2002] See Appendix B.

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

3.1.1.4 Manufacturers shall provide the customer the necessary brackets, mounting hardware, and installation instructions that if followed properly will ensure the vendor's equipment is installed in accordance with all appropriate Federal Motor Vehicle Safety Standards (FMVSS) that are in place at the time of the contract between the vendor and the consumer.

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. This can be simulated by the use of UL's articulated probe consisting of a radial tip of one inch as defined in UL 250.

3.1.2.1 All cameras should default to autofocus. The manufacturer may provide an autofocus override system for all except the front-facing camera if desired. An autofocus override system for the front-facing camera shall be provided. The override system should be configurable to prevent operation while the vehicle is in motion.

3.1.2.2 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 vehicle dash illumination control. The viewing screen light level shall be controlled simultaneously with the controls or independently. The viewing screen shall be capable of being completely dimmed. An operator must have the ability to blackout the system on demand.

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 also 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 and (if included) a replacement to the factory-installed rear-view mirror that meets applicable federal standards, 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 C) 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 the outside of 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 it wants 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 Before being placed into service, equipment installed in the passenger compartment should be checked by drivers and occupants of various sizes and builds in order to ensure that it does not interfere with any speedometer, warning lights, gauges, mirrors, or essential controls, placed in the vehicle by the OEM.

3.1.3.4 Manufacturers shall specify equipment-mounting locations to comply with this specification in their installer's guide or owner's manual, or will provide a list of vehicles for which the vendors' 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 housing such as the camera body, control panel, and monitor shall comply with the appropriate certification requirements as referenced in NFPA70 and applicable UL Standards. 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 guides or owner's manuals that specifies the proper wiring, fuses, connectors, and connection points with the vehicle electrical system and grounding points.

3.1.5 Elimination of hazardous pinch points.

3.1.5.1 Care shall be taken in the design to minimize potential injury of officer due to pinching by moveable parts (e.g. doors, brackets, latches).

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 Laboratories Standards for shock/electrocution and burn prevention. All batteries used in such devices shall meet Underwriters Laboratories 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 a 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 great 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 control 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 injury from strangulation, cutting off of blood flow or laceration during assault, slipping, falling, or other types of incidents. Body-worn cords shall also be of such construction that they minimize possible injury 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 type of incident. 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 shall 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 light shall be able to be disabled.

Section 4 – General Mobile Video System Specifications

4.1 Mobile Video Systems Components

This document applies to vehicle-mounted digital video recording systems that record at least one camera. This document also applies to vehicle-mounted digital video and audio recording systems that at least one camera and at least one microphone.

4.1.1 The DME shall accurately and reliably reproduce the viewable image, the audible sound, and associated metadata.

4.1.2 The system shall maintain consistent audio/visual recording quality while subject to interference from the following sources:

a) High-powered radio frequency transmissions
b) Other radio frequency interference (including UHF, VHF, and HF transmitters)
c) Automobile alternator, ignition, and electrical systems
d) Fan motors from automobile heaters and air conditioners
e) Other patrol vehicle electrical systems to include radios, emergency lights, sirens, mobile data computers, and speed-measuring devices.
f) High-voltage power line, traffic signals, neon signs, etc.

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

4.1.4 The Vehicular Recording System shall operate within the range of temperatures from 0 to 120 degrees Fahrenheit or between -17.8 and 48.9 degree Celsius.

4.2 Vehicular Recording Front-Facing Primary Camera System

4.2.1 The Vehicular Recording System camera and lens will be equipped with autofocus, automatic exposure, and automatic white balance.

4.2.2 The Vehicular Recording System camera shall have a backlight compensation setting.

4.2.3 The Vehicular Recording System's Front-Facing Camera shall be capable of being rotated 360 degrees on its mount in a horizontal plane or 180 degrees in either direction from its front-facing position without having to loosen any screws or knobs.

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

4.2.5 The Vehicular Recording System shall provide both automatic and manual focus capabilities which are user selectable.

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

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

4.2.8 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).

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

4.2.10 The Vehicular Recording Device shall operate independently of the monitor. "Operate independently" means that the system shall be able to record without the image or sound being displayed.

4.2.11 The Vehicular Recording System Monitor shall have the capability to selectively display: date/time, user identification information, emergency light indication, siren indication, braking indicator and microphone activation indicator. These items shall be captured for each video frame in the metadata and not superimposed onto, added to, or be embedded in the video stored on the recording.

4.2.12 The Vehicular Recording System shall be capable of recording audio from a wireless microphone at a range of 1,000 feet, line of sight, under ideal conditions.

4.2.13 The Vehicular Recording System wireless microphone shall contain an integrated antenna.

4.2.14 The Vehicular Recording System's operator shall have the ability to deactivate audio from the wireless microphone without stopping or disabling the recording of video.

4.2.15 The Vehicle Recording wireless microphone shall be able to activate audio and video recording from the remote transmitter.

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

4.2.17 The Vehicular Recording wireless microphone shall use FCC-approved frequency bands.

4.2.18 The Vehicular Recording wireless microphone shall be able to be synchronized or paired to a specific receiver in the vehicle without any manual adjustment by the user.

4.2.19 The Vehicular Recording wireless microphone shall contain a rechargeable battery with a minimum battery-life of 15 hours (passive mode) or a talk time of 3.5 hours (active mode).

4.2.20 The Camera or Vehicular Recording System shall provide the following controls:

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

4.2.21 The Camera or 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) Rewind
g) Stop
h) Time Counter
i) Diagnostic Display showing the results as specified in 5.7.1 through 5.7.1.3

4.2.22 The Vehicular Recorder System's recording functions shall be activated by any of the following methods:

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

4.2.23 The Vehicular Recording System shall be capable of recording events uninterrupted for a minimum of three and a half (3.5) hours at a minimum image refresh rate of 30 frames per second (fps) per camera.

4.2.24 When pre-event and/or post-event DME capture is provided by the Vehicular Recording System, it shall be possible to enable or disable the pre-event and post-event audio capture capability while continuing to capture the remaining DME items.

4.3 Vehicular System Electric Conditions

4.3.1 The Vehicular Recording System shall be protected from damage due to input of voltage, reverse polarity, and electrical transients that may be encountered.

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

4.3.3 Loss of operating power or disconnection from the vehicle battery shall not result in the system requiring programming. Sudden loss of power shall not cause loss of any DME previously written to DME storage.

Section 5 – Security Features

5.1 Restricted Access to Programming Functions

The Vehicular Recording System shall have the capability to restrict access to the programming functions, including but not limited to time/date features.

5.2 Erasure Prevention

The Vehicular Recording System shall have the capability of preventing the user from erasing, altering, and/or recording over previously recorded information from either inside the vehicle or at the recording device controls.

5.3 Vehicular Recording System Integrity

User interfaces shall prevent the input of invalid data that exceeds the system's expected ranges.

5.4 Consistency

5.4.1 Time Consistency

5.4.1.1 The Vehicular Recording Video Capture System shall provide a mechanism to capture the time and date of DME creation.

5.4.1.2 Time stamping of DME elements (video, audio, metadata) shall be consistent within all system components.

5.4.1.3 All elements of the Digital Multimedia Evidence (DME) shall remain accurate with respect to the recording as it was captured.

5.4.1.4 The Vehicle Recorder, Active Storage, and Archival Storage Systems clocks shall be capable of being synchronized to an external time reference.

5.4.1.5 The Vehicular Recording System's recorder clocks shall be capable of remaining synchronized with each other within 33 milliseconds when connected to an external time reference. The DME Audit Log and DME metadata shall indicate when time synchronization to the external time reference was not available.

5.5 DME Verification

5.5.1 The DME, or removable media containing the DME, shall indicate either the ID number(s) of the operator(s)/officer(s) assigned when the DME was captured or the vehicle ID in which the DME was recorded.

5.5.2 All electronic transfer of the DME shall have an automated verification mechanism. Information consisting of a minimum 128 bit hash value shall be attached to the DME when first recorded. The automated mechanism shall not introduce any visible or audible artifacts into the DME.

5.6 Transfer of Digital Assets

5.6.1 Physical Digital Asset Transfer Using Removable Media:

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

5.6.1.2 The DME Audit Log shall contain the following items when the DME 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) A verification check per section 5.5.2 shall be performed and logged to validate that the DME transferred to the Active Storage is an exact duplicate prior to any clearing of data on the removable storage media;

c) Active Storage retention period for the DME

5.6.2 Wireless Data Transfer:

An integrity check shall be used to validate that the DME on the Active Storage is an exact duplicate to any data on the recorder prior to the information being deleted from the recorder

5.6.2.1 Wireless Transfer Network Topology:

A wireless network used to transfer the DME from the recorder to Active Storage shall, at a minimum, use 128-bit encryption to create a secure connection for the DME to be transferred. Manufacturers, at their customers' discretion, may provide other security technologies that surpass 128-bit encryption.

IEEE standards-based wireless networking equipment shall support the following security standards:

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 the manufacturer.

If non-IEEE standards-based wireless networking equipment is used, it should be configured to at least meet the equivalent minimums defined in 5.6.2.1.

5.6.2.2 DME Audit Log on the Active Storage

The DME Audit Log shall contain the following items when wireless DME transfer from the recorder to Active Storage is used:

a) An indication that a successful wireless connection with the recorder was completed;
b) Time/date of transfer;
c) Active Storage retention period for the DME;
d) A verification check per section 5.5.2 shall be performed and logged to validate that the DME 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:

An integrity check shall be used to validate that the original DME transferred to the Active Storage is an exact duplicate to any DME on the recorder prior to the information being deleted from the recorder.

5.6.3.1 Wired Transfer Network Topology

A private network (i.e. separate from any other networks) used to transfer the DME 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.

A public network (i.e. where the data must cross over another non-private network) used to transfer the DME 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 DME to be transferred. Manufacturers, at their customers' discretion, may provide other security technologies that surpass 128-bit encryption.

5.6.3.2 DME Audit Log Items on the Active Storage

The DME Audit Log shall contain the following items when a wired DME transfer from the recorder to Active Storage is used:

a) An indication that a successful wired connection with the recorder was completed;
b) Time/date of transfer
c) Active Storage retention period for the DME
d) A verification check per section 5.5.2 shall be performed and logged to validate that the DME 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 DME Audit Log shall contain the following items when the DME is transferred from Active Storage to Archival Storage:

a) The identity of the user initiating the transfer (if the process is not automated);
b) Time/date of the transfer;
c) Archival Storage retention for the DME – 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 DME;
d) A verification check per section 5.5.2 shall be performed and logged to validate that the DME transferred from Active Storage to Archival Storage is an exact duplicate prior to the clearing of Active Storage.

5.6.5 Retrieval of DME from Archival Storage back to Archive Storage

The DME Audit Log shall contain the following items when the DME is transferred from Archival Storage to Active Storage:

a) The identity of the user initiating the transfer (if the process is not automated);
b) Time/date of the transfer;
c) A verification check per section 5.5.2 shall be performed to validate that the DME transferred back to Active Storage is an exact duplicate should the DME stored in Archival Storage be removed;
d) An Active Storage retention period for the DME – It is anticipated that the Active Storage retention period will be recomputed and is not necessarily related to the previous Archival Storage retention period associated with the DME. The DME shall be returned to the Archival Storage after expiration of the Active Storage retention period.

5.6.5.1 The Active and Archival Storage systems shall provide a mechanism for backing-up the DME.

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

5.6.6 Removal of DME from both Active Storage and Archival Storage

5.6.6.1 The DME Audit Log shall contain the following items when any portion of the DME is permanently removed from both Active Storage and Archival Storage:

a) The user identity initiating the removal (if the process is not automated);
b) Time/date of the removal;
c) An indication of what components of the DME were removed.

5.6.6.2 In systems that may support the creation of a lower bit-rate instance of the DME, the DME Audit Log shall also contain an indication that a lower bit-rate instance of the removed DME components has been created.

5.7 Vehicular Recorder System Security

The following items shall be included to protect the Vehicular Recording System and its removable media:

5.7.1 Equipment Diagnostics

5.7.1.1 When powered, the recorder shall perform a self-test to ensure 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 the amount of storage space remaining on the 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 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 Removable Media Security

5.7.3.1 The recording media shall be secured using a security 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 If non-removable recording media is being used, it shall be housed inside the recorder to prevent tampering with and/or destruction of the media.

5.7.3.4 The manufacturer shall provide guidelines on the media life-cycle.

5.7.3.5 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 identifies each media and makes that media unique.

Section 6 – Digital Asset Recording

6.1 Video Systems Measurements

These tests apply to video obtained under section 7.1.1. from the primary camera.

6.1.1 Dynamic Range Measurement

The purpose of this test is to determine the degree to which the system under test will be able to record both light and dark contents in the scenes.

6.1.1.1 Record several seconds of video of a step tablet, illuminated in a sensitometer, with a brightness range of 10,000 to 1.

6.1.1.2 Light should be nominally 2,800 to 3,200 degrees Kelvin.

6.1.1.3 Capture a number of frames as per the process provided by the system vendor and open them in a software program such as Adobe Photoshop.

6.1.1.4 Using a sampling tool with at least 5x5 pixels, measure the red, green, and blue values of each of the steps.

6.1.1.5 Using the data for the sensitometer, plot the brightness values for each step as a function of its log (base 10) exposure value (corrected for color temperature).

6.1.1.6 Determine the point on the log exposure axis at which the response curve is flat due to saturation. This is the saturation point.

6.1.1.7 Determine the point on the response where the signal due to both light and noise is equal to twice the noise level alone. This is the threshold point.

6.1.1.8 Subtract the threshold point value from the saturation point value. This is the dynamic range in terms of log exposure.

6.1.1.9 The system should have a range of 2.0 log exposure or more.

6.1.2 Static Resolution

The purpose of this test is to determine if the system is able to capture images of small items of importance in the typical scenes it is likely to encounter in practice.

6.1.2.1 Working at an incident light level in the range from 500 lux to 2,000 lux, record several frames of video of a high-contrast, bar-type resolution test target.

6.1.2.2 Capture selected video frames and examine them to determine that the bars are clear enough to be counted correctly.

6.1.2.3 The target should have bars that are nominally horizontal, vertical, and at 45 degrees.

6.1.2.4 The system should be capable of resolving bars that represent one-half of a line pair per inch (both lines of equal width, one black and one white) at a frame width of 24 ft. This requirement will increase to one line pair per inch one year after this initial specification goes into effect.

6.1.2.5 Equivalent geometry can be used.

6.1.3 Aspect Ratio

The purpose of this test is to determine if the system presents images to the user that have the correct aspect ratio (width to height) so that measurements can be made.

6.1.3.1 Record several frames of a test target with a circle and a square.

6.1.3.2 Capture several frames and measure the height and the width of the test target elements to assure that they have their claimed aspect ratio to within 2% of 1 to 1.

6.1.4 Color Fidelity

The purpose of this test is to determine the degree to which the system under test can capture colors accurately so that color can be reliably used in analyses of the recorded video.

6.1.4.1 Record several frames of video of a Macbeth Corporation Color Checker™. The light should be at 5,000 to 6,000 Kelvin and between 300 and 400 lux incident light.

6.1.4.2 The target has well rendered primaries (red, green, blue, cyan, magenta, and yellow) and six shades of gray.

6.1.4.3 Determine the CIE/Lab dimensions for each patch in the test target.

6.1.4.4 Open the frames in image editing software such as Adobe Photoshop and measure the CIE/Lab parameters for each patch using a sampling tool with a view of at least 5x5 pixels.

6.1.4.5 Subtract the measured values from the respective patch values for all 12 patches.

6.1.4.6 Square the individual differences and sum them.

6.1.4.7 Divide by 36 (the number of values). This is the mean squared error. The mean squared error for the system under test should be less than 204.

6.1.5 Dynamic Modulation

The purpose of this test is to determine the ability of the system under test to reproduce moving portions of the scene as a function of item size, velocity, and scene brightness. It invokes the system's shutter function, compression function, and image capture process.

6.1.5.1 Record a test target moving at known velocities ranging from the equivalent of up to 45 miles per hour at a frame width of 24 feet and distance of 35 feet, or optical equivalent.

6.1.5.2 The test target should move across the video frame and it should cover at least 40% of the frame height.

6.1.5.3 The test target should have two series of white and black bars that are the equivalent of two and four inches wide each.

6.1.5.4 The test target will be illuminated at two levels: between 1,800 lux and 2,200 lux incident and between 9,000 and 10,000 lux incident.

6.1.5.5 Capture frames and open them in an editing software package such as Adobe Photoshop.

6.1.5.6 Render the images as grayscale images.

6.1.5.7 Measure the brightness levels of the dark and light bars using a sampling tool with a window of at least 5x5 pixels.

6.1.5.8 Subtract the dark bar values from the light bar values to determine the modulation.

6.1.5.9 Normalize the modulation for each velocity by dividing it by the modulation of the stationary test target.

6.1.5.10 Plot the relative modulation as a function of the velocity of the target.

6.1.5.11 The relative modulation should be at least 50% at 15 miles per hour equivalent at both light levels.

6.1.5.12 There shall be no dropped frames. The test shall capture the expected number of frames as specified by the manufacturer and as determined by target motion used in section 6.1.5.1. Each captured frame shall show the target progressing through the frame the expected number of pixels as determined by the target motion used in section 6.1.5.1.

6.1.6 Rolling Shutter Distortion

The purpose of this test is to provide an indication of the angle between a moving vertical line and the representation of that line that is caused by the process the camera uses to sample the real image formed by the camera lens.

6.1.6.1 The angle between the bars recorded in the dynamic modulation test and true vertical will be measured at each light level.

6.1.6.2 This is a measure that a forensic video analyst can use to correct any measurements that might be made. There will be no basic requirement in this specification.

6.1.7 Microphone

The purpose of this test is to determine whether the transmitter can communicate intelligibly with the in-car mounted system over the required distance.

6.1.7.1 Procedure

6.1.7.2 Set out 500, 750, and 1,000 foot markers along an open pathway.

6.1.7.3 With the transmitter positioned to prevent any object from impeding the transmission path to the in-car receiver, play recorded audio (at normal roadside speaking volumes) to the microphone at each of the distances, starting at the 1,000 ft. mark.

6.1.7.4 Record the transmitted signal at the in-car system.

6.1.7.5 Compare the system recording to the original for clarity.

6.1.7.6 The recoded sound message must be intelligible.

Section 7 – Interoperability

7.1 Active or Archival Storage Server (see Appendix D)

The Active Storage Server or the Archival Storage Server shall provide two interoperability formats to export the DME.

7.1.1 Decompressed DME Export

7.1.1.1 The DME (images, sounds, metadata, and DME Audit Log) shall be capable of being exported in decompressed industry-standard file formats that are viewable and playable without the need for proprietary codecs, players, or viewers available from only the system manufacturer.

7.1.1.2 The decompression mechanism shall provide an accurate representation of the images, sounds, and metadata as recorded.

7.1.1.3 The decompressed images and sounds shall minimally comply with section 6.0

7.1.1.4 A DME verification check shall be performed to confirm the automatic verification mechanism of Section 5.5.2 prior to exporting the decompressed DME.

7.1.1.5 A verification report shall be included with the Decompressed DME Export stating the results of a DME verification check in section 7.1.1.4.

7.1.1.6 The DME Audit Log on the Active Storage

The DME Audit Log shall contain the following items when the Decompressed DME Export is performed:

a) Identification of the person performing the export;
b) Identification of the person receiving the export;
c) Time and date of the export;
d) A verification check per section 5.5.2 shall be performed and logged to validate the DME immediately prior to the decompressed DME export;
e) A hash or other verification shall be computed for the exported decompressed DME using an industry-standard method, without the need for proprietary codecs, players, or viewers available from only the system manufacturer, and shall be provided with the exported decompressed DME.

7.1.2 Compressed DME Export

7.1.2.1 The DME (images, sounds, metadata, and DME Audit Log) shall be capable of being exported in industry-standard file formats that are viewable and playable without the need for proprietary codecs, players, or viewers available from only the system manufacturer.

7.1.2.2 A DME verification check shall be performed to confirm the automatic verification mechanism of Section 5.5. prior to exporting the compressed DME.

7.1.2.3 A verification report shall be included with the Compressed DME Export stating the results of a DME verification check in Section 7.1.2.2.

7.1.2.4 The DME Audit Log on the Active Storage

The DME Audit Log shall contain the following items when the compressed DME export if performed:

a) Identification of the person performing the export;
b) Identification of the person receiving the export;
c) Time and date of the export;
d) A verification check per section 5.5.2 shall be performed and logged to validate the DME immediately prior to the compressed DME export;
e) A hash or other verification shall be computed for the exported compressed DME using an industry-standard method, without the need for proprietary codecs, players, or viewers available from only the system manufacturer, and shall be provided with the exported compressed DME.

7.2 Active Storage and Archival Storage Interoperable Exchange

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

Appendix A – Recommended Policies and Best Practices

1.1 All mobile video systems should be of industrial/commercial grade and in full production. No prototype models will be considered for testing.

1.2 Requirements:

1.2.1 The mobile video system (in-car camera) should have a proven, reliable record in actual vehicular use under a variety of conditions. This record should be evidenced by either 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 should provide business and financial history upon request.

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

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

1.2.3.3 To document vendors' experience in the manufacturing, sales, and support of mobile video systems, the vendor should provide a list of several agencies to which mobile video systems were sold. Letters of reference for verification should also 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 specifications 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 should be warranted to ensure that they are fit for their intended purposes for a minimum of one year.

1.3.2 All defective equipment should 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 the initial installation of the said equipment in the vehicle.

1.4 Vehicle Recording System Integrity

1.4.1 If the unit does not have a discrete login capability, the officer assigned to the vehicle should 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 should visually verify that the equipment has not been tampered with or been damaged.

1.4.3 The IACP Model Policy requires that the officer conduct an operational readiness test of the system prior to the beginning of a tour of duty. If the system is malfunctioning, the officer should notify a supervisor and communications. The supervisor should 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 should 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 backed up at an off-site 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 should be governed by the agency's policies and procedures and should include additional levels of user authentication prior to granting access.

1.5.5 Electronic notification should be provided for each DME intended to be removed from Active and Archival Storage at a time prior to removal based on operating agency policy according to the retention period for the DME.

1.6 Removable Media Security

1.6.1 Physical Tamper Detection

1.6.1.1 The operator of the recorder should perform a physical "check" of the removable media to ensure no tampering has occurred and that physical tamper-detection devices are in place.

1.6.2 Key Management – Keys should be managed via agency policies and procedures such as:

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

1.7 Back Office Equipment Security

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

a) Equipment housed in secured facility with limited employee access;
b) Secured system access;
c) System captures standard "audit" information when user logs into the system;
d) System captures number of times user attempts to log into the system;
e) System user accounts become inoperable if more than three unsuccessful login attempts have been made.

1.7.1 System "passwords" governed by agency policy requirements:

a) 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.

b) Force "character" requirements for passwords (e.g. numeric, alpha, caps, etc.)

1.7.2 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 DME from the vehicle takes place;
b) Available storage capacity remaining limit at which point the DME 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.
    iii) Identification of individuals who can replicate keys.

d) Who is allowed to initiate the transfer or handle any removable media;
e) How to maintain a manual audit trail;
f) Recommend audit trail metrics for instances when the physical (manual) transfer of the DME from the recorder to Active Storage uses a removable media device (e.g. spinning optical, flash, digital tape, removable magnetic);
g) A system for establishing the identification (badge number or employee number) of the officer or person submitting the DME for transfer. (It is recommended that when a major incident occurs, authorized personnel respond to the scene and take custody of the DME);
h) Media identification numbering system (if tracked by the department);
i) The capture of the time/date of the transfer;
j) The capture of the size of the DME transferred;
k) The capture of the number of "copies" made to other media (e.g. tape, spinning, optical media, other server storage location);
l) Acceptable retention periods for DME;
m) How integrity checks are to be performed as a means to validate that the DME transferred to the active storage as an exact duplicate prior to any clearing of DME on the removable storage media;
n) Indicate successful transfer of the DME capture; and
o) Dictate how metadata are specifically coordinated and managed, to include where and how a user may or may not be permitted access.

1.8.2 Archival Policies – How long the DME needs to be archived should 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 the DME – Proof of where the DME was captured through verification by the officer in the stated location.

1.8.4 Electronic check of the DME Audit Log on the media.

1.9 Manufacturers' Considerations

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

1.9.1 Storage Solution

- What are the methods of DME retention offered by the manufacturer?

- Does the manufacturer provide a storage solution that facilitates the removal of the DME from the vehicle?

- Types of storage solutions:
  i. Hard drive;
  ii. Digital cassette;
  iii. Optical media;
  iv. Flash media.

- Transfer Methods:
  i. Automatic;
  ii. Manual;
  iii. Wireless;
  iv. 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 the individual 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 system provide protection against failure of the storage solution?

- Does the manufacturer's vehicular equipment contain mechanisms to minimize the damage to the DME 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 DME is original?

- Does the manufacturer include a CPU or Hardware ID of the vehicle recorder in the DME Audit Log?

- Is there an ability to indicate where and when the DME was captured?

- Does the equipment provide electronic validation of location and time synchronization between recorders through the use of GPS equipment?

- Is the time and date on the recorders synchronized to the back office equipment?

- Does the manufacturer provide evidence that the 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 DME on removable media so that it cannot be accessed by unauthorized equipment?

- Does the manufacturer provide synchronization between the record streams and the 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 the DME 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, 3 DES, 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 DME. 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 DME 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 DME, once decrypted on the other side of the transfer, is an exact duplicate of the original and meets the integrity requirements laid out in these specifications.

Appendix B – Federal Motor Vehicle Safety Standards 201, "Occupant Protection in Interior Impact"

§571.201 Standard No. 201; Occupant protection in interior impact.

S1. Purpose and scope. This standard specifies requirements to afford impact protection for occupants.

S2. Application. This standard applies to passenger cars and to multipurpose passenger vehicles, trucks, and buses with a GVWR of 4,536 kilograms or less, except that the requirements of S6 do not apply to buses with a GVWR of more than 3,860 kilograms.

S3. Definitions.

A-pillar means any pillar that is entirely forward of a transverse vertical plane passing through the seating reference point of the driver's seat.

Ambulance means a motor vehicle designed exclusively for the purpose of emergency medical care, as evidenced by the presence of a passenger compartment to accommodate emergency medical personnel, one or more patients on litters or cots, and equipment and supplies for emergency care at a location or during transport.

B-pillar means the forward most pillars on each side of the vehicle that is, in whole or in part, rearward of a transverse vertical plane passing through the seating reference point of the driver's seat, unless:

(1) There is only one pillar rearward of that plane and it is also a rearmost pillar; or

(2) There is a door frame rearward of the A-pillar and forward of any other pillar or rearmost pillar.

Brace means a fixed diagonal structural member in an open body vehicle that is used to brace the roll-bar and that connects the roll-bar to the main body of the vehicle structure.

Convertible means a vehicle whose A-pillars are not joined with the B-pillars (or rearmost pillars) by a fixed, rigid structural member.

Convertible roof frame means the frame of a convertible roof. Convertible roof linkage mechanism means any anchorage, fastener, or device necessary to deploy a convertible roof frame.

Convertible roof linkage mechanism means any anchorage, fastener, or device necessary to deploy a convertible roof frame.

Daylight opening means, for openings on the side of the vehicle, other than a door opening, the locus of all points where a horizontal line, perpendicular to the vehicle longitudinal centerline, is tangent to the periphery of the opening. For openings on the front and rear of the vehicle, other than a door opening, daylight opening means the locus of all points where a horizontal line, parallel to the vehicle longitudinal centerline, is tangent to the periphery of the opening. If the horizontal line is tangent to the periphery at more than one point at any location, the most inboard point is used to determine the daylight opening.

Door frame means the rearmost perimeter structure, including trim but excluding glass, of the forward door and the forward most perimeter structure, including trim but excluding glass, of the rear door of a pair of adjacent side doors that:

(1) Have opposing hinges;

(2) Latch together without engaging or contacting an intervening pillar;

(3) Are forward of any pillar other than the A-pillar on the same side of the vehicle; and

(4) Are rearward of the A-pillar.

Door opening means, for door openings on the side of the vehicle, the locus of all points where a horizontal line, perpendicular to the vehicle longitudinal centerline, is tangent to the periphery of the side door opening. For door openings on the back end of the vehicle, door opening means the locus of all points where a horizontal line, parallel to the vehicle longitudinal centerline, is tangent to the periphery of the back door opening. If the horizontal line is tangent to the periphery at more than one point at any location, the most inboard point is the door opening.

Dynamically deployed upper interior head protection system means a protective device or devices which are integrated into a vehicle and which, when activated by an impact, provide, through means requiring no action from occupants, protection against head impacts with upper interior structures and components of the vehicle in crashes.

Forehead impact zone means the part of the free motion headform surface area that is determined in accordance with the procedure set forth in S8.10.

Free motion headform means a test device which conforms to the specifications of part 572, subpart L of this chapter.

Interior rear quarter panel means a vehicle interior component located between the rear edge of the side door frame, the front edge of the rearmost seat back, and the daylight opening.

Mid-sagittal plane of a dummy means a longitudinal vertical plane passing through the seating reference point of a designated seating position.

Other door frame means the rearmost perimeter structure, including trim but excluding glass, of the forward door and the forward most perimeter structure, including trim but excluding glass, of the rear door of a pair of adjacent side doors that:

(1) Have opposing hinges;

(2) Latch together without engaging or contacting an intervening pillar; and

(3) Are rearward of the B-pillar.

Other pillar means any pillar which is not an A-pillar, a B-pillar, or a rearmost pillar.

Pillar means any structure, excluding glazing and the vertical portion of door window frames, but including accompanying moldings, attached components such as safety belt anchorages and coat hooks, which:

(1) Supports either a roof or any other structure (such as a roll-bar) that is above the driver's head, or

(2) Is located along the side edge of a window.

Roll-bar means a fixed overhead structural member, including its vertical support structure, that extends from the left to the right side of the passenger compartment of any open body vehicles and convertibles. It does not include a header.

Seat belt anchorage means any component involved in transferring seat belt loads to the vehicle structure, including, but not limited to, the attachment hardware, but excluding webbing or straps, seat frames, seat pedestals, and the vehicle structure itself, whose failure causes separation of the belt from the vehicle structure.

Seat belt mounting structure means:

(a) A vehicle body or frame component, including trim, that incorporates an upper seat belt anchorage conforming to the requirements of S4.2.1 and S4.3.2 of 49 CFR 571.210, that is located rearward of the rearmost outboard designated seating position, and that extends above a horizontal plane 660 mm above the seating reference point (SgRP) of that seating position; and

(b) A vehicle body or frame component, including trim, that incorporates an upper seat belt anchorage conforming to the requirements of S4.2.1 and S4.3.2 of 49 CFR 571.210, that is located forward of the rearmost outboard designated seating position, and that extends above a horizontal plane 460 mm above the SgRP of that seating position located rearward of the anchorage.

(c) The seat belt mounting structure is not a pillar, roll bar, brace or stiffener, side rail, seat, interior rear quarter panel, or part of the roof.

Sliding door track means a track structure along the upper edge of a side door opening that secures the door in the closed position and guides the door when moving to and from the open position.

Stiffener means a fixed overhead structural member that connects one roll-bar to another roll-bar or to a header of any open body vehicle or convertible.

Upper roof means the area of the vehicle interior that is determined in accordance with the procedure set forth in S8.15.

Windshield trim means molding of any material between the windshield glazing and the exterior roof surface, including material that covers a part of either the windshield glazing or exterior roof surface.

S4 Requirements

S4.1 Except as provided in S4.2, each vehicle shall comply with either:

(a) The requirements specified in S5, or,

(b) The requirements specified in S5 and S6.

S4.2 Vehicles manufactured on or after September 1, 1998 shall comply with the requirements of S5 and S6.

S5 Requirements for instrument panels, seat backs, interior compartment doors, sun visors, and armrests. Each vehicle shall comply with the requirements specified in S5.1 through S5.5.2.

S5.1 Instrument panels. Except as provided in S5.1.1, when that area of the instrument panel that is within the head impact area is impacted in accordance with S5.1.2 by a 6.8 kilogram, 165 mm diameter head form at—

(a) A relative velocity of 24 kilometers per hour for all vehicles except those specified in paragraph (b) of this section,

(b) A relative velocity of 19 kilometers per hour for vehicles that meet the occupant crash protection requirements of S5.1 of 49 CFR 571.208 by means of inflatable restraint systems and meet the requirements of S4.1.5.1(a)(3) by means of a Type 2 seat belt assembly at the right front designated seating position, the deceleration of the head form shall not exceed 80 g continuously for more than 3 milliseconds.

S5.1.1 The requirements of S5.1 do not apply to:

(a) Console assemblies;

(b) Areas less than 125 mm inboard from the juncture of the instrument panel attachment to the body side inner structure;

(c) Areas closer to the windshield juncture than those statically contactable by the head form with the windshield in place;

(d) Areas outboard of any point of tangency on the instrument panel of a 165 mm diameter head form tangent to and inboard of a vertical longitudinal plane tangent to the inboard edge of the steering wheel; or

(e) Areas below any point at which a vertical line is tangent to the rearmost surface of the panel.

S5.1.2 Demonstration procedures. Tests shall be performed as described in Society of Automotive Engineers Recommended Practice J921, "Instrument Panel Laboratory Impact Test Procedure," June 1965, using the specified instrumentation or instrumentation that meets the performance requirements specified in Society of Automotive Engineers Recommended Practice J977, "Instrumentation for Laboratory Impact Tests," November 1966, except that:

(a) The origin of the line tangent to the instrument panel surface shall be a point on a transverse horizontal line through a point 125 mm horizontally forward of the seating reference point of the front outboard passenger designated seating position, displaced vertically an amount equal to the rise which results from a 125 mm forward adjustment of the seat or 19 mm; and

(b) Direction of impact shall be either:

(b)(1) In a vertical plane parallel to the vehicle longitudinal axis; or

(b)(2) In a plane normal to the surface at the point of contact.

S5.2 Seat Backs. Except as provided in S5.2.1, when that area of the seat back that is within the head impact area is impacted in accordance with S5.2.2 by a 6.8 kilogram, 165 mm diameter head form at a relative velocity of 24 kilometers per hour, the deceleration of the head form shall not exceed 80g continuously for more than 3 milliseconds.

S5.2.1 The requirements of S5.2 do not apply to seats installed in school buses which comply with the requirements of Standard No. 222, School Bus Passenger Seating and Occupant Protection (49 CFR 571.222) or to rearmost side-facing, back-to-back, folding auxiliary jump, and temporary seats.

S5.2.2 Demonstration procedures. Tests shall be performed as described in Society of Automotive Engineers Recommended Practice J921, "Instrument Panel Laboratory Impact Test Procedure," June 1965, using the specified instrumentation or instrumentation that meets the performance requirements specified in Society of Automotive Engineers Recommended Practice J977, "Instrumentation for Laboratory Impact Tests," November 1966, except that:

(a) The origin of the line tangent to the uppermost seat back frame component shall be a point on a transverse horizontal line through the seating reference point of the right rear designated seating position, with adjustable forward seats in their rearmost design driving position and reclinable forward seat backs in their nominal design driving position;

(b) Direction of impact shall be either:

(b)(1) In a vertical plane parallel to the vehicle longitudinal axis; or

(b)(2) In a plane normal to the surface at the point of contact.

(c) For seats without head restraints installed, tests shall be performed for each individual split or bucket seat back at points within 100 mm left and right of its centerline, and for each bench seat back between points 100 mm outboard of the centerline of each outboard designated seating position;

(d) For seats having head restraints installed, each test shall be conducted with the head restraints in place at its lowest adjusted position, at a point on the head restraint centerline; and

(e) For a seat that is installed in more than one body style, tests conducted at the fore and aft extremes identified by application of subparagraph (a) shall be deemed to have demonstrated all intermediate conditions.

S5.3 Interior compartment doors. Each interior compartment door assembly located in an instrument panel, console assembly, seat back, or side panel adjacent to a designated seating position shall remain closed when tested in accordance with either S5.3.1(a) and S5.3.1(b) or S5.3.1(a) and S5.3.1(c). Additionally, any interior compartment door located in an instrument panel or seat back shall remain closed when the instrument panel or seat back is tested in accordance with S5.1 and S5.2. All interior compartment door assemblies with a locking device must be tested with the locking device in an unlocked position.

S5.3.1 Demonstration procedures.

(a) Subject the interior compartment door latch system to an inertia load of 10g in a horizontal transverse direction and an inertia load of 10g in a vertical direction in accordance with the procedure described in section 5 of SAE Recommended Practice J839b, "Passenger Car Side Door Latch Systems," May 1965, or an approved equivalent.

(b) Impact the vehicle perpendicularly into a fixed collision barrier at a forward longitudinal velocity of 48 kilometers per hour.

(c) Subject the interior compartment door latch system to a horizontal inertia load of 30g in a longitudinal direction in accordance with the procedure described in section 5 of SAE Recommended Practice J839b, "Passenger Car Side Door Latch Systems," May 1965, or an approved equivalent.

S5.4 Sun visors.

S5.4.1 A sun visor that is constructed of or covered with energy-absorbing material shall be provided for each front outboard designated seating position.

S5.4.2 Each sun visor mounting shall present no rigid material edge radius of less than 3.2 mm that is statically contactable by a spherical 165 mm diameter head form.

S5.5 Armrests.

S5.5.1 General. Each installed armrest shall conform to at least one of the following:

(a) It shall be constructed with energy-absorbing material and shall deflect or collapse laterally at least 50 mm without permitting contact with any underlying rigid material.

(b) It shall be constructed with energy-absorbing material that deflects or collapses to within 32 mm of a rigid test panel surface without permitting contact with any rigid material. Any rigid material between 13 and 32 mm from the panel surface shall have a minimum vertical height of not less than 25 mm.

(c) Along not less than 50 continuous mm of its length, the armrest shall, when measured vertically in side elevation, provide at least 50 mm of coverage within the pelvic impact area.

S5.5.2 Folding armrests. Each armrest that folds into the seat back or between two seat backs shall either:

(a) Meet the requirements of S5.5.1; or

(b) Be constructed of or covered with energy-absorbing material.

S6 Requirements for upper interior components.

S6.1 Vehicles manufactured on or after September 1, 1998, and before September 1, 2002. Except as provided in S6.3 and S6.1.4, for vehicles manufactured on or after September 1, 1998 and before September 1, 2002, a percentage of the manufacturer's production, as specified in S6.1.1, S6.1.2, or S6.1.3 shall conform, at the manufacturer's option, to either S6.1(a) or S6.1(b). For vehicles manufactured by final stage manufacturers on or after September 1, 1998 and before September 1, 2006, a percentage of the manufacturer's production as specified in S6.1.4 shall, except as provided in S6.3, conform, to either S6.1(a) or S6.1(b). The manufacturer shall select the option by the time it certifies the vehicle and may not thereafter select a different option for the vehicle.

(a) When tested under the conditions of S8, comply with the requirements specified in S7 at the target locations specified in S10 when impacted by the free motion headform specified in S8.9 at any speed up to and including 24 km/h (15 mph). The requirements do not apply to any target that cannot be located using the procedures of S10.

(b) When equipped with a dynamically deployed upper interior head protection system and tested under the conditions of S8, comply with the requirements specified in S7 at the target locations specified in S10 as follows:

(b)(1) Targets that are not located over any point inside the area measured along the contour of the vehicle surface within 50 mm (2.0 inch) of the periphery of the stowed system projected perpendicularly onto the vehicle interior surface, including mounting and inflation components but exclusive of any cover or covers, shall be impacted by the free motion headform specified in S8.9 at any speed up to and including 24 km/h (15 mph). The requirements do not apply to any targets that can not be located by using the procedures of S10.

(b)(2) Targets that are over any point inside the area measured along the contour of the vehicle interior within 50 mm (2.0 inch) of the periphery of the stowed system projected perpendicularly onto the vehicle interior surface, including mounting and inflation components but exclusive of any cover or covers, when the dynamically deployed upper interior head protection system is not deployed, shall be impacted by the free motion headform specified in S8.9 at any speed up to and including 19 km/h (12 mph) with the system undeployed. The requirements do not apply to any target that can not be located using the procedures of S10.

(b)(3) Each vehicle shall, when equipped with a dummy test device specified in part 572, subpart M, and tested as specified in S8.16 through S8.28, comply with the requirements specified in S7 when crashed into a fixed, rigid pole of 254 mm in diameter, at any velocity between 24 kilometers per hour (15 mph) and 29 kilometers per hour (18 mph).

S6.1.1 Phase-in Schedule #1

S6.1.1.1 Vehicles manufactured on or after September 1, 1998 and before September 1, 1999. Subject to S6.1.5(a), for vehicles manufactured by a manufacturer on or after September 1, 1998 and before September 1, 1999, the amount of vehicles complying with S7 shall be not less than 10 percent of:

(a) The manufacturer's average annual production of vehicles manufactured on or after September 1, 1996 and before September 1, 1999, or

(b) The manufacturer's production on or after September 1, 1998 and before September 1, 1999.

S6.1.1.2 Vehicles manufactured on or after September 1, 1999 and before September 1, 2000. Subject to S6.1.5(b), for vehicles manufactured by a manufacturer on or after September 1, 1999 and before September 1, 2000, the amount of vehicles complying with S7 shall be not less than 25 percent of:

(a) The manufacturer's average annual production of vehicles manufactured on or after September 1, 1997 and before September 1, 2000, or

(b) The manufacturer's production on or after September 1, 1999 and before September 1, 2000.

S6.1.1.3 Vehicles manufactured on or after September 1, 2000 and before September 1, 2001. Subject to S6.1.5(c), for vehicles manufactured by a manufacturer on or after September 1, 2000 and before September 1, 2001, the amount of vehicles complying with S7 shall be not less than 40 percent of:

(a) The manufacturer's average annual production of vehicles manufactured on or after September 1, 1998 and before September 1, 2001, or

(b) The manufacturer's production on or after September 1, 2000 and before September 1, 2001.

S6.1.1.4 Vehicles manufactured on or after September 1, 2001 and before September 1, 2002. Subject to S6.1.5(d), for vehicles manufactured by a manufacturer on or after September 1, 2001 and before September 1, 2002, the amount of vehicles complying with S7 shall be not less than 70 percent of:

(a) The manufacturer's average annual production of vehicles manufactured on or after September 1, 1999 and before September 1, 2002, or

(b) The manufacturer's production on or after September 1, 2001 and before September 1, 2002.

S6.1.2 Phase-in Schedule #2

S6.1.2.1 Vehicles manufactured on or after September 1, 1998 and before September 1, 1999. Subject to S6.1.5(a), for vehicles manufactured by a manufacturer on or after September 1, 1998 and before September 1, 1999, the amount of vehicles complying with S7 shall be not less than seven percent of:

(a) The manufacturer's average annual production of vehicles manufactured on or after September 1, 1996 and before September 1, 1999, or

(b) The manufacturer's production on or after September 1, 1998 and before September 1, 1999.

S6.1.2.2 Vehicles manufactured on or after September 1, 1999 and before September 1, 2000. Subject to S6.1.5(b), for vehicles manufactured by a manufacturer on or after September 1, 1999 and before September 1, 2000, the amount of vehicles complying with S7 shall be not less than 31 percent of:

(a) The manufacturer's average annual production of vehicles manufactured on or after September 1, 1997 and before September 1, 2000, or

(b) The manufacturer's production on or after September 1, 1999 and before September 1, 2000.

S6.1.2.3 Vehicles manufactured on or after September 1, 2000 and before September 1, 2001. Subject to S6.1.5(c), for vehicles manufactured by a manufacturer on or after September 1, 2000 and before September 1, 2001, the amount of vehicles complying with S7 shall be not less than 40 percent of:

(a) The manufacturer's average annual production of vehicles manufactured on or after September 1, 1998 and before September 1, 2001, or

(b) The manufacturer's production on or after September 1, 2000 and before September 1, 2001.

S6.1.2.4 Vehicles manufactured on or after September 1, 2001 and before September 1, 2002. Subject to S6.1.5(d), for vehicles manufactured by a manufacturer on or after September 1, 2001 and before September 1, 2002, the amount of vehicles complying with S7 shall be not less than 70 percent of:

(a) The manufacturer's average annual production of vehicles manufactured on or after September 1, 1999 and before September 1, 2002, or

(b) The manufacturer's production on or after September 1, 2001 and before September 1, 2002.

S6.1.3 Phase-in Schedule #3

S6.1.3.1 Vehicles manufactured on or after September 1, 1998 and before September 1, 1999 are not required to comply with the requirements specified in S7.

S6.1.3.2 Vehicles manufactured on or after September 1, 1999 shall comply with the requirements specified in S7.

S6.1.4 Phase-in Schedule #4. A final stage manufacturer or alterer may, at its option, comply with the requirements set forth in S6.1.4.1 and S6.1.4.2.

S6.1.4.1 Vehicles manufactured on or after September 1, 1998 and before September 1, 2009 are not required to comply with the requirements specified in S7.

S6.1.4.2 Vehicles manufactured on or after September 1, 2009 shall comply with the requirements specified in S7.

S6.1.5 Calculation of complying vehicles.

(a) For the purposes of complying with S6.1.1.1 or S6.1.2.1, a manufacturer may count a vehicle if it is manufactured on or after May 8, 1997, but before September 1, 1999.

(b) For the purposes of complying with S6.1.1.2 or S6.1.2.2, a manufacturer may count a vehicle if it:

(b)(1) Is manufactured on or after May 8, 1997, but before September 1, 2000, and

(b)(2) Is not counted toward compliance with S6.1.1.1 or S6.1.2.1, as appropriate.

(c) For the purposes of complying with S6.1.1.3 or S6.1.2.3, a manufacturer may count a vehicle if it:

(c)(1) Is manufactured on or after May 8, 1997, but before September 1, 2001, and

(c)(2) Is not counted toward compliance with S6.1.1.1, S6.1.1.2, S6.1.2.1, or S6.1.2.2, as appropriate.

(d) For the purposes of complying with S6.1.1.4 or S6.1.2.4, a manufacturer may count a vehicle if it:

(d)(1) Is manufactured on or after May 8, 1997, but before September 1, 2002, and

(d)(2) Is not counted toward compliance with S6.1.1.1, S6.1.1.2, S6.1.1.3, S6.1.2.1, S6.1.2.2, or S6.1.2.3, as appropriate.

S6.1.6 Vehicles produced by more than one manufacturer.

S6.1.6.1 For the purpose of calculating average annual production of vehicles for each manufacturer and the number of vehicles manufactured by each manufacturer under S6.1.1 through S6.1.4, a vehicle produced by more than one manufacturer shall be attributed to a single manufacturer as follows, subject to S6.1.6.2.

(a) A vehicle which is imported shall be attributed to the importer.

(b) A vehicle manufactured in the United States by more than one manufacturer, one of which also markets the vehicle, shall be attributed to the manufacturer which markets the vehicle.

S6.1.6.2 A vehicle produced by more than one manufacturer must be attributed to any one of the vehicle's manufacturers specified by an express written contract, reported to the National Highway Traffic Safety Administration under 49 CFR Part 585, between the manufacturer so specified and the manufacturer to which the vehicle would otherwise be attributed under S6.1.6.1.

S6.2 Vehicles manufactured on or after September 1, 2002 and vehicles built in two or more stages manufactured after September 1, 2006. Except as provided in S6.1.4 and S6.3, vehicles manufactured on or after September 1, 2002 shall, when tested under the conditions of S8, conform, at the manufacturer's option, to either S6.2(a) or S6.2(b). Vehicles manufactured by final stage manufacturers on or after September 1, 2006 shall, except as provided in S6.3, when tested under the conditions of S8, conform, at the manufacturer's option, to either S6.2(a) or S6.2(b). The manufacturer shall select the option by the time it certifies the vehicle and may not thereafter select a different option for the vehicle.

(a) When tested under the conditions of S8, comply with the requirements specified in S7 at the target locations specified in S10 when impacted by the free motion headform specified in S8.9 at any speed up to and including 24 km/h (15 mph). The requirements do not apply to any target that cannot be located using the procedures of S10.

(b) When equipped with a dynamically deployed upper interior head protection system and tested under the conditions of S8, comply with the requirements specified in S7 at the target locations specified in S10 as follows:

(b)(1) Targets that are not located over any point inside the area measured along the contour of the vehicle surface within 50 mm (2.0 inch) of the periphery of the stowed system projected perpendicularly onto the vehicle interior surface, including mounting and inflation components but exclusive of any cover or covers, shall be impacted by the free motion headform specified in S8.9 at any speed up to and including 24 km/h (15 mph). The requirements do not apply to any targets that cannot be located by using the procedures of S10.

(b)(2) Targets that are over any point inside the area measured along the contour of the vehicle interior within 50 mm (2.0 inch) of the periphery of the stowed system projected perpendicularly onto the vehicle interior surface, including mounting and inflation components but exclusive of any cover or covers, when the dynamically deployed upper interior head protection system is not deployed, shall be impacted by the free motion headform specified in S8.9 at any speed up to and including 19 km/h (12 mph) with the system undeployed. The requirements do not apply to any target that cannot be located using the procedures of S10.

(b)(3) Except as provided in S6.2(b)(4), each vehicle shall, when equipped with a dummy test device specified in 49 CFR part 572, subpart M, and tested as specified in S8.16 through S8.28, comply with the requirements specified in S7 when crashed into a fixed, rigid pole of 254 mm in diameter, at any velocity between 24 kilometers per hour (15 mph) and 29 kilometers per hour (18 mph).

(b)(4) Vehicles certified as complying with the vehicle-to-pole requirements of S9 of 49 CFR 571.214, Side Impact Protection, need not comply with the pole test requirements specified in S6.2(b)(3) of this section.

S6.3 A vehicle need not meet the requirements of S6.1 through S6.2 for:

(a) Any target located on a convertible roof frame or a convertible roof linkage mechanism.

(b) Any target located rearward of a vertical plane 600 mm behind the seating reference point of the rearmost designated seating position. For altered vehicles and vehicles built in two or more stages, including ambulances and motor homes, any target located rearward of a vertical plane 300 mm behind the seating reference point of the driver's designated seating position (tests for altered vehicles and vehicles built in two or more stages do not include, within the time period for measuring HIC(d), any free motion headform contact with components rearward of this plane). If an altered vehicle partition positioned between the seating reference point of the driver's designated seating position and a vertical plane 300 mm behind the seating reference point of the driver's designated seating position, any target located rearward of the vertical partition is excluded.

(c) Any target in a vehicle manufactured in two or more stages that is delivered to a final stage manufacturer without an occupant compartment. Note: Motor homes, ambulances, and other vehicles manufactured using chassis cab, a cut-away van, or any other incomplete vehicle delivered to a final stage manufacturer with a furnished front compartment are not excluded under this S6.3(c).

(d) Any target in a walk-in van-type vehicles.

(e) Any target located on the seat belt mounting structures, door frames and other door frames before December 1, 2005.

S7 Performance Criterion. The HIC(d) shall not exceed 1000 when calculated in accordance with the following formula:

$$HIC = \left[\frac{1}{(t_2 - t_1)} \int_{t_1}^{t_2} a\,dt \right]^{2.5} (t_2 - t_1)$$

Where the term a is the resultant head acceleration expressed as a multiple of g (the acceleration of gravity), and t^1 and t^2 are any two points in time during the impact which are separated by not more than a 36 millisecond time interval.

(a) For the free motion headform; HIC(d)=0.75446 (free motion headform HIC)+166.4.

(b) For the part 572, subpart M, anthropomorphic test dummy; HIC(d)=HIC.

S8 Target location and test conditions. The vehicle shall be tested and the targets specified in S10 located under the following conditions.

S8.1 Vehicle test attitude.

(a) The vehicle is supported off its suspension at an attitude determined in accordance with S8.1(b).

(b) Directly above each wheel opening, determine the vertical distance between a level surface and a standard reference point on the test vehicle's body under the conditions of S8.1(b)(1) through S8.1(b)(3).

(b)(1) The vehicle is loaded to its unloaded vehicle weight, plus its rated cargo and luggage capacity or 136 kg, whichever is less, secured in the luggage area. The load placed in the cargo area is centered over the longitudinal centerline of the vehicle.

(b)(2) The vehicle is filled to 100 percent of all fluid capacities.

(b)(3) All tires are inflated to the manufacturer's specifications listed on the vehicle's tire placard.

S8.2 Windows and Sunroofs.

(a) Movable vehicle windows are placed in the fully open position.

(b) For testing, any window on the opposite side of the longitudinal centerline of the vehicle from the target to be impacted may be removed.

(c) For testing, movable sunroofs are placed in the fully open position.

S8.3 Convertible tops. The top, if any, of convertibles and open-body type vehicles is in the closed passenger compartment configuration.

S8.4 Doors.

(a) Except as provided in S8.4(b) or S8.4(c), doors, including any rear hatchback or tailgate, are fully closed and latched but not locked.

(b) During testing, any side door on the opposite side of the longitudinal centerline of the vehicle from the target to be impacted may be open or removed.

(c) During testing, any rear hatchback or tailgate may be open or removed for testing any target except targets on the rear header, rearmost pillars, or the rearmost other side rail on either side of the vehicle.

S8.5 Sun visors. Each sun visor shall be placed in any position where one side of the visor is in contact with the vehicle interior surface (windshield, side rail, front header, roof, etc.).

S8.6 Steering wheel and seats.

(a) During targeting, the steering wheel and seats may be placed in any position intended for use while the vehicle is in motion.

(b) During testing, the steering wheel and seats may be removed from the vehicle.

S8.7 Seat belt anchorages. If a target is on a seat belt anchorage, and if the seat belt anchorage is adjustable, tests are conducted with the anchorage adjusted to a point midway between the two extreme adjustment positions. If the anchorage has distinct adjustment positions, none of which is midway between the two extreme positions, tests are conducted with the anchorage adjusted to the nearest position above the midpoint of the two extreme positions.

S8.8 Temperature and humidity.

(a) The ambient temperature is between 19 ºC and 26 ºC, at any relative humidity between 10 percent and 70 percent.

(b) Tests are not conducted unless the headform specified in S8.9 is exposed to the conditions specified in S8.8(a) for a period not less than four hours.

S8.9 Headform. The headform used for testing conforms to the specifications of part 572, subpart L of this chapter.

S8.10 Forehead impact zone. The forehead impact zone of the headform is determined according to the procedure specified in (a) through (f).

(a) Position the headform so that the baseplate of the skull is horizontal. The midsagittal plane of the headform is designated as Plane S.

(b) From the center of the threaded hole on top of the headform, draw a 69 mm line forward toward the forehead, coincident with Plane S, along the contour of the outer skin of the headform. The front end of the line is designated as Point P. From Point P, draw a 100 mm line forward toward the forehead, coincident with Plane S, along the contour of the outer skin of the headform. The front end of the line is designated as Point O.

(c) Draw a 125 mm line which is coincident with a horizontal plane along the contour of the outer skin of the forehead from left to right through Point O so that the line is bisected at Point O. The end of the line on the left side of the headform is designated as Point a and the end on the right as Point b.

(d) Draw another 125 mm line which is coincident with a vertical plane along the contour of the outer skin of the forehead through Point P so that the line is bisected at Point P. The end of the line on the left side of the headform is designated as Point c and the end on the right as Point d.

(e) Draw a line from Point a to Point c along the contour of the outer skin of the headform using a flexible steel tape. Using the same method, draw a line from Point b to Point d.

(f) The forehead impact zone is the surface area on the FMH forehead bounded by lines a-O-b and c-P-d, and a-c and b-d.

S8.11 Target circle. The area of the vehicle to be impacted by the headform is marked with a solid circle 12.7 mm in diameter, centered on the targets specified in S10, using any transferable opaque coloring medium.

S8.12 Location of head center of gravity.

(a) Location of head center of gravity for front outboard designated seating positions (CG-F). For determination of head center of gravity, all directions are in reference to the seat orientation.

(a)(1) Location of rearmost CG-F (CG-F2). For front outboard designated seating positions, the head center of gravity with the seat in its rearmost normal design driving or riding position (CG-F2) is located 160 mm rearward and 660 mm upward from the seating reference point.

(a)(2) Location of forward most CG-F (CG-F1). For front outboard designated seating positions, the head center of gravity with the seat in its forward most adjustment position (CG-F1) is located horizontally forward of CG-F2 by the distance equal to the fore-aft distance of the seat track.

(b) Location of head center of gravity for rear outboard designated seating positions (CG-R). For rear outboard designated seating positions, the head center of gravity (CG-R) is located 160 mm rearward, relative to the seat orientation, and 660 mm upward from the seating reference point.

S8.13 Impact configuration.

S8.13.1 The headform is launched from any location inside the vehicle which meets the conditions of S8.13.4. At the time of launch, the midsagittal plane of the headform is vertical and the headform is upright.

S8.13.2 The headform travels freely through the air, along a velocity vector that is perpendicular to the headform's skull cap plate, not less than 25 mm before making any contact with the vehicle.

S8.13.3 At the time of initial contact between the headform and the vehicle interior surface, some portion of the forehead impact zone of the headform must contact some portion of the target circle.

S8.13.4 Approach Angles. The headform launching angle is as specified in Table 1. For components for which Table 1 specifies a range of angles, the headform launching angle is within the limits determined using the procedures specified in S8.13.4.1 and S8.13.4.2, and within the range specified in Table I, using the orthogonal reference system specified in S9.

S8.13.4.1 Horizontal Approach Angles for Headform Impacts.

(a) Left A-Pillar Horizontal Approach Angles.

(a)(1) Locate a line formed by the shortest horizontal distance between CG-F1 for the left seat and the right A-pillar. The maximum horizontal approach angle for the left A-pillar equals 360 degrees minus the angle formed by that line and the X-axis of the vehicle, measured counterclockwise.

(a)(2) Locate a line formed by the shortest horizontal distance between CG-F2 for the left seat and the left A-pillar. The minimum horizontal approach angle for the left A-pillar impact equals the angle formed by that line and the X-axis of the vehicle, measured counterclockwise.

(b) Right A-Pillar Horizontal Approach Angles.

(b)(1) Locate a line formed by the shortest horizontal distance between CG-F1 for the right seat and the left A-pillar. The minimum horizontal approach angle for the right A-pillar equals 360 degrees minus the angle formed by that line and the X-axis of the vehicle, measured counterclockwise.

(b)(2) Locate a line formed by the shortest horizontal distance between CG-F2 for the right seat and the right A-pillar. The maximum horizontal approach angle for the right A-pillar impact equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise.

(c) Left B-Pillar Horizontal Approach Angles.

(c)(1) Locate a line formed by the shortest horizontal distance between CG-F2 for the left seat and the left B-pillar. The maximum horizontal approach angle for the left B-pillar equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise, or 270 degrees, whichever is greater.

(c)(2) Locate a line formed by the shortest horizontal distance between CG-R for the left seat and the left B-pillar. The minimum horizontal approach angle for the left B-pillar equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise.

(d) Right B-Pillar Horizontal Approach Angles.

(d)(1) Locate a line formed by the shortest horizontal distance between CG-F2 for the right seat and the right B-pillar. The minimum horizontal approach angle for the right B-pillar equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise, or 90 degrees, whichever is less.

(d)(2) Locate a line formed by the shortest horizontal distance between CG-R for the right seat and the right B-pillar. The maximum horizontal approach angle for the right B-pillar equals the angle between that line and the X-axis of the vehicle measured counterclockwise.

(e) Left door frame horizontal approach angles.

(e)(1) Locate a line formed by the shortest horizontal distance between CG-F2 for the left seat and the left door frame. The maximum horizontal approach angle for the left door frame equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise, or 270 degrees, whichever is greater.

(e)(2) Locate a line formed by the shortest horizontal distance between CG-R for the left seat and the left door frame. The minimum horizontal approach angle for the left door frame equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise.

(f) Right door frame horizontal approach angles.

(f)(1) Locate a line formed by the shortest horizontal distance between CG-F2 for the right seat and the right door frame. The minimum horizontal approach angle for the right door frame equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise, or 90 degrees, whichever is less.

(f)(2) Locate a line formed by the shortest horizontal distance between CG-R for the right seat and the right door frame. The maximum horizontal approach angle for the right door frame equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise

(g) Left seat belt mounting structure horizontal approach angles.

(g)(1) Locate a line formed by the shortest horizontal distance between CG-F2 for the left seat and the left seat belt mounting structure. If the seat belt mounting structure is below a horizontal plane passing through CG-F2 for the left seat, locate the point 200 mm directly below CG-F2 and locate a line formed by the shortest horizontal distance between that point and the left seat belt mounting structure. The maximum horizontal approach angle for the left seat belt mounting structure equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise, or 270 degrees, whichever is greater.

(g)(2) Locate a line formed by the shortest horizontal distance between CG-R for the left seat and the left seat belt mounting structure. If the seat belt mounting structure is below a horizontal plane passing through CG-R for the left seat, locate the point 200 mm directly below CG-R and locate a line formed by the shortest horizontal distance between that point and the left seat belt mounting structure. The minimum horizontal approach angle for the left seat belt mounting structure equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise. If the CG-R does not exist, or is forward of the seat belt mounting structure, the maximum horizontal approach angle is 270 degrees.

(h) Right seat belt mounting structure horizontal approach angles.

(h)(1) Locate a line formed by the shortest horizontal distance between CG-F2 for the right seat and the right seat belt mounting structure. If the seat belt mounting structure is below a horizontal plane passing through CG-F2 for the right seat, locate the point 200 mm directly below that CG-F2 and locate a line formed by the shortest horizontal distance between that point and the right seat belt mounting structure. The minimum horizontal approach angle for the right seat belt mounting structure equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise, or 90 degrees, whichever is less.

(h)(2) Locate a line formed by the shortest horizontal distance between CG-R for the right seat and the right seat belt mounting structure. If the seat belt mounting structure is below a horizontal plane passing through CG-R, locate the point 200 mm directly below CG-R and locate a line formed by the shortest horizontal distance between that point and the right seat belt mounting structure. The maximum horizontal approach angle for the right seat belt mounting structure equals the angle formed by that line and the X-axis of the vehicle measured counterclockwise. If the CG-R does not exist, or is forward of the seat belt mounting structure, the maximum horizontal approach angle is 90 degrees.

S8.13.4.2 Vertical Approach Angles.

(a) Position the forehead impact zone in contact with the selected target at the prescribed horizontal approach angle. If a range of horizontal approach angles is prescribed, position the forehead impact zone in contact with the selected target at any horizontal approach angle within the range which may be used for testing.

(b) Keeping the forehead impact zone in contact with the target, rotate the FMH upward until the lip, chin or other part of the FMH contacts the component or other portion of the vehicle interior.

(b)(1) Except as provided in S8.13.4.2(b)(2), keeping the forehead impact zone in contact with the target, rotate the FMH downward by 5 degrees for each target to determine the maximum vertical angle.

(b)(2) For all pillars, except A-pillars, and all door frames and seat belt mounting structures, keeping the forehead impact zone in contact with the target, rotate the FMH downward by 10 degrees for each target to determine the maximum vertical angle.

S8.14 Multiple impacts.

(a) A vehicle being tested may be impacted multiple times, subject to the limitations in S8.14(b), (c), (d) and (e).

(b) As measured as provided in S8.14(d), impacts within 300 mm of each other may not occur less than 30 minutes apart.

(c) As measured as provided in S8.14(d), no impact may occur within 150 mm of any other impact.

(d) For S8.14(b) and S8.14(c), the distance between impacts is the distance between the center of the target circle specified in S8.11 for each impact, measured along the vehicle interior.

(e) No impact may occur within the "exclusion zone" of any pillar target specified in S10.1 through S10.4, door frame target specified in S10.14 and S10.15, upper roof target specified in S10.9, or seat belt mounting structure target specified in S10.16. The "exclusion zone" is determined according to the procedure in S8.14(f) through S8.14(k).

(f) Locate the point, Point X, at the center of the target circle specified in S8.11 for the tested target.

(g) Determine two spheres centered on Point X. Radii of these spheres are 150 mm and 200 mm, respectively.

(h) Locate a horizontal plane passing through Point X. Determine the intersection points, if they exist, of the small sphere surface, the horizontal plane, and the vehicle interior surface. Relative to Point X, the point on the left is Point L and the point on the right is Point R.

(i) Locate a vertical plane, Plane Z, passing through Point X and coincident (within ± 5˚) with the horizontal approach angle used or intended for use in testing the target centered on Point X.

(j) If either Point L or Point R does not exist, extend Line LX and/or Line RX, as appropriate, perpendicular to Plane Z beyond Point X by 150 mm. The end of the line is designated as Point L or Point R, as appropriate.

(k) Locate a vertical plane, Plane ZL, passing through Point L and parallel to Plane Z. Locate another vertical plane, Plane ZR, passing through Point R and parallel to Plane Z. The "exclusion zone" is the vehicle interior surface area between Plane ZL and Plane ZR below the upper boundary of the smaller sphere and above the lower boundary of the larger sphere. Points on the intersection of the vehicle interior surface and the large sphere below the target, the small sphere above the target, Plane ZL and Plane ZR are not included in the "exclusion zone."

S8.15 Upper Roof. The upper roof of a vehicle is determined according to the procedure specified in S8.15 (a) through (h).

(a) Locate the transverse vertical plane A at the forward most point where it contacts the interior roof (including trim) at the vehicle centerline.

(b) Locate the transverse vertical plane B at the rearmost point where it contacts the interior roof (including trim) at the vehicle centerline.

(c) Measure the horizontal distance (D1) between Plane A and Plane B.

(d) Locate the vertical longitudinal plane C at the leftmost point at which a vertical transverse plane, located 300 mm rearward of the A-pillar reference point described in S10.1(a), contacts the interior roof (including trim).

(e) Locate the vertical longitudinal plane D at the rightmost point at which a vertical transverse plane, located 300 mm rearward of the A-pillar reference point described in S10.1(a), contacts the interior roof (including trim).

(f) Measure the horizontal distance (D2) between Plane C and Plane D.

(g) Locate a point (Point M) on the interior roof surface, midway between Plane A and Plane B along the vehicle longitudinal centerline.

(h) The upper roof zone is the area of the vehicle upper interior surface bounded by the four planes described in S8.15(h)(1) and S8.15(h)(2):

(h)(1) A transverse vertical plane E located at a distance of (.35 D1) forward of Point M and a transverse vertical plane F located at a distance of (.35 D1) rearward of Point M, measured horizontally.

(h)(2) A longitudinal vertical plane G located at a distance of (.35 D2) to the left of Point M and a longitudinal vertical plane H located at a distance of (.35 D2) to the right of Point M, measured horizontally.

S8.16 Test weight—vehicle to pole test. Each vehicle shall be loaded to its unloaded vehicle weight, plus 136 kilograms (300 pounds) or its rated cargo and luggage capacity (whichever is less), secured in the luggage or load-carrying area, plus the weight of the necessary anthropomorphic test dummy. Any added test equipment shall be located away from impact areas in secure places in the vehicle.

S8.17 Vehicle test attitude—vehicle to pole test. Determine the distance between a level surface and a standard reference point on the test vehicle's body, directly above each wheel opening, when the vehicle is in its "as delivered" condition. The "as delivered" condition is the vehicle as received at the test site, filled to 100 percent of all fluid capacities and with all tires inflated to the manufacturer's specifications listed on the vehicle's tire placard. Determine the distance between the same level surface and the same standard reference points in the vehicle's "fully loaded condition." The "fully loaded condition" is the test vehicle loaded in accordance with S8.16. The load placed in the cargo area shall be centered over the longitudinal centerline of the vehicle. The pretest vehicle attitude shall be the same as either the "as delivered" or "fully loaded" attitude or is between the "as delivered" attitude and the "fully loaded" attitude. If the test configuration requires that the vehicle be elevated off the ground, the pretest vehicle attitude must be maintained.

S8.18 Adjustable seats—vehicle to pole test. Initially, adjustable seats shall be adjusted as specified in S8.3.1 of Standard 214 (49 CFR 571.214).

S8.19 Adjustable seat back placement—vehicle to pole test. Initially, position adjustable seat backs in the manner specified in S8.3.1 of Standard 214 (49 CFR 571.214).

S8.20 Adjustable steering wheels—vehicle to pole test. Adjustable steering controls shall be adjusted so that the steering wheel hub is at the geometric center of the locus it describes when it is moved through its full range of driving positions.

S8.21 Windows and sunroof—vehicle to pole test. Movable windows and vents shall be placed in the fully open position. Any sunroof shall be placed in the fully closed position.

S8.22 Convertible tops—vehicle to pole test. The top, if any, of convertibles and open-body type vehicles shall be in the closed passenger compartment configuration.

S8.23 Doors—vehicle to pole test. Doors, including any rear hatchback or tailgate, shall be fully closed and latched but not locked.

S8.24 Impact reference line—vehicle to pole test. On the striking side of the vehicle, place an impact reference line at the intersection of the vehicle exterior and a transverse vertical plane passing through the center of gravity of the head of the dummy seated in accordance with S8.28, in the front outboard designated seating position.

S8.25 Rigid Pole—vehicle to pole test. The rigid pole is a vertical metal structure beginning no more than 102 millimeters (4 inches) above the lowest point of the tires on the striking side of the test vehicle when the vehicle is loaded as specified in S8.16 and extending above the highest point of the roof of the test vehicle. The pole is 254 mm ±3 mm (10 inches) in diameter and set off from any mounting surface, such as a barrier or other structure, so that the test vehicle will not contact such a mount or support at any time within 100 milliseconds of the initiation of vehicle to pole contact.

S8.26 Impact configuration—vehicle to pole test. The rigid pole shall be stationary. The test vehicle shall be propelled sideways so that its line of forward motion forms an angle of 90 degrees (±3 degrees) with the vehicle's longitudinal center line. The impact reference line shall be aligned with the center line of the rigid pole so that, when the vehicle-to-pole contact occurs, the center line of the pole contacts the vehicle area bounded by two transverse vertical planes 38 mm (1.5 inches) forward and aft of the impact reference line.

S8.27 Anthropomorphic test dummy—vehicle to pole test.

S8.27.1 The anthropomorphic test dummy used for evaluation of a vehicle's head impact protection shall conform to the requirements of subpart M of part 572 of this chapter (49 CFR part 572, subpart M). In a test in which the test vehicle is striking its left side, the dummy is to be configured and instrumented to strike on its left side, in accordance with subpart M of part 572. In a test in which the test vehicle is striking its right side, the dummy is to be configured and instrumented to strike its right side, in accordance with subpart M of part 572.

S8.27.2 The part 572, subpart M, test dummy specified is clothed in form fitting cotton stretch garments with short sleeves and midcalf length pants. Each foot of the test dummy is equipped with a size 11EEE shoe, which meets the configuration size, sole, and heel thickness specifications of MIL-S-13192 (1976) and weighs 0.57 ±0.09 kilograms (1.25 ±0.2 pounds).

S8.27.3 Limb joints shall be set at between 1 and 2 g's. Leg joints are adjusted with the torso in the supine position.

S8.27.4 The stabilized temperature of the test dummy at the time of the side impact test shall be at any temperature between 20.6 ºC and 22.2 ºC.

S8.27.5 The acceleration data from the accelerometers installed inside the skull cavity of the test dummy are processed according to the practices set forth in SAE Recommended Practice J211, March 1995, "Instrumentation for Impact Tests," Class 1000.

S8.28 Positioning procedure for the Part 572 Subpart M test dummy— vehicle to pole test. The part 572, subpart M, test dummy is initially positioned in the front outboard seating position on the struck side of the vehicle in accordance with the provisions of S12.1 of Standard 214 (49 CFR 571.214), and the vehicle seat is positioned as specified in S8.3.1 of that standard. The position of the dummy is then measured as follows. Locate the horizontal plane passing through the dummy head center of gravity. Identify the rearmost point on the dummy head in that plane. Construct a line in the plane that contains the rearward point of the front door daylight opening and is perpendicular to the longitudinal vehicle centerline. Measure the longitudinal distance between the rearmost point on the dummy head and this line. If this distance is less than 50 mm (2 inches) or the point is not forward of the line, then the seat and/or dummy positions is adjusted as follows. First, the seat back angle is adjusted, a maximum of 5 degrees, until a 50 mm (2 inches) distance is achieved. If this is not sufficient to produce the 50 mm (2 inches) distance, the seat is moved forward until the 50 mm (2 inches) distance is achieved or until the knees of the dummy contact the dashboard or knee bolster, whichever comes first. If the required distance cannot be achieved through movement of the seat, the seat back angle is adjusted even further forward until the 50 mm (2 inches) distance is obtained or until the seat back is in its fully upright locking position.

S9. Orthogonal Reference System. The approach angles specified in S8.13.4 are determined using the reference system specified in S9.1 through S9.4.

S9.1 An orthogonal reference system consisting of a longitudinal X axis and a transverse Y axis in the same horizontal plane and a vertical Z axis through the intersection of X and Y is used to define the horizontal direction of approach of the headform. The X-Z plane is the vertical longitudinal zero plane and is parallel to the longitudinal centerline of the vehicle. The X-Y plane is the horizontal zero plane parallel to the ground. The Y-Z plane is the vertical transverse zero plane that is perpendicular to the X-Y and X-Z planes. The X coordinate is negative forward of the Y-Z plane and positive to the rear. The Y coordinate is negative to the left of the X-Z plane and positive to the right. The Z coordinate is negative below the X-Y plane and positive above it. (See Figure 1.)

S9.2 The origin of the reference system is the center of gravity of the headform at the time immediately prior to launch for each test.

S9.3 The horizontal approach angle is the angle between the X axis and the headform impact velocity vector projected onto the horizontal zero plane, measured in the horizontal zero plane in the counter-clockwise direction. A 0 degree horizontal vector and a 360 degree horizontal vector point in the positive X direction; a 90 degree horizontal vector points in the positive Y direction; a 180 degree horizontal vector points in the negative X direction; and a 270 horizontal degree vector points in the negative Y direction. (See Figure 2.)

S9.4 The vertical approach angle is the angle between the horizontal plane and the velocity vector, measured in the midsagittal plane of the headform. A 0 degree vertical vector in Table I coincides with the horizontal plane and a vertical vector of greater than 0 degrees in Table I makes an upward angle of the same number of degrees with that plane.

S10 Target Locations.

(a) The target locations specified in S10.1 through S10.16 are located on both sides of the vehicle and, except as specified in S10(b), are determined using the procedures specified in those paragraphs.

(b) Except as specified in S10(c), if there is no combination of horizontal and vertical angles specified in S8.13.4 at which the forehead impact zone of the free motion headform can contact one of the targets located using the procedures in S10.1 through S10.16, the center of that target is moved to any location within a sphere with a radius of 25 mm, centered on the center of the original target, which the forehead impact zone can contact at one or more combination of angles.

(c) If there is no point within the sphere specified in S10(b) which the forehead impact zone of the free motion headform can contact at one or more combination of horizontal and vertical angles specified in S8.13.4, the radius of the sphere is increased by 25 mm increments until the sphere contains at least one point that can be contacted at one or more combination of angles.

S10.1 A-pillar targets.

(a) A-pillar reference point and target AP1. On the vehicle exterior, locate a transverse vertical plane (Plane 1) which contacts the rearmost point of the windshield trim. The intersection of Plane 1 and the vehicle exterior surface is Line 1. Measuring along the vehicle exterior surface, locate a point (Point 1) on Line 1 that is 125 mm inboard of the intersection of Line 1 and a vertical plane tangent to the vehicle at the outboard most point on Line 1 with the vehicle side door open. Measuring along the vehicle exterior surface in a longitudinal vertical plane (Plane 2) passing through Point 1, locate a point (Point 2) 50 mm rearward of Point 1. Locate the A-pillar reference point (Point APR) at the intersection of the interior roof surface and a line that is perpendicular to the vehicle exterior surface at Point 2. Target AP1 is located at point APR.

(b) Target AP2. Locate the horizontal plane (Plane 3) which intersects point APR. Locate the horizontal plane (Plane 4) which is 88 mm below Plane 3. Target AP2 is the point in Plane 4 and on the A-pillar which is closest to CG-F2 for the nearest seating position.

(c) Target AP3. Locate the horizontal plane (Plane 5) containing the highest point at the intersection of the dashboard and the A-pillar. Locate a horizontal plane (Plane 6) half-way between Plane 3 and Plane 5. Target AP3 is the point on Plane 6 and the A-pillar which is closest to CG-F1 for the nearest seating position.

S10.2 B-pillar targets.

(a) B-pillar reference point and target BP1. Locate the point (Point 3) on the vehicle interior at the intersection of the horizontal plane passing through the highest point of the forward most door opening and the centerline of the width of the B-pillar, as viewed laterally. Locate a transverse vertical plane (Plane 7) which passes through Point 3. Locate the point (Point 4) at the intersection of the interior roof surface, Plane 7, and the plane, described in S8.15(h), defining the nearest edge of the upper roof. The B-pillar reference point (Point BPR) is the point located at the middle of the line from Point 3 to Point 4 in Plane 7, measured along the vehicle interior surface. Target BP1 is located at Point BPR.

(b) Target BP2. If a seat belt anchorage is located on the B-pillar, Target BP2 is located at any point on the anchorage.

(c) Target BP3. Target BP3 is located in accordance with this paragraph. Locate a horizontal plane (Plane 8) which intersects Point BPR. Locate a horizontal plane (Plane 9) which passes through the lowest point of the daylight opening forward of the pillar. Locate a horizontal plane (Plane 10) half-way between Plane 8 and Plane 9. Target BP3 is the point located in Plane 10 and on the interior surface of the B-pillar, which is closest to CG-F(2) for the nearest seating position.

(d) Target BP4. Locate a horizontal plane (Plane 11) half-way between Plane 9 and Plane 10. Target BP4 is the point located in Plane 11 and on the interior surface of the B-pillar which is closest to CG-R for the nearest seating position.

S10.3 Other pillar targets.

(a) Target OP1.

(a)(1) Except as provided in S10.3(a)(2), target OP1 is located in accordance with this paragraph. Locate the point (Point 5), on the vehicle interior, at the intersection of the horizontal plane through the highest point of the highest adjacent door opening or daylight opening (if no adjacent door opening) and the centerline of the width of the other pillar, as viewed laterally. Locate a transverse vertical plane (Plane 12) passing through Point 5. Locate the point (Point 6) at the intersection of the interior roof surface, Plane 12 and the plane, described in S8.15(h), defining the nearest edge of the upper roof. The other pillar reference point (Point OPR) is the point located at the middle of the line between Point 5 and Point 6 in Plane 12, measured along the vehicle interior surface. Target OP1 is located at Point OPR.

(a)(2) If a seat belt anchorage is located on the pillar, Target OP1 is any point on the anchorage.

(b) Target OP2. Locate the horizontal plane (Plane 13) intersecting Point OPR. Locate a horizontal plane (Plane 14) passing through the lowest point of the daylight opening forward of the pillar. Locate a horizontal plane (Plane 15) half-way between Plane 13 and Plane 14. Target OP2 is the point located on the interior surface of the pillar at the intersection of Plane 15 and the centerline of the width of the pillar, as viewed laterally.

S10.4 Rearmost pillar targets

(a) Rearmost pillar reference point and target RP1. Locate the point (Point 7) at the corner of the upper roof nearest to the pillar. The distance between Point M, as described in S8.15(g), and Point 7, as measured along the vehicle interior surface, is D. Extend the line from Point M to Point 7 along the vehicle interior surface in the same vertical plane by (3*D/7) beyond Point 7 or until the edge of a daylight opening, whichever comes first, to locate Point 8. The rearmost pillar reference point (Point RPR) is at the midpoint of the line between Point 7 and Point 8, measured along the vehicle interior. Target RP1 is located at Point RPR.

(b) Target RP2.

(b)(1) Except as provided in S10.4(b)(2), target RP2 is located in accordance with this paragraph. Locate the horizontal plane (Plane 16) through Point RPR. Locate the horizontal plane (Plane 17) 150 mm below Plane 16. Target RP2 is located in Plane 17 and on the pillar at the location closest to CG-R for the nearest designated seating position.

(b)(2) If a seat belt anchorage is located on the pillar, Target RP2 is any point on the anchorage.

S10.5 Front header targets.

(a) Target FH1. Locate the contour line (Line 2) on the vehicle interior trim which passes through the APR and is parallel to the contour line (Line 3) at the upper edge of the windshield on the vehicle interior. Locate the point (Point 9) on Line 2 that is 125 mm inboard of the APR, measured along that line. Locate a longitudinal vertical plane (Plane 18) that passes through Point 9. Target FH1 is located at the intersection of Plane 18 and the upper vehicle interior, halfway between a transverse vertical plane (Plane 19) through Point 9 and a transverse vertical plane (Plane 20) through the intersection of Plane 18 and Line 3.

(b) Target FH2.

(b)(1) Except as provided in S10.5(b)(2), target FH2 is located in accordance with this paragraph. Locate a point (Point 10) 275 mm inboard of Point APR, along Line 2. Locate a longitudinal vertical plane (Plane 21) that passes through Point 10. Target FH2 is located at the intersection of Plane 21 and the upper vehicle interior, halfway between a transverse vertical plane (Plane 22) through Point 10 and a transverse vertical plane (Plane 23) through the intersection of Plane 21 and Line 3.

(b)(2) If a sun roof opening is located forward of the front edge of the upper roof and intersects the mid-sagittal plane of a dummy seated in either front outboard seating position, target FH2 is the nearest point that is forward of a transverse vertical plane (Plane 24) through CG-F(2) and on the intersection of the mid-sagittal plane and the interior sunroof opening.

S10.6 Targets on the side rail between the A-pillar and the B-pillar or rearmost pillar in vehicles with only two pillars on each side of the vehicle.

(a) Target SR1. Locate a transverse vertical plane (Plane 25) 150 mm rearward of Point APR. Locate the point (Point 11) at the intersection of Plane 25 and the upper edge of the forward most door opening. Locate the point (Point 12) at the intersection of the interior roof surface, Plane 25 and the plane, described in S8.15(h), defining the nearest edge of the upper roof. Target SR1 is located at the middle of the line between Point 11 and Point 12 in Plane 25, measured along the vehicle interior.

(b) Target SR2. Locate a transverse vertical plane (Plane 26) 300 mm rearward of the APR or 300 mm forward of the BPR (or the RPR in vehicles with no B-pillar). Locate the point (Point 13) at the intersection of Plane 26 and the upper edge of the forward most door opening. Locate the point (Point 14) at the intersection of the interior roof surface, Plane 26 and the plane, described in S8.15(h), defining the nearest edge of the upper roof. Target SR2 is located at the middle of the line between Point 13 and Point 14 in Plane 26, measured along the vehicle interior.

S10.7 Other side rail target (target SR3).

(a) Except as provided in S10.7(b), target SR3 is located in accordance with this paragraph. Locate a transverse vertical plane (Plane 27) 150 mm rearward of either Point BPR or Point OPR. Locate the point (Point 15) as provided in either S10.7(a)(1) or S10.7(a)(2), as appropriate. Locate the point (Point 16) at the intersection of the interior roof surface, Plane 27 and the plane, described in S8.15(h), defining the nearest edge of the upper roof. Target SR3 is located at the middle of the line between Point 15 and Point 16 in Plane 27, measured along the vehicle interior surface.

(a)(1) If Plane 27 intersects a door or daylight opening, the Point 15 is located at the intersection of Plane 27 and the upper edge of the door opening or daylight opening.

(a)(2) If Plane 27 does not intersect a door or daylight opening, the Point 15 is located on the vehicle interior at the intersection of Plane 27 and the horizontal plane through the highest point of the door or daylight opening nearest Plane 27. If the adjacent door(s) or daylight opening(s) are equidistant to Plane 27, Point 15 is located on the vehicle interior at the intersection of Plane 27 and either horizontal plane through the highest point of each door or daylight opening.

(b) Except as provided in S10.7(c), if a grab handle is located on the side rail, target SR3 is located at any point on the anchorage of the grab-handle. Folding grab-handles are in their stowed position for testing.

(c) If a seat belt anchorage is located on the side rail, target SR3 is located at any point on the anchorage.

S10.8 Rear header target (target RH). Locate the point (Point 17) at the intersection of the surface of the upper vehicle interior, the mid-sagittal plane (Plane 28) of the outboard rearmost dummy and the plane, described in S8.15(h), defining the rear edge of the upper roof. Locate the point (Point 18) as provided in S10.8(a) or S10.8(b), as appropriate. Except as provided in S10.8(c), Target RH is located at the mid-point of the line that is between Point 17 and Point 18 and is in Plane 28, as measured along the surface of the vehicle interior.

(a) If Plane 28 intersects a rear door opening or daylight opening, then Point 18 is located at the intersection of Plane 28 and the upper edge of the door opening or the daylight opening (if no door opening).

(b) If Plane 28 does not intersect a rear door opening or daylight opening, then Point 18 is located on the vehicle interior at the intersection of Plane 28 and a horizontal plane through the highest point of the door or daylight opening nearest to Plane 28. If the adjacent door(s) or daylight opening(s) are equidistant to Plane 28, Point 18 is located on the vehicle interior at the intersection of Plane 28 and either horizontal plane through the highest point of each door or daylight opening.

(c) If Target RH is more than 112 mm from Point 18 on the line that is between Point 17 and Point 18 and is in Plane 28, as measured along the surface of the vehicle interior, then Target RH is the point on that line which is 112 mm from Point 18.

S10.9 Upper roof target (target UR). Target UR is any point on the upper roof.

S10.10 Sliding door track target (target SD). Locate the transverse vertical plane (Plane 29) passing through the middle of the widest opening of the sliding door, measured horizontally and parallel to the vehicle longitudinal centerline. Locate the point (Point 19) at the intersection of the surface of the upper vehicle interior, Plane 29 and the plane, described in S8.15(h), defining the nearest edge of the upper roof. Locate the point (Point 20) at the intersection of Plane 29 and the upper edge of the sliding door opening. Target SD is located at the middle of the line between Point 19 and Point 20 in Plane 29, measured along the vehicle interior.

S10.11 Roll-bar targets.

(a) Target RB1. Locate a longitudinal vertical plane (Plane 30) at the mid-sagittal plane of a dummy seated in any outboard designated seating position. Target RB1 is located on the roll-bar and in Plane 30 at the location closest to either CG-F2 or CG-R, as appropriate, for the same dummy.

(b) Target RB2. If a seat belt anchorage is located on the roll-bar, Target RB2 is any point on the anchorage.

S10.12 Stiffener targets.

(a) Target ST1. Locate a transverse vertical plane (Plane 31) containing either CG-F2 or CG-R, as appropriate, for any outboard designated seating position. Target ST1 is located on the stiffener and in Plane 31 at the location closest to either CG-F2 or CG-R, as appropriate.

(b) Target ST2. If a seat belt anchorage is located on the stiffener, Target ST2 is any point on the anchorage.

S10.13 Brace target (target BT) Target BT is any point on the width of the brace as viewed laterally from inside the passenger compartment.

S10.14 Door frame targets.

(a) Target DF 1. Locate the point (Point 21) on the vehicle interior at the intersection of the horizontal plane passing through the highest point of the forward door opening and a transverse vertical plane (Plane 32) tangent to the rearmost edge of the forward door, as viewed laterally with the adjacent door open. Locate the point (Point 22) at the intersection of the interior roof surface, Plane 32, and the plane, described in S8.15(h), defining the nearest edge of the upper roof. The door frame reference point (Point DFR) is the point located at the middle of the line from Point 21 to Point 22 in Plane 32, measured along the vehicle interior surface. Target DF1 is located at Point DFR.

(b) Target DF2. If a seat belt anchorage is located on the door frame, Target DF2 is located at any point on the anchorage.

(c) Target DF3. Locate a horizontal plane (Plane 33) which intersects Point DFR. Locate a horizontal plane (Plane 34) that passes through the lowest point of the adjacent daylight opening forward of the door frame. Locate a horizontal plane (Plane 35) half-way between Plane 33 and Plane 34. Target DF3 is the point located in Plane 35 and on the interior surface of the door frame, which is closest to CG-F2 for the nearest seating position.

(d) Target DF4. Locate a horizontal plane (Plane 36) half-way between Plane 34 and Plane 35. Target DF4 is the point located in Plane 36 and on the interior surface of the door frame that is closest to CG-R for the nearest seating position.

S10.15 Other door frame targets.

(a) Target OD1.

(a)(1) Except as provided in S10.15(a)(2), target OD1 is located in accordance with this paragraph. Locate the point (Point 23) on the vehicle interior, at the intersection of the horizontal plane through the highest point of the highest adjacent door opening or daylight opening (if there is no adjacent door opening) and the center line of the width of the other door frame, as viewed laterally with the doors in the closed position. Locate a transverse vertical plane (Plane 37) passing through Point 23. Locate the point (Point 24) at the intersection of the interior roof surface, Plane 37 and the plane, described in S8.15(h), defining the nearest edge of the upper roof. The other door frame reference point (Point ODR) is the point located at the middle of the line between Point 23 and Point 24 in Plane 37, measured along the vehicle interior surface. Target OD1 is located at Point ODR.

(a)(2) If a seat belt anchorage is located on the door frame, Target OD1 is any point on the anchorage.

(b) Target OD2. Locate the horizontal plane (Plane 38) intersecting Point ODR. Locate a horizontal plane (Plane 39) passing through the lowest point of the daylight opening forward of the door frame. Locate a horizontal plane (Plane 40) half-way between Plane 38 and Plane 39. Target OD2 is the point located on the interior surface of the door frame at the intersection of Plane 40 and the center line of the width of the door frames, as viewed laterally, with the doors in the closed position.

S10.16 Seat belt mounting structure targets.

(a) Target SB1. Target SB1 is located at any point on the seat belt anchorage mounted on the seat belt mounting structure.

(b) Target SB2. Locate a horizontal plane (Plane 41), containing either CG-F2 or CG-R, as appropriate, for any outboard designated seating position whose seating reference point, SgRP, is forward of and closest to, the vertical center line of the width of the seat belt mounting structure as viewed laterally. Target SB2 is located on the seat belt mounting structure and in Plane 41 at the location closest to either CG-F2 or CG-R, as appropriate.

(c) Target SB3. Locate a horizontal plane (Plane 42), containing CG-R for any outboard designated seating position rearward of the forward most designated seating position or positions whose seating reference point, SgRP, is rearward of and closest to, the vertical center line of the width of the seat belt mounting structure, as viewed laterally. Locate a horizontal plane (Plane 43) 200 mm below Plane 42. Target SB3 is located on the seat belt mounting structure and in Plane 43 at the location closest to CG-R, as appropriate.

Figures and Table to §571.201

FIGURE 1 - ORTHOGONAL REFERENCE SYSTEM

FIGURE 2 - VERTICAL AND HORIZONTAL APPROACH ANGLE PLANE

TABLE 1.—APPROACH ANGLE LIMITS
[In degrees]

Target component angle	Horizontal angle	Vertical
Front Header	180	0-50
Rear Header	0 or 360	0-50
Left Side Rail	270	0-50
Right Side Rail	90	0-50
Left Sliding Door Track	270	0-50

Right Sliding Door Track	90	0-50
Left A-Pillar	195-255	-5-50
Right A-Pillar	105-165	-5-50
Left B-Pillar	195-345	-10-50
Right B-Pillar	15-165	-10-50
Left Door Frame	195-345	-10-50
Right Door Frame	15-165	-10-50
Other Left Pillars	270	-10-50
Other Right Pillars	90	-10-50
Other Left Door Frame	270	-10-50
Other Right Door Frame	90	-10-50
Left Rearmost Pillar	270-345	-10-50
Right Rearmost Pillar	15-90	-10-50
Upper Roof	Any	0-50
Overhead Rollbar	0 or 180	0-50
Brace or Stiffener	90 or 270	0-50
Left Seat Belt Mounting Structure	195-345	-10-50
Right Seat Belt Mounting Structure.	15-165	-10-50
Seat Belt Anchorages	Any	0-50

[36 FR 22902, Dec. 2, 1971, as amended at 44 FR 68475, Nov. 29, 1979; 47 FR 52451, Nov. 22, 1982; 56 FR 26039, June 6, 1991; 60 FR 43050 and 43055, Aug. 18, 1995; 62 FR 16725, Apr. 8, 1997; 62 FR 16725, Apr. 8, 1997; 63 FR 28, Jan. 2, 1998; 63 FR 41464, Aug. 4, 1998; 63 FR 45965, Aug. 28, 1998; 64 FR 7140, Feb. 12, 1999; 64 FR 69671, Dec. 14, 1999; 67 FR 79439, Dec. 27, 2002; 68 FR 51711, Aug. 28, 2003; 69 FR 9226, Feb. 27, 2004; 69 FR 70914, Dec. 8, 2004; 70 FR 51669, Aug. 31, 2005; 71 FR 51133, Aug. 29, 2006; 72 FR 50906, Sept. 5, 2007; 72 FR 51956, Sept. 11, 2007]

Appendix C – Federal Motor Vehicle Safety Standards 205, "Glazing Materials"

S1. Scope. This standard specifies requirements for glazing materials for use in motor vehicles and motor vehicle equipment.

S2. Purpose. The purpose of this standard is to reduce injuries resulting from impact to glazing surfaces, to ensure a necessary degree of transparency in motor vehicle windows for driver visibility, and to minimize the possibility of occupants being thrown through the vehicle windows in collisions.

S3. Application and Incorporation by Reference.

S3.1 Application.

(a) This standard applies to passenger cars, multipurpose passenger vehicles, trucks, buses, motorcycles, slide-in campers, pickup covers designed to carry persons while in motion and low speed vehicles, and to glazing materials for use in those vehicles.

(b) For glazing materials manufactured before September 1, 2006, and for motor vehicles, slide-in campers and pickup covers designed to carry persons while in motion, manufactured before November 1, 2006, the manufacturer may, at its option, comply with 49 CFR 571.205(a) of this section.

S3.2 Incorporation by Reference.

(a) "American National Standard for Safety Glazing Materials for Glazing Motor Vehicles and Motor Vehicle Equipment Operating on Land Highways-Safety Standard" ANSI/SAE Z26.1-1996, Approved by American National Standards Institute August 11, 1997 (ANSI/SAE Z26.1-1996) is incorporated by reference in Section 5.1 and is hereby made part of this Standard. The Director of the Federal Register approved the material incorporated by reference in accordance with 5 U.S.C. 552(a) and 1 CFR part 51 (see §571.5 of this part). A copy of ANSI/SAE Z26.1-1996 may be obtained from the Society of Automotive Engineers, Inc., 400 Commonwealth Drive, Warrendale, PA 15096-0007. A copy of ANSI/SAE Z26.1-1996 may be inspected at NHTSA's technical reference library, 400 Seventh Street, SW., Room 5109, Washington, DC or at the Office of the Federal Register, 900 North Capitol Street, NW., Suite 700, Washington, DC.

(b) The Society of Automotive Engineers (SAE) Recommended Practice J673, revised April 1993, “Automotive Safety Glasses” (SAE J673, rev. April 93) is incorporated by reference in Section S5.1, and is hereby made part of this Standard. The Director of the Federal Register approved the material incorporated by reference in accordance with 5 U.S.C. 552(a) and 1 CFR part 51 (see Sec. 571.5 of this part). A copy of SAE J673, rev. April 93 may be obtained from SAE at the Society of Automotive Engineers, Inc., 400 Commonwealth Drive, Warrendale, PA 15096. A copy of SAE J673, rev. April 93 may be inspected at NHTSA's technical reference library, 400 Seventh Street, SW., Room 5109, Washington, DC, or at the Office of the Federal Register, 900 North Capitol Street, NW., Suite 700, Washington, DC.

(c) The Society of Automotive Engineers (SAE) Recommended Practice J100, revised June 1995, “Class ‘A’ Vehicle Glazing Shade Bands” (SAE J100, rev. June 95) is incorporated by reference in Section S5.3, and is hereby made part of this Standard. The Director of the Federal Register approved the material incorporated by reference in accordance with 5 U.S.C. 552(a) and 1 CFR part 51 (see Sec. 571.5 of this part). A copy of SAE J100, rev. June 95 may be obtained from SAE at the Society of Automotive Engineers, Inc., 400 Commonwealth Drive, Warrendale, PA 15096. A copy of SAE J100, rev. 95 may be inspected at NHTSA's technical reference library, 400 Seventh Street, SW., Room 5109, Washington, DC, or at the Office of the Federal Register, 900 North Capitol Street, NW., Suite 700, Washington, DC.

S4. Definitions.

Bullet resistant shield means a shield or barrier that is installed completely inside a motor vehicle behind and separate from glazing materials that independently comply with the requirements of this standard.

Camper means a structure designed to be mounted in the cargo area of a truck, or attached to an incomplete vehicle with motive power, for the purpose of providing shelter for persons.

Glass–plastic glazing material means a laminate of one or more layers of glass and one or more layers of plastic in which a plastic surface of the glazing faces inward when the glazing is installed in a vehicle.

Pickup cover means a camper having a roof and sides but without a floor, designed to be mounted on and removable from the cargo area of a truck by the user.

Prime glazing manufacturer means a manufacturer that fabricates, laminates, or tempers glazing materials.

Slide–in camper means a camper having a roof, floor, and sides, designed to be mounted on and removable from the cargo area of a truck by the user.

S5. Requirements.

S5.1 Glazing materials for use in motor vehicles must conform to ANSI/SAE Z26.1-1996 unless this standard provides otherwise.

S5.1.1 Multipurpose passenger vehicles. Except as otherwise specifically provided by this standard, glazing for use in multipurpose passenger vehicles shall conform to the requirements for glazing for use in trucks as specified in ANSI/SAE Z26.1-1996.

S5.1.2 Aftermarket replacement glazing. Glazing intended for aftermarket replacement is required to meet the requirements of this standard or the requirements of 49 CFR 571.205(a) applicable to the glazing being replaced.

S5.1.3 Location of arrow within "AS" markings. In ANSI/SAE Z26.1- 1996 (August 11, 1997) Section 7. "Marking of Safety Glazing Materials," on page 33, in the right column, in the first complete sentence, the example markings “AS↓1”, “AS↓14” and “AS↑2” are corrected to read “A↓S1”, “A↓S14” and “A↑S2”. Note that the arrow indicating the portion of the material that complies with Test 2 is placed with its base adjacent to a horizontal line.

S5.2 Each of the test specimens described in ANSI/SAE Z26.1-1996 Section 5.7 (fracture test) must meet the fracture test requirements of that section when tested in accordance with the test procedures set forth in that section.

S5.3 Shade bands. Shade band areas for windshields shall comply with the requirements of either S5.3.1 or S5.3.2.

S5.3.1 Shade bands for windshields shall comply with SAE J100 JUNE 1995.

S5.3.2 Except as provided in S5.3.2.1, the lower boundary of shade bands for windshields shall be a plane inclined upwards from the X axis of the vehicle at 7 degrees, passing through point V_1, and parallel to the Y axis. The coordinate system and point V_1 shall be as specified in Annexes 18 and 19 of European Commission for Europe (ECE) Regulation No. 43 Revision 2 – Amendment 1.

S5.3.2.1 In the area 300 mm wide centered on the intersection of the windshield surface and longitudinal vertical median plane of the vehicle, the lower boundary of shade bands for windshields shall be a plane inclined upwards from the X axis of the vehicle at 3 degrees, passing through point V_1, and parallel to the Y axis.

S5.4 Low speed vehicles. Windshields of low speed vehicles must meet the ANSI/SAE Z26.1-1996 specifications for either AS-1 or AS-4 glazing.

S5.5 Item 4A Glazing. Item 4A glazing may be used in all areas in which Item 4 safety glazing may be used, and also for side windows rearward of the "C" pillar. I.e., Item 4A glazing may be used under Item 4A paragraph (b) of ANSI/SAE Z26.1-1996 only in side windows rearward of the "C" pillar.

S6. Certification and marking.

S6.1 A prime glazing material manufacturer must certify, in accordance with 49 U.S.C. 30115, each piece of glazing material to which this standard applies that is designed--

(a) As a component of any specific motor vehicle or camper; or

(b) To be cut into components for use in motor vehicles or items of motor vehicle equipment.

S6.2 A prime glazing manufacturer certifies its glazing by adding to the marks required by section 7 of ANSI/SAE Z26.1-1996, in letters and numerals of the same size, the symbol “DOT” and a manufacturer's code mark that NHTSA assigns to the manufacturer. NHTSA will assign a code mark to a manufacturer after the manufacturer submits a written request to the Office of Vehicle Safety Compliance, National Highway Traffic Safety Administration, 400 Seventh Street, SW., Washington, DC 20590. The request must include the company name, address, and a statement from the manufacturer certifying its status as a prime glazing manufacturer as defined in S4.

S6.3 A manufacturer or distributor who cuts a section of glazing material to which this standard applies, for use in a motor vehicle or camper, must–

(a) Mark that material in accordance with section 7 of ANSI/SAE Z26.1-1996; and

(b) Certify that its product complies with this standard in accordance with 49 U.S.C. 30115.

[37 FR 12239, June 21, 1972, as amended at 37 FR 13097, July 1, 1972; 37 FR 24036, Nov. 11, 1972; 37 FR 24826, Nov. 22, 1972; 42 FR 61466, Dec. 5, 1977; 45 FR 47151, July 14, 1980; 46 FR 43690, Aug. 31, 1981; 48 FR 52065, Nov. 16, 1983; 49 FR 6734, Feb. 23, 1984; 56 FR 12674, Mar. 27, 1991; 56 FR 18531, Apr. 23, 1991; 56 FR 49149, Sept. 27, 1991; 57 FR 1654, Jan. 15, 1992; 57 FR 13656, Apr. 17, 1992; 57 FR 30164, July 8, 1992; 57 FR 58150, Dec. 9, 1992; 60 FR 13646, Mar. 14, 1995; 61 FR 41743, Aug. 12, 1996; 67 FR 79439, Dec. 27, 2002; 68 FR 43971, July 25, 2003; 68 FR 55545, Sept. 26, 2003; 69 FR 51191, Aug. 18, 2004; 70 FR 39965, July 12, 2005; 71 FR 64474, Nov. 2, 2006]

Appendix D – DVS Interoperability Chart

Type 1a	**Type 1 b**	**Type 2**
6.2.a	**6.2.b**	**6.2.c**
7.1.1	**7.1.2**	**Vendor Option to Provide Proprietary Viewer**

Appendix E – Acknowledgements: "Digital Video Systems for Public Safety: Developing Minimum Performance Specifications" Executive Committee

Advisory Panel Executive Committee Co-Chairs:

Captain Thomas Didone
Montgomery (MD) County Department of Police
Law Enforcement Executive Co-Chair

Mike Burridge
L-3 Communications, Display Systems
Industry Executive Co-Chair

Executive Committee Task Group Chairs:

Herbert L. Blitzer
Executive Director, Institute for Forensic Imaging
Quality Measurement Task Group Chair

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

Raymond Cooke
Principal Architect, IBM Global Services Technology
Interoperability Task Group Chair

Gregory A. Dertz
Distinguished Member of the Technical Staff, Motorola, Inc.
Data Security Task Group Chair

Sergeant Scott Galbreath
Delaware State Police
Operational Measurements Task Group Chair

Lieutenant Ronald Castleberry and Captain James D. Wells, Jr.
Florida Highway Patrol
Officer Safety Task Group Chairs

Appendix F – Acknowledgements: Participating Agencies/Organizations

A4S Security, Inc
C Media Solutions Corporation
Cherry Road GT
City of White Plains, New York –Department of Public Safety
Coban Research and Technologies, Inc.
Control Concepts, Inc.
Cruisecam International
Custody Video
Data 911
Decatur Electronics, Inc.
Dedicated Micros
Delaware State Police
Digital Ally, Inc
Drivecam Video Systems
EDO Corporation
Enforcement Technologies International, LLC
Everett, WA Police Department
Farmington, NM Police Department
Federal Bureau of Investigation Academy/TDU
Fleet Safety Equipment
Florida Highway Patrol
Forensic Video Solutions, LLC
FSCAM/ Fleet Safety
Gasser Consulting
IBM Global Services
ICOP Digital, Inc.
Insight Video Net Corporation
Institute for Forensic Imaging
Integrian, Inc.
International Police Technologies, Inc.
JFK Forensics
Kustom Signals, Inc.
L-3 Communications Mobile Vision, Inc.
L-3 Display Systems
Los Angeles County Sheriff's Department
Los Angeles Police Department
McCoy's Law Line, Inc.
Montgomery County, MD Department of Police
MPH Industries
Mobile Police Solutions
Motorola Inc.
National Institute of Justice

National Institute of Standards and Technology
National Law Enforcement and Corrections Technology Center- West (NLECTC)
National Transportation Safety Board
New Albany, OH Police Department
New York Police Department
NL Technology
Noblis, Inc.
Northland Security Products-MobileEye
NTIA
On Patrol Video International
Panasonic AVC Networks Company
Panasonic Computer Solutions Company
Prince Georges County, MD Police Department
Raytheon JPS Communications
Security Industry Association
Sony Electronics
Stalker Radar and Video, Applied Concepts, Inc.
Tarrant County, TX Criminal District Attorney's Office
The Ashcroft Group, LLC
TranTech, Inc.
Toronto, ON Police Service
Underwriters Laboratories, Inc.
United States Park Police
ViewPointe Solutions, LLC
Verint
Washington State Patrol
WatchGuard Video

Appendix G– IACP Staff Acknowledgements

IACP Research Center Directorate – Digital Video Systems Project Staff:

John C. Grant
Senior Program Manager
Cutting Edge of Technology

Ian Hamilton
Project Coordinator
Cutting Edge of Technology

Past Contributors (IACP)

William Albright
Albert Arena
Wm. Grady Baker
Sara Dziejma
Mike Fergus
Kristy Fowler
Melissa Hays
Victoria Kallini
Darron Mason
Tamika Scott
Tiffany Williams

4. COMPANY BACKGROUND AND REFERENCES

4.1 VENDOR INFORMATION

4.1.1 Vendor must provide a company profile in the table format below.

Question	Response
Company name:	***Digital Ally, Inc.***
Ownership (sole proprietor, partnership, etc.):	***Corporation***
State of incorporation:	***Nevada***
Date of incorporation:	***2004***
# of years in business:	***12***
List of top officers:	***CEO: Stanton Ross, CFO: Tom Heckman***
Location of company headquarters:	***9705 Loiret Blvd, Lenexa, KS, 66219***
Location(s) of the company offices:	***9705 Loiret Blvd, Lenexa, KS, 66219***
Location(s) of the office that will provide the services described in this RFP:	***9705 Loiret Blvd, Lenexa, KS, 66219***
Number of employees locally with the expertise to support the requirements identified in this RFP:	***Approximately 140***
Number of employees nationally with the expertise to support the requirements in this RFP:	***Approximately 180***
Location(s) from which employees will be assigned for this project:	***9705 Loiret Blvd, Lenexa, KS, 66219***

4.1.2 **Please be advised,** pursuant to NRS 80.010, a corporation organized pursuant to the laws of another state must register with the State of Nevada, Secretary of State's Office as a foreign corporation before a contract can be executed between the State of Nevada and the awarded vendor, unless specifically exempted by NRS 80.015. ***Upon award of the contract, Digital Ally will register with the State of Nevada, Secretary of State's Office as a foreign corporation before a contract is executed between the State of Nevada and Digital Ally.***

4.1.3 The selected vendor, prior to doing business in the State of Nevada, must be appropriately licensed by the State of Nevada, Secretary of State's Office pursuant to NRS76. Information regarding the Nevada Business License can be located at http://nvsos.gov.

Question	Response
Nevada Business License Number:	***BL12-00500***
Legal Entity Name:	***Digital Ally, Inc.***

Is "Legal Entity Name" the same name as vendor is doing business as?

Yes	***X***	No	

If "No", provide explanation.

4.1.4 Vendors are cautioned that some services may contain licensing requirement(s). Vendors shall be proactive in verification of these requirements prior to proposal submittal. Proposals that do not contain the requisite licensure may be deemed non-responsive.

4.1.5 Has the vendor ever been engaged under contract by any State of Nevada agency?

Yes		No	***X***

If "Yes", complete the following table for each State agency for whom the work was performed. Table can be duplicated for each contract being identified.

Question	**Response**
Name of State agency:	
State agency contact name:	
Dates when services were performed:	
Type of duties performed:	
Total dollar value of the contract:	

4.1.6 Are you now or have you been within the last two (2) years an employee of the State of Nevada, or any of its agencies, departments, or divisions?

Yes		No	***X***

If "Yes", please explain when the employee is planning to render services, while on annual leave, compensatory time, or on their own time?

If you employ (a) any person who is a current employee of an agency of the State of Nevada, or (b) any person who has been an employee of an agency of the State of Nevada within the past two (2) years, and if such person will be performing or producing the services which you will be contracted to provide under this contract, you must disclose the identity of each such person in your response to this RFP, and specify the services that each person will be expected to perform.

4.1.7 Disclosure of any significant prior or ongoing contract failures, contract breaches, civil or criminal litigation in which the vendor has been alleged to be liable or held liable in a matter involving a contract with the State of Nevada or any other governmental entity. Any pending claim or litigation occurring within the past six (6) years which may adversely affect the vendor's ability to perform or fulfill its obligations if a contract is awarded as a result of this RFP must also be disclosed.

Does any of the above apply to your company?

Yes		No	***X***

If "Yes", please provide the following information. Table can be duplicated for each issue being identified.

Question	Response	
Date of alleged contract failure or breach:		
Parties involved:		
Description of the contract failure, contract breach, or litigation, including the products or services involved:		
Amount in controversy:		
Resolution or current status of the dispute:		
If the matter has resulted in a court case:	Court	Case Number
Status of the litigation:		

4.1.8 Vendors must review the insurance requirements specified in ***Attachment E, Insurance Schedule for RFP 3273.*** Does your organization currently have or will your organization be able to provide the insurance requirements as specified in ***Attachment E.***

Yes	***X***	No	

Any exceptions and/or assumptions to the insurance requirements ***must*** be identified on ***Attachment B, Technical Proposal Certification of Compliance with Terms and Conditions of RFP.*** Exceptions and/or assumptions will be taken into consideration as part of the evaluation process; however, vendors must be specific. If vendors do not specify any exceptions and/or assumptions at time of proposal submission, the State will not consider any additional exceptions and/or assumptions during negotiations.

Upon contract award, the successful vendor ***must*** provide the Certificate of Insurance identifying the coverages as specified in ***Attachment E, Insurance Schedule for RFP 3273.***

4.1.9 Company background/history and why vendor is qualified to provide the services described in this RFP. Limit response to no more than five (5) pages.

The State of Nevada requires a comprehensive Body Worn Camera product and services with future In-Car video integration. Digital Ally, Inc. is pleased to provide this bid response for the Body Worn Cameras project for the State of Nevada. Digital Ally proposes to supply the State of Nevada with 477 FirstVu HD Body Cameras, cloud storage, and digital management system then 477 DVM-800 In-Car Video systems on the State's requested timeline. We can meet and exceed the State of Nevada's expectations by not only providing the required hardware and evidence management system, but also by providing excellent customer service, support, and the scalability required to make such a solution work efficiently.

Established in 2004, Digital Ally, Inc. adopted a "think tank" approach, utilizing multi-disciplined engineers, sales and support staff, as well as collaborating with cutting-edge firms to design innovative products. Digital Ally, Inc.'s products have been developed for applications in industries such as law enforcement, fire, EMS, and commercial fleet management.

Digital Ally, Inc. revolutionized mobile video by introducing a complete video system integrated into a rear-view mirror that provides a more efficient use of space in vehicles, as well as providing a user-friendly system that can be positioned so it is not distracting to users. All of the video systems designed by Digital Ally, Inc. offer many important benefits such as being fully-automatic, capturing irrefutable evidence, and total solution for easy management, review, and archiving of recorded evidence.

We presently have approximately 140 employees, plus approximately 20 Sales Representatives in the USA, and an additional 40 Sub-Agents. We have 40 international distributors representing us throughout the world. Digital Ally has approximately 50,000 units deployed in all 50 states across the US, as well as 90 foreign countries. In addition, we have been awarded several contracts with purchasing cooperatives to include GSA, Purchasing Cooperative of America (PCA), MIDEAL, PA COSTARS, TX-DIR, NPP Gov, and more.

Since the introduction of the DVM series of In-Car Video Systems, we have expanded our product offerings to include the FirstVu HD line of body-worn cameras, the VuLink body-camera auto activation unit, VuVault.com evidence management and cloud storage solution, and the MicroVu in-car camera solution. New products are always in the pipeline to enable our customers to stay up to date with the latest in technology.

Digital Ally is determined to provide said state digital video systems and Law Enforcement products that are simple to operate, will enhance officer safety, reduce liability, be trouble free, long lasting and cost-effective. With new, forward-looking products being designed constantly, Digital Ally, Inc. strives to offer customers the solutions they need to capture the truth in situations where it matters the most.

4.1.10 Length of time vendor has been providing services described in this RFP to the public and/or private sector. Please provide a brief description.
Digital Ally has been in business since 2004. Our company was started and is devoted to developing the latest technology for the law enforcement, security and Homeland Security markets. In 2006, we began shipping product.

4.2 SUBCONTRACTOR INFORMATION

4.2.1 Does this proposal include the use of subcontractors?

Yes		No	***X***

If "Yes", vendor must:

4.2.1.1 Identify specific subcontractors and the specific requirements of this RFP for which each proposed subcontractor will perform services.

4.2.1.2 If any tasks are to be completed by subcontractor(s), vendors must:
A. Describe the relevant contractual arrangements;
B. Describe how the work of any subcontractor(s) will be supervised, channels of communication will be maintained and compliance with contract terms assured; and
C. Describe your previous experience with subcontractor(s).

4.2.1.3 Vendors must describe the methodology, processes and tools utilized for:
A. Selecting and qualifying appropriate subcontractors for the project/contract;
B. Ensuring subcontractor compliance with the overall performance objectives for the project;
C. Ensuring that subcontractor deliverables meet the quality objectives of the project/contract; and
D. Providing proof of payment to any subcontractor(s) used for this project/contract, if requested by the State. Proposal should include a plan by which, and the State's request, the State will be notified of such payments.

4.2.1.4 Provide the same information for any proposed subcontractors as requested in ***Section 4.1, Vendor Information.***

4.2.1.5 Business references as specified in ***Section 4.3, Business References*** must be provided for any proposed subcontractors.

4.2.1.6 Vendor shall not allow any subcontractor to commence work until all insurance required of the subcontractor is provided to the vendor.

4.2.1.7 Vendor must notify the using agency of the intended use of any subcontractors not identified within their original proposal and provide the information originally requested in the RFP in ***Section 4.2, Subcontractor Information.*** The vendor must receive agency approval prior to subcontractor commencing work.

4.3 BUSINESS REFERENCES

4.3.1 Vendor must provide at least three (3) law enforcement agencies within the last two (2) years as references, for which it is verifiable that the vendor has deployed at least 100 active BWS's that have been in service for at least six (6) months for each of those references.

4.3.2 Vendors must provide the following information for ***every*** business reference provided by the vendor and/or subcontractor:

The "Company Name" must be the name of the proposing vendor or the vendor's proposed subcontractor.

Reference #:	***Reference 1***		
Company Name:	***Evansville Police Department Evansville, Indiana***		
Identify role company will have for this RFP project (Check appropriate role below):			
X	***VENDOR***		***SUBCONTRACTOR***
Project Name:			
Primary Contact Information			
Name:		***Matt Knight***	
Street Address:		***15 NW M. L. King Blvd.***	
City, State, Zip:		***Evansville, IN, 47708***	
Phone, including area code:		***(812)436-7974***	
Facsimile, including area code:		***(812)435-6175***	
Email address:		***mknight@evansvillepolice.com***	
Alternate Contact Information			
Name:		***Vernon Lutz***	
Street Address:		***15 NW M. L. King Blvd.***	
City, State, Zip:		***Evansville, IN, 47708***	
Phone, including area code:		***(812)436-7971***	
Facsimile, including area code:		***(812)435-6175***	
Email address:		***vlutz@evansvillepolice.com***	
Project Information			
Brief description of the project/contract and description of services performed, including technical environment (i.e., software applications, data communications, etc.) if applicable:		***Digital Ally provided Evansville Police Department with 235 FirstVu HD, with a local sever solution, and VuVault local video management solution.***	
Original Project/Contract Start Date:		***2011***	
Original Project/Contract End Date:		***Current Contract***	
Original Project/Contract Value:		***Disclosure left to reference's discursion.***	
Final Project/Contract Date:		***Current Contract***	
Was project/contract completed in time originally allotted, and if not, why not?		***Yes***	
Was project/contract completed within or under the original budget/cost proposal, and if not, why?		***Yes***	

Reference #:	***Reference 2***		
Company Name:	***SEPTA Transit Police***		
Identify role company will have for this RFP project (Check appropriate role below):			
X	***VENDOR***		***SUBCONTRACTOR***
Project Name:			
Primary Contact Information			
Name:		***Tim Catto***	
Street Address:		***1234 Market St, 4th Floor***	
City, State, Zip:		***Philadelphia, PA, 19107***	
Phone, including area code:		***(215)580-7860***	

Facsimile, including area code:	-
Email address:	tcatto@septa.org
Alternate Contact Information	
Name:	*Tim Catto*
Street Address:	*1234 Market St, 4th Floor*
City, State, Zip:	*Philadelphia, PA, 19107*
Phone, including area code:	*(215)580-7860*
Facsimile, including area code:	-
Email address:	tcatto@septa.org
Project Information	
Brief description of the project/contract and description of services performed, including technical environment (i.e., software applications, data communications, etc.) if applicable:	*Digital Ally has provided SEPTA Transit police with 300 FirstVu HD, cloud storage, and VuVault.com video management system.*
Original Project/Contract Start Date:	*2014*
Original Project/Contract End Date:	*Current contract*
Original Project/Contract Value:	*Disclosure left to reference's discursion.*
Final Project/Contract Date:	*Current contract*
Was project/contract completed in time originally allotted, and if not, why not?	*Yes*
Was project/contract completed within or under the original budget/cost proposal, and if not, why?	*Yes*

Reference #:	*Reference 3*		
Company Name:	*Richmond California Police Department*		
Identify role company will have for this RFP project (Check appropriate role below):			
X	*VENDOR*		*SUBCONTRACTOR*
Project Name:			
Primary Contact Information			
Name:	*Eric Tam*		
Street Address:	*1701 Regatta Blvd*		
City, State, Zip:	*Richmond, CA, 94804*		
Phone, including area code:	*(510)621-1819*		
Facsimile, including area code:	*(510)620-6880*		
Email address:	etam@richmondpd.net		
Alternate Contact Information			
Name:	*Eric Tam*		
Street Address:	*1701 Regatta Blvd*		
City, State, Zip:	*Richmond, CA, 94804*		
Phone, including area code:	*(510)621-1819*		
Facsimile, including area code:	*(510)620-6880*		
Email address:	etam@richmondpd.net		
Project Information			

Brief description of the project/contract and description of services performed, including technical environment (i.e., software applications, data communications, etc.) if applicable:	***Digital Ally provided Richmond Police Department with 122 FirstVu HD, cloud storage, and VuVault.com video management solution.***
Original Project/Contract Start Date:	***2014***
Original Project/Contract End Date:	***Current Contract***
Original Project/Contract Value:	***Disclosure left to reference's discursion.***
Final Project/Contract Date:	***Current Contract***
Was project/contract completed in time originally allotted, and if not, why not?	***Yes***
Was project/contract completed within or under the original budget/cost proposal, and if not, why?	***Yes***

4.3.3 Vendors must also submit ***Attachment F, Reference Questionnaire*** to the business references that are identified in ***Section 4.3.2.***

Digital Ally has submitted Reference Questionnaires to the 3 above business references.

4.3.4 The company identified as the business references must submit the Reference Questionnaire directly to the Purchasing Division.

4.3.5 It is the vendor's responsibility to ensure that completed forms are received by the Purchasing Division on or before the deadline as specified in ***Section 8, RFP Timeline*** for inclusion in the evaluation process. Reference Questionnaires not received, or not completed may adversely affect the vendor's score in the evaluation process.

4.3.6 The State reserves the right to contact and verify any and all references listed regarding the quality and degree of satisfaction for such performance.

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Digital Ally, Inc.***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***X***	**Subcontractor:**	

The following information requested pertains to the individual being proposed for this project.

Name:	***Jacob McKenzie***	**Key Personnel: (Yes/No)**	***Yes***
Individual's Title:	***Regional Sales Manager***		
# of Years in Classification:	***1***	**# of Years with Firm:**	***1***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

I have worked for Digital Ally as a Regional Sales Manager for 15 months, and have covered the territories of Northern California and Nevada, as well as Oklahoma and North Texas.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

June 2015 – Present
Digital Ally, Inc.
9705 Loiret Blvd, Lenexa, Ks, 66219
Regional Sales Manager

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Hutchinson Community College
Hutchinson, Ks
Associate in Science
December 15, 2008

Friends University
Wichita, Ks
Bachelor of Science in Business Administration with a Minor in Marketing
May 8, 2015

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

N/A

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

Greg Dyer, *VP of National Sales | Law Enforcement*
Digital Ally, Inc.
1-800-440-4947
Greg.dyer@digitalallyinc.com

Mark Gordon, *Director of Technical Services*
Digital Ally, Inc.
1-800-440-4947
Greg.dyer@digitalallyinc.com

Larry Dado, *Customer Service Manager*
Digital Ally, Inc.
1-800-440-4947
Greg.dyer@digitalallyinc.com

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Digital Ally, Inc.***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***X***	**Subcontractor:**	

The following information requested pertains to the individual being proposed for this project.

Name:	***Brian Hill***	**Key Personnel: (Yes/No)**	***Yes***
Individual's Title:	***Regional Sales Manager***		
# of Years in Classification:	***4***	**# of Years with Firm:**	***6***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

I have worked for Digital Ally, Inc. for six years. For the last 4 years I have been the General Sales Manager responsible for the success of the sales team. I work closely with the Regional Sales Managers to increase their sales from setting sales goals, to training.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

2010 – Present
Digital Ally, Inc.
9705 Loiret Blvd, Lenexa, Ks, 66219
General Sales Manager

2006-2010
Ka-Comm, Inc.
1201 W Old 56 Hwy, Olathe, KS, 66061
Sales Representative

2003-2006
Conrad Fire Equipment
887 N Jan Mar Ct., Olathe, KS, 66061
Inside Sales/Customer Service

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

University of Arizona and Pima Community College
Tucson, AZ
Business and Accounting

Learning International
Schaumburg, IL
Professional Selling Skills

University of North Florida, Institute of Police Technology and Management
Jacksonville, FL
Police Radar and Traffic Laser Instructor/Operator

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

N/A

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

Greg Dyer, *VP of National Sales | Law Enforcement*
Digital Ally, Inc.
1-800-440-4947
Greg.dyer@digitalallyinc.com

Mark Gordon, *Director of Technical Services*
Digital Ally, Inc.
1-800-440-4947
Greg.dyer@digitalallyinc.com

Larry Dado, *Customer Service Manager*
Digital Ally, Inc.
1-800-440-4947
Greg.dyer@digitalallyinc.com

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Digital Ally, Inc.***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	X	**Subcontractor:**	

The following information requested pertains to the individual being proposed for this project.

Name:	***Trevor Frizzell***	**Key Personnel: (Yes/No)**	Yes
Individual's Title:	***Sales Support Technician***		
# of Years in Classification:	***1.5***	**# of Years with Firm:**	***3+***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

Midwest Pool Management
Life Guard & Swim Lesson Instructor, March 2011 – September 2011
O'Reilly Automotive
Parts Specialist & Key Holder, October 2011 – August 2012
Hill Engineering and Manufacturing Co.
Assembly & Refinishing Technician, May 2013
Digital Ally Inc.
Product & Sales Support Technician, June 2013 – Current

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

Digital Ally Inc. Lenexa, KS

Product Support Technician, June 2013 – January 2015

- Interact with customers and provide outstanding customer service
- Troubleshoot and assist with Digital Ally software and hardware
- Software implementation and scheduling
- Handle online account request and access

Sales Support Technician, January 2015 – Current

- Handle deployments for Test & Evaluation equipment as well as new clients
- Develop and adapt the software and hardware solutions for customers' environments
- Design and tailor server and/or storage offerings for customers' environments
- Handle customer accounts and access to Digital Ally's online cloud website
- Advanced troubleshooting of hardware and software (including MS-SQL)

Con't on next page…

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Career & Technology Center @ Fort Osage Independence, MO

Courses: *Computer Support Specialist I*

- *Software and Hardware troubleshooting and installation*
- *Security and customer service/support*
- *Basic networking*

Automotive Technology II

- *Troubleshooting of all automotive systems*
- *Industry Tools and Safety*
- *Advanced Electrical*

GPA: 4.0

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

No relevant certifications at this time.

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

Larry Dado, *Customer Service Manager*
Digital Ally Inc.
1-800-440-4947
larry.dado@digitalallyinc.com

Mark Gordon, *Director of Technical Services*
Digital Ally Inc.
1-800-440-4947
mark.gordon@digitalallyinc.com

Greg Johnson, *Technical Services Manager Commercial Division*
Digital Ally Inc.
1-800-440-4947
greg.johnson@digitalallyinc.com

Other Informational Material

RFP Page #	Section	Specification
21	3.11.3.27	The vendor must offer a multi-dock station capable of uploading digital evidence from multiple cameras simultaneously and have the capability to upload video via Wi-Fi and/or cellular LTE connectivity. If via cellular, product should be compatible with Fenny Wireless Skyus X modem.

FirstVu HD™ Docking and Charging Station

The FirstVu HD docking station provides automated, simultaneous uploading and charging for up to 12 FirstVu HD ™ devices and 12 external batteries. It is desk or wall mountable with included hardware. Simply slide your FirstVu HD ™ into the dock and walk away. Status LED's will inform you of the upload process and battery charging process for each attached device.

The docking station provides fast, secure transfers over gigabit wired connection to your VuVault server. Within minutes, videos can be viewed on any VuVault enabled computer within your network.

RFP Page #	Section	Specification
22	3.11.3.37	Describe device wireless activation features (e.g. device is automatically activated with the activation of patrol vehicle's light bar), if applicable.

VuLink™

The VuLink™ is the first patented product on the market that can link multiple body cameras, in-car video systems, or activate off of triggers with a body camera. With the FirstVu HD Body-Worn Camera and our patented VuLink™ an officer can simultaneously start his or her FirstVu HD & their In-Car Video system, or simultaneously activate his body camera with the blue light, siren, microphone, etc. The pairing of these two devices, a first for the Law Enforcement industry, has the potential to greatly assist an officer in a time of stress by eliminating the need to manually start their body-worn camera. In VuVault, our back office software, both recordings can be linked together into the same incident to streamline the review and reporting process.