

AGREEMENT FOR BODY WORN CAMERA SYSTEM

THIS AGREEMENT is made and entered into this ____ day of _____, 2016, by and between the CITY OF NORMAN, OKLAHOMA, a municipal corporation (hereinafter referred to as City) and ENFORCEMENT VIDEO, LLC., dba WATCHGUARD VIDEO, a corporation incorporated in the State of Texas (hereinafter referred to as Service Provider).

WITNESSETH

WHEREAS, City issued a Request for Proposals, RFP #1516-45 (the RFP) dated January 22, 2016; and

WHEREAS, Service Provider responded to the RFP and City has found Service Provider's response to be the most advantageous to the City's interests; and

WHEREAS, the RFP dated January 22, 2016, VISTA No-Fault Extended Hardware Warranty, Evidence Library Software Maintenance Plan and Evidence Library End User License Agreement shall be incorporated and be made a part of this Agreement; and

NOW, THEREFORE, for and in consideration of the mutual agreements and covenants herein contained, the parties to this Agreement have agreed as follows.

- 1. Term.** The Agreement shall commence upon the date of this Agreement and shall expire at the two (2) year anniversary of the signing of this Agreement, unless earlier terminated pursuant to Section 12. In no event will the term of this Agreement extend beyond two (2) years from the date of this Agreement unless extended by the parties by mutual written agreement.
- 2. Scope of Work.** Service Provider will perform certain services and provide deliverables for City as described in the Statement of Work attached hereto as Schedule 1 (the "Initial Services"). During the term of this Agreement, City may request Service Provider to perform additional services which shall be outlined in an additional description of services acknowledged by both parties as set forth in Paragraph 3. Such additional Statement(s) of Work (the "Additional Services") shall be subject to the terms and conditions of this Agreement, in addition to any additional terms and conditions set forth in such Statement(s) of Work (collectively, "this Agreement".) The Initial Services and Additional Services, if any, shall be referred to collectively in this Agreement as the "Services". All Schedules and Exhibits attached hereto are hereby incorporated by this reference.
- 3. Notice.** Any notice request or other communication to either party by the other concerning the terms and conditions of this Agreement shall be in writing and shall be deemed given when actually received by the addressee, having been hand delivered or sent postage prepaid, by certified or registered United States mail, return receipt requested, addressed as follows:

If to City: City of Norman
Major Kevin Foster
201 W. Gray
Norman, OK 73069

If to Service Provider: Enforcement Video, LLC, dba WatchGuard Video

415 Century Parkway
Allen, Texas 75013

4. City Provided Services and Equipment. City may choose to perform certain tasks or provide equipment needed to complete the agreed upon Scope of Work. These services shall be described in the Statement of Work attached hereto as Schedule 1 (the "Initial Services") and detailed in Appendix A to Schedule 1. City acknowledges that these tasks or equipment are required and the City's failure to perform or deliver these tasks may result in additional costs and or delays.

5. Fees and Payment Schedule. City will pay Service Provider those fees and expenses included in the Solution Cost Breakdown, if any, in the amount and on the terms and conditions described in Schedule 1 for the performance of the Initial Services. In the event the parties agree to any Additional Services, the fee arrangement for the Additional Services shall be outlined in the applicable Statement of Work descriptions if different than the Initial Services.

WatchGuard Video will demonstrate to City, through testing and demonstrations, that the 4RE and VISTA WiFi solution, and all its related components and software, are fully functional and representative of the products and services represented by WatchGuard Video. WatchGuard Video represents that it has the skills to perform the services required, and will invoice City according to the attached Solution Cost Breakdown dated November 21, 2016.

City will pay Service Provider within thirty (30) days upon receipt, review and approval of Service Provider's invoice, detailing the Services rendered, time spent and fee. Project invoices will be broken into two parts. Invoices for hardware will be submitted to City after the items are delivered. Invoices for services will be submitted upon completion of the services. Good faith billing disputes shall not justify non-performance of any obligations under the Agreement.

6. Manner of Performance/Warranties.

(a) Service Provider represents and warrants that it and Service Provider's employees and authorized subcontractors performing Services hereunder (i) have the requisite expertise, ability and legal right to render the Services and will perform the Services in an efficient and timely manner; (ii) will abide by all laws, rules and regulations that apply to the performance of the Services, including applicable requirements regarding equal employment opportunity and (iii) its performance of the Services will not violate or in any way infringe any patent, trademark, copyright or other proprietary interest of any third party.

(b) Service Provider shall maintain accurate and complete records specifically relating to the Services in accordance with generally accepted accounting principles and industry practices and retain such records for a period of one (1) year following the completion of the Services. City may audit such records during normal business hours upon prior notice to Service Provider.

7. **Confidentiality.** In the course of performing the Services, it is anticipated that Service Provider will learn of information that City regards as confidential or proprietary, including but not limited to, the nature of services, evidence and data relating to evidence, personally identifiable information, pricing, costs, know-how, strategies, programs, processes, and practices and confidential and proprietary information City receives from third parties (collectively, "Confidential Information"). WatchGuard shall hold such Confidential Information in strictest confidence and shall exercise at least the same degree of care as it uses with its own most valuable information (but in no event less than reasonable care) to safeguard the confidentiality of the Confidential Information; and except as provided in this Agreement, the Confidential Information shall not be used, duplicated or in any way disclosed to others in whole or in part without the prior express written permission of City.

8. **Independent Contractor.** Service Provider is an independent contractor, not an employee or agent of City. Nothing in this Agreement shall render Service Provider, or any of its employees, subcontractors or agents, an employee, subcontractor or agent of City, nor authorize or empower Service Provider or its employees, subcontractors or agents to speak for, represent or obligate City in any way. Service Provider assumes any and all liabilities regarding Section 1706 of the Tax Reform Act of 1986 and Section 414(n) of the Internal Revenue Code of 1986, as amended.

9. **Indemnification.**

(a) Service Provider shall indemnify and hold harmless City, and its controlling persons, directors, officers, employees, agents and customers and those of its affiliates (collectively, "City") from and against any and all losses, expenses, claims, actions, lawsuits and judgments thereon (including reasonable attorneys' fees and costs of litigation) ("Claims"), arising out of or in connection with any act or omission by Service Provider, its employees or subcontractors in the performance of any services provided under the terms of this Agreement, including without limitation any claim that any of the Services infringed a patent, copyright, trademark or other proprietary interest of any third party, except to the extent any Claim results from any acts of negligence or willful misconduct by City.

(b) City shall indemnify and hold harmless Service Provider, and its controlling persons, directors, officers, employees, agents and its affiliates (collectively, "Service Provider") from and against any and all losses, expenses, claims, actions, lawsuits and judgments thereon (including reasonable attorneys' fees and costs of litigation) ("Claims"), arising out of or in connection with any act or omission by City, its employees or subcontractors in the performance of any terms of this Agreement, including without limitation any Claim that any of the Services infringed a patent, copyright, trademark or other proprietary interest of any third party, except to the extent any claim results from any acts of negligence or willful misconduct by Service Provider.

(c) Each party shall promptly notify the other of any claims that may be presented to it by any person or entity as set forth in Paragraph 3. No settlement which prevents City from continuing to use the Services or Work Product shall be made without City's prior written consent. In all events, City shall have the right to participate in the defense of any suit or proceeding through counsel of its own.

10. Insurance. Service Provider shall procure and maintain in full force and effect during the period that this Agreement is in effect with an insurance company a standard General Liability insurance policy including errors and omissions protecting against any loss, liability or expense due to bodily injury, death or property damage arising out of this Agreement or Services delivered hereunder, to the extent such loss, liability or expense is not due to the negligence of City. Such policy shall have a combined single limit of a minimum of One Million Dollars (\$1,000,000.00). Contractor shall provide such evidence of insurance to City upon request.

11. Remedies. Service Provider will promptly re-perform any services not performed in accordance with the representations and warranties set forth in this Agreement at no additional expense to City to correct any non-conformance to City's reasonable satisfaction. If Service Provider is unable within a reasonable time to comply with the foregoing obligations, Service Provider will refund to City the lesser of (a) the amount paid for the non-conforming Services or (b) the last amount paid for the last invoice submitted to City. The remedies set forth in this paragraph are non-exclusive.

12. Termination.

(a) City may terminate this Agreement by giving Service Provider written notice of termination if Service Provider: (i) breaches any of its obligations, representations or warranties hereunder; or (ii) is placed on the List of Excluded Individuals/Entities or is banned from Government contracts by the General Services Administration.

(b) If City determines that it no longer requires the services of Service Provider, it may terminate this Agreement by giving Service Provider fifteen (15) days written notice and agree to pay reasonable project ramp down fees not to exceed the total invoiced billings over the last seven (7) calendar days prior to termination notice.

(c) In the event this Agreement or any Schedule is terminated by City without cause prior to expiration of the term of this Agreement, or as set forth in any Schedule, Service Provider shall (i) immediately stop all work and upon City's request, if applicable, transfer the project as expeditiously as possible; and (ii) not undertake further work, incur additional expenses, or enter into further commitments. Service Provider shall be entitled to all undisputed payments due and owing under this Agreement at the time of any termination notice, for (i) work completed and accepted by City, (ii) work in progress up to the provisions in section 10b, and (iii) non-cancelable commitments with supporting documentation.

13. General.

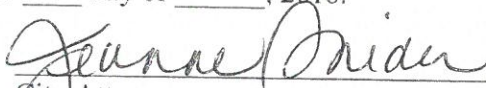
- (a) In the event of the actual or threatened breach of any of the terms of this Agreement, City will have the right to specific performance and injunctive relief. The rights granted by this paragraph are in addition to all other remedies and rights available at law or in equity.
- (b) No assignment by Service Provider of this Agreement or any sums due under it will be binding on City without City's prior written consent.
- (c) This Agreement shall be governed by and construed according with the laws of the State of Oklahoma.
- (d) None of the terms of this Agreement shall be amended or changed, except in writing signed by an authorized representative of each party, or as amended as set forth in Paragraph 3 from both parties.
- (e) Unless otherwise provided with a list of names of authorized representatives, a representative from either party engaging in an email chain, regarding the Services covered under this Agreement while using an official email address from their respected Party's email domain, is representing themselves as having the authority to make the claims, responses, or requests will be considered an authorized representative.
- (f) This Agreement, including all Schedules, Exhibits and any description of Additional Services signed/acknowledged by both parties, contain the entire agreement between the parties relating to the Services and supersede all prior oral or written agreements and understandings between the parties.
- (g) No omission or delay by either party to this Agreement at any time to enforce any right or remedy reserved to it, or to require performance of any of the terms of this Agreement, shall be a waiver of any such right or remedy to which either party is entitled, nor shall it in any way affect the right of either party to enforce such provisions thereafter.
- (h) If any provisions of this Agreement shall be held to be invalid, illegal or unenforceable, the validity of all other provisions hereof shall in no way be affected thereby.
- (i) This Agreement constitutes the entire Agreement between the parties and supersedes all previous agreements and understandings related to the services to be performed under this Agreement.
- (j) This Agreement may be signed in any number of counterparts, each of which shall be deemed an original, but which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the said parties have caused this Agreement to be executed by their duly authorized representatives as of the date first written above.

CITY OF NORMAN, OKLAHOMA
a municipal corporation

By: _____
Lynne Miller, Mayor

Approved as to form and legality this ____ day of _____, 2016.



City Attorney

Approved by the City of Norman this ____ day of _____, 2016.

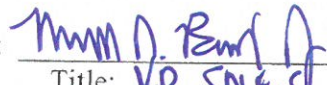
ATTEST:

City Clerk

Lynne Miller, Mayor

**ENFORCEMENT VIDEO, LLC., dba
WATCHGUARD VIDEO, a Texas corporation**

ATTEST:

By: 
Title: V.P. SALES

Address: 415 Century Parkway
Allen, TX 74013
(866) 325-2836

SOLUTION COST BREAKDOWN

SOLUTION COST BREAKDOWN

Item #	Description	Qty.	Unit Price	Extended Price
IN-CAR CAMERA HARDWARE				
1	4RE High Definition In-Car Video System <i>Includes:</i> Zero Sightline HD Front Camera Separate Back Seat Camera Integrated GPS Crash detection DVR with integrated 64GB solid state drive 16GB USB drive 4.3" touch screen remote display control panel Cabin microphone Hi-Fi Wireless microphone kit All mounting hardware and cabling and accessories needed for installation 1-Year warranty on ALL in-car components (See Warranty and Maintenance section)	5	\$4,250.00	\$21,250.00
2	4RE Motorcycle Video System <i>Includes:</i> SD Front Camera Integrated GPS Crash detection DVR with integrated 64GB solid state drive 16GB USB drive 4.3" touch screen remote display control panel Hi-Fi Wireless microphone kit All mounting hardware and cabling and accessories needed for installation 1-Year warranty on ALL in-car components (See Warranty and Maintenance section)	2	\$4,995.00	\$9,990.00
3	4RE IN-CAR 802.11n WIRELESS KIT, 5GHz	7	\$200.00	\$1,400.00
4	HD Zoom Camera Upgrade		\$200.00	\$0.00
5	HD Panoramic Camera Upgrade		\$200.00	\$0.00
BODY CAMERA HARDWARE				
6	VISTA HD Wi-Fi Wearable Camera <i>Includes: Mounting Hardware and One (1) Year warranty on ALL components</i>	75	\$995.00	\$74,625.00
7	VISTA HD, USB Charge and Upload Docking Base		\$95.00	\$0.00
8	4RE, VISTA, Smart PoE Switch <i>Connects the 4RE In-Car Video System to the VISTA HD Wi-Fi wearable camera in the vehicle</i>	7	\$145.00	\$1,015.00
9	Download Station (32-bay) <i>Includes: 48U enclosed rack with 10U locking door, Upload Server, UPS, Network Switch, 8 -8-bay Transfer Stations, and all internal wiring.</i>	1	\$13,500.00	\$13,500.00
10	VISTA HD 8 Bay Ethernet Transfer Station	2	\$1,495.00	\$2,990.00
11	VISTA, VISTA HD, WiFi Charging Radio Base Station	7	\$200.00	\$1,400.00
EVIDENCE MANAGEMENT SOFTWARE				
12	Evidence Library 4 Site License	1	\$1,000.00	\$1,000.00
13	Evidence Library 4 - 4RE Device License	7	\$150.00	\$1,050.00
14	Evidence Library 4 - VISTA/4RE Combo-Discount Device License <i>Includes 1st year of Software Maintenance</i>	7	\$75.00	\$525.00
15	Evidence Library 4 - VISTA Device License <i>Includes 1st year of Software Maintenance</i>	68	\$150.00	\$10,200.00
WARRANTIES AND MAINTENANCE				
16	Warranty, 4RE, In-Car, 1st Year (Months 1-12)	7	--	Included

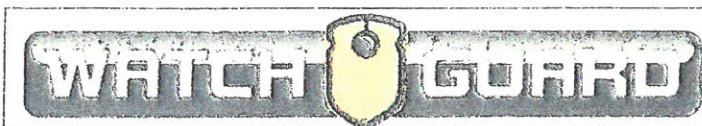
17	Warranty, 4RE, In-Car, 2nd Year (Months 13-24)	7	\$100.00	\$700.00
18	Warranty, 4RE, In-Car, 3rd Year (Months 25-36)	7	\$200.00	\$1,400.00
19	Warranty, 4RE, In-Car, 4th Year (Months 37-48)		\$325.00	\$0.00
20	Warranty, 4RE, In-Car, 5th Year (Months 49-60)		\$450.00	\$0.00
21	Warranty, 4RE, 5 Year Hardware and Software Bundle		\$1,375.00	\$0.00
22	VISTA Warranty, 1st Year (Months 1-12)		--	Included
23	VISTA No Fault Warranty, Years 1-3 <i>Replaces standard warranty and must be purchased up front</i>		\$380.00	\$0.00
24	VISTA No Fault Warranty, Hardware and Software Bundle <i>Replaces standard warranty and must be purchased up front</i>	75	\$580.00	\$43,500.00
25	Evidence Library 4 Software Maintenance, 1st Year <i>Included in Evidence Library Device License. Basic CLOUD-SHARE: 24 Shares per Device</i>	7	--	Included
26	Evidence Library 4 Software Maintenance, 2nd Year <i>Basic CLOUD-SHARE: 24 Shares per Device</i>	7	\$150.00	\$1,050.00
27	Evidence Library 4 Software Maintenance, 3rd Year <i>Basic CLOUD-SHARE: 24 Shares per Device</i>	7	\$150.00	\$1,050.00
28	Evidence Library 4 Software Maintenance, 4th Year <i>Basic CLOUD-SHARE: 24 Shares per Device</i>		\$150.00	\$0.00
29	Evidence Library 4 Software Maintenance, 5th Year <i>Basic CLOUD-SHARE: 24 Shares per Device</i>		\$150.00	\$0.00
IMPLEMENTATION SERVICES				
30	System Configuration - 1st Location <i>Includes: Configuration services per location WG Technical Services on-site installing and configuring Evidence Library, Remote Client, and SQL database Programming all access points and available DVR units End-to-end system testing Training for: hardware end users, back office software users, and system administrators</i>	1	\$2,500.00	\$2,500.00
31	System Configuration - Additional Locations	2	\$1,000.00	\$2,000.00
32	Removal/Install per Vehicle - Optional service that can be provided by WatchGuard or an installer of your choice.	5	\$430.00	\$2,150.00
33	Removal/Install per Motorcycle - Optional service that can be provided by WatchGuard or an installer of your choice.	2	\$475.00	\$950.00
Shipping				\$1,370.00
SOLUTION TOTAL				\$195,615.00

OPTIONAL ITEMS

Item #	Description	Qty.	Unit Price	Extended Price
1	VISTA HD 7 Port USB Hub		\$30.00	
2	VISTA USB Charge and Upload Docking Base		\$95.00	
3	VISTA HD Chest Mount with Straps		\$80.00	
4	VISTA HD Duty Belt Clip		\$25.00	
5	VISTA HD Shirt Clip with Slider		\$40.00	
6	VISTA HD Standard Battery, LI-ION, 3.6V 2700mAH		\$40.00	
7	VISTA HD Extended Battery, LI-ION, 3.6V 4050mAH		\$55.00	
8	Evidence Library 4 - Full Cloud Share (per device, per year)		\$45.00	
9	Evidence Library 4 - Extended Cloud Share (per device, per year)		\$100.00	

SCHEDULE 1

Initial Services Statement of Work



**Schedule 1
Initial Services Statement of Work**

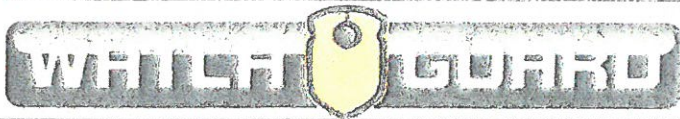
Under the terms and conditions of the Services Agreement dated <Effective Date> by and between Service Provider and Norman PD, the Service Provider shall provide and deliver the Initial Services and Deliverables set forth below.

Provided Services:

WatchGuard Video will provide to Norman PD services resulting in the successful and satisfactory installation and configuration of the WatchGuard Video 4RE High Definition In-Car Video System with Integrated VISTA Wi-Fi and Evidence Library software. Table 1 lists the work required to complete a successful installation. The "Appendix A Reference Number" column represents the line item in which each party is responsible. If an "X" is listed under the "WGV" column then WatchGuard Video is responsible for that particular task. If an "X" is listed under the "Agency" column, then Norman PD is responsible for that particular task. Detail descriptions of each major section (indicated by Bold Text) are included in Appendix A which is incorporated by reference.

Table 1. Work Breakdown Structure

Appendix A Reference Number	WGV	Agency	Short Description (See Appendix A for details on each item)
SVR-01		X	Installation of server in Equipment Rack
SVR-02		X	Provide a suitable Rack
SVR-03		X	Mounting or Racking the Server
SVR-04		X	Connecting the server (Power (connector), KVM, Network Cabling and switches, JBOD, UPS)
SVR-05		X	Provide a physical or Virtual Server that meets the specified Server Requirements
SVR-06		X	Installation and configuration of Windows Operating System and disk storage systems
SVR-07		X	Provide Operating System License
SVR-08		X	Install and configure Operating System (includes current patches)
SVR-09		X	Setup and perform backups
SVR-10		X	Setup recommended disk configuration
SVR-11		X	Install and configure for remote access
SQL-01		X	Installation of Microsoft SQL Server
SQL-02		X	Provide SQL Server Licenses
SQL-03		X	Install and configure SQL Server
SQL-04		X	SQL Backup and Maintenance plan
SQL-05	N/A	N/A	Setup SQL Instance (if shared database server).
EL-01	X		Installing and configuration of Evidence Library
EL-02	X		Install and configure Base Software
EL-03		X	Add Security Groups



EL-04	X		Configure Evidence Library
EL-05	N/A	N/A	Install and configure Upload Servers (if used)
EL-06	X		Installation of Evidence Library Clients on Agency's computers
EL-07		X	Provide client computers that meet client Hardware and Software requirements
EL-08		X	Connect computers to Agency Network and Active Directory Domain
4RE-01	X		Configuring available DVR units
4RE-02	X		Create Configuration USB
4RE-03	X		Configure Each DVR as installs are completed
4RE-04	N/A	N/A	Change DVR IP configuration (if required)
4RE-05	N/A	N/A	MDC Application (if required)
4RE-06	N/A	N/A	Provide client computers that meet client Hardware and Software requirements for the MDC Application.
4RE-07	N/A	N/A	Install and configure MDC application on each computer.
4RE-08	N/A	N/A	Setup or configure in-car network for DVR to Computer connectivity which includes modifying Computer policy systems (i.e. NetMotion)
4RE-09	N/A	N/A	4RE System In-Car Installation
VISTA-01	X		Configuring available VISTA WiFi cameras
VISTA-02	X		Create Configuration
VISTA-03	X		Configure Each VISTA camera
TEST-01	X		Finish Testing Function of WatchGuard system
TEST-02	X		Complete Test checklist
TRAIN-01	X		Training
TRAIN-02	X		4RE DVR Installation Training
TRAIN-03	X		4RE and VISTA WiFi End User Training (Officers)
TRAIN-05	X		Evidence Library User Training (Officers/Supervisors)
TRAIN-06	X		Evidence Library Administrative Training
Go Live-01	X	X	Go-Live Support
Close-01	X	X	Project Sign-Off

Appendix A

Scope: This document covers the "Statement of Work" for deploying the VISTA/Evidence Library system at an agency location. The table of contents includes the reference number for the task assigned to the appropriate party.



Table of Contents

SVR-01-Installation of Server in Equipment Rack	4
SVR-02-Rack Requirements	4
SVR-03-Mounting or “Racking the Server”	5
SVR-04-Connecting the Server.....	5
SVR-05-Server Specifications – Physical and Virtual	6
SVR-06-Installation and Configuration of Windows Operating System/ Disc Storage System	7
SVR-07-Provide Operating System License key	7
SVR-08-Configure Operating System.....	8
SVR-09-Setup and Perform Backups:.....	9
SVR-10-Setup Recommended Disk Configuration (virtual and physical)	9
SVR-11-Install TeamViewer	9
AP-01-Access Point Wiring and Installation.....	9
AP-02-Cabling	10
AP-03-Mounting the Access Points	10
AP-05-Access Point and Radio Configuration	13
AP-06- Provide Access Points	13
AP-07- Configure Access Points:	13
AP-08- Configure In-Car Wireless Radio configuration:	13
AP-09-MDC Configuration	14
SQL-01-Installing Microsoft SQL Server (Full Version).....	15
SQL-02-Provide License Key.....	15
SQL-03- Install and Configure SQL Server:.....	15
SQL-04- Setup SQL Backup and Maintenance Plan:	16
SQL-05-Special Considerations:	16
EL-01-Installing and Configuring Evidence Library Server components.....	17
EL-02- Evidence Library Server Installation	17
EL-03-Add Active Directory Groups	18
EL-04-Configure Evidence Library Settings	18
EL-05-Remote Upload Server (if applicable).....	18
EL-06-Installation of Evidence Library Transfer Agent on Agency Workstations	18
EL-07-Minimum Workstation Hardware Requirements.....	21

EL-08-Domain / Network Connectivity	21
EL-09- Cloud Storage.....	22
4RE-01-Configuring 4RE DVR units	22
4RE-02-Create a Configuration USB.....	22
4RE-03-Configure 4RE DVR's	22
4RE-04-Change IP Address on DVR (if applicable)	23
4RE-05-MDC Application (if applicable)	23
4RE-06-MDC Application Requirements.....	23
4RE-07-Install MDC application	24
4RE-08-Setup MDC Network	24
4RE-09-4RE In-Car System Installation	24
VISTA-01-Configuring VISTA WiFi cameras.....	24
VISTA-02-Create a Configuration.....	24
VISTA-03-Configure VISTA Cameras	25
VISTA-04-Install/Configure Smart PoE Switch in Vehicle (if applicable).....	25
TEST-01- Test Function of WatchGuard system	25
TEST-02-Checklist.....	25
TRAIN-01-Training.....	26
TRAIN-02-4RE and VISTA WiFi End User Training (Officers).....	26
TRAIN-03-Evidence Library User Training (Officers/Supervisors).....	26
TRAIN-04- Evidence Library Administrative Training.....	26

SVR-01-Installation of Server in Equipment Rack

If purchasing a 3U Rack-mount server or additional JBOD unit from WatchGuardVideo, the hardware will need to be installed in a four post server rack. The rack can be floor mounted, or on wheels.

SVR-02-Rack Requirements

You will need a standard four post server rack with the following specifications

- Adjustable mounting depth of 6" – 30" (152 – 762 mm)
- Overall rack depth of 39" (990 mm)
- Universal square holes.
- Rolling rack or bolt in rack will both work

Once the rack is installed, it is up to the customer to ensure proper grounding. Preferably to a copper grounding block that has been professionally installed by an electrician.

Non proper grounding of the server rack could result in failure of the server and will VOID the warranty

This picture will give you a good idea of the cross section of the server rack with side panels and doors removed. It is important that you abide by these requirements or your rack will NOT fit the server.



SVR-03 Mounting or "Racking the Server"

The server must be mounted prior to the arrival of the WatchGuard Video Personnel. The server weighs 60 lbs. and is very large, therefore we recommend 2 people to rack the server.

- The first step to installing the server is to open the box and find the mounting rails and the installation instructions.
- The mounting rails will be marked left and right, follow the diagrams on the instructions on how to connect the rails to the server rack, as well as, how to connect the rails to the server itself.
- Once the rails are attached to the rack, and the rails are connected to the server, the server can be pushed all the way back in to the server.
- See server documentation (located in server box) for additional details.

SVR-04-Connecting the Server

Once the server is racked, connect power along with the keyboard, mouse, monitor, and network connections.

- WatchGuard highly recommends that the server be plugged into a UPS device that is rated to maintain power to the server and all peripherals in case of a power outage. The time frame should be long enough to allow the server to be powered off normally before the server power completely fails.
By doing this, it will ensure that the server runs normally in case of brown outs and power surges. **WatchGuard does NOT provide this equipment** and it is the responsibility of the customer to purchase separately.
- The server has two standard 120v power connectors and both will need to be plugged in. The cables to connect the power supplies are included in the box
- Plug the WatchGuard Video server into your local network. Plug a cat 5e or cat 6 Ethernet cable into a switch on your network and plug the other into one of the open Ethernet ports on the back of the WatchGuard Video server.
- Plug in the access point to the open Ethernet port covered in the Access Point Installation section of this document.
- Provide a Keyboard, Mouse and Monitor, or some type of KVM device for the on-site technician to use during software installation and configuration. WatchGuard does not provide these peripherals unless ordered with the server.

SVR-05-Server Specifications – Physical and Virtual

In conjunction with the in-car components, a back end server is required to run WatchGuard Video's Evidence Library software. The server can be a physical standalone server, or installed in a virtual environment. The following specifications must be met to guarantee a successful installation of Evidence Library.

Hardware Requirements (1-5 Concurrent Vehicles)

Physical server, 1-5 concurrent vehicles

Component	Minimum	Recommended
Motherboard	Intel® Socket 1156	Intel 5520 chip set, 96 GB RAM support, PCI-E 2.0
Processor	Intel i5-650 or similar	Intel Xeon Quad Core or similar
RAM	6 GB 1333 MHz DDR3	8 GB 1333 MHz DDR3
Hard drive controller	RAID 5, RAID 6, or RAID 10	
Operating system storage	40 GB	80 GB
Staging	200 GB	500 GB
Final storage	Depends on retention	
Optional expanded video storage	NAS, SAN, JBOD, or cloud (Microsoft® Azure)	
Network cards	1 network card	2 network cards
Disk media drive	Optional	Dual layer DVD reader/burner
Peripherals	Monitor, USB keyboard, USB mouse	Monitor, USB keyboard, USB mouse, speakers

- See Storage requirements below

Virtual Machine

- The VM should be dedicated to the WatchGuard Application

Component	Minimum	Recommended
Processor	1 virtual processor	2 Virtual processors
Network cards	1 virtual network card	2 virtual network cards
RAM	4 GB	6 GB
Operating system volume	40 GB	80 GB
Staging volume	200 GB	500 GB
Final storage volume	Depends on retention	

Hardware Requirements (1-25 Concurrent Vehicles)

- Intel Socket 1156 Motherboard *Minimum*
 - (Intel 5520 Chip set, 96GB RAM support, PCI-E 2.0 **Recommended**)
- 3.20GHz Intel Core i5-650 processor *Minimum*
 - (Intel Xeon E5620, 2.40GHz Quad Core **Recommended**)
- 6GB 1333MHz DDR3 Memory *Minimum*
 - (8 GB 1333MHz DDR3 **Recommended**)
- LSI 9240-4I RAID Controller *Minimum* (Or Similar)
 - (LSI SAS9260-4I, 6Gbps, SAS/SATA w/ Battery Backup **Recommended Or Similar**)
- Intel or Equivalent Dual NIC card *Minimum*
- 8x DVD+RW Multi Drive DVD reader/burner *Minimum*
 - (Dual Layer DVD Reader/Burner **Recommended**)
- Monitor, USB Keyboard, USB Mouse **Required**
- 3 Year Full Service Warranty, Next Day On-Site **Recommended**
- NAS, SAN or JBOD for expanded video storage **Optional**
- See Storage requirements below

Virtual Server Requirements

- The VM should be dedicated to the WatchGuard Application
- 2 Processors *Minimum*
 - 4 processors are **Recommended**
- 2 Virtual Network Cards
- 6-12 GB of RAM

SVR-06-Installation and Configuration of Windows Operating System/ Disc Storage System

- Install Server Operating system
- Change Password of local administrator to WGV standard (unless agency has a different policy)
- Provide and Activate Windows Server License Key
- Set the local Security Policy to 0 days (unless different from department policy)
- Power Options – “ Put the computer to sleep: NEVER” (applies to Windows client operating system)
- Set the Administrator password to “Never Expires” (preferred)
- Configure IE/ESC security settings to OFF for Administrators
- Change windows update to the desired state for agency

SVR-07-Provide Operating System License key

Specified party will purchase/provide license key for compatible Windows operating system.

Software Requirements

An account with local Administrative level permissions is required to install the WatchGuard Video Evidence Library Software on the server. **If integrating with Active Directory, domain user with Local Admin rights is required.** Additionally the system requires the following software components.

- Operating System – *(Please note it must be one of the two options below)*
 - Microsoft Windows 7 Professional 64-bit or Windows 10 Professional 64-bit *Minimum*
 - Microsoft Windows Server
 - 2008R2 64-bit
 - 2012 64-bit
 - 2012R2 64-bit **Recommended**
- SQL Server – *(Please note that we require one of the EXACT versions of SQL Listed Below)*
 - Microsoft SQL Server 2008 R2 Standard with 5 or more CALs
 - Microsoft SQL Server 2012 Standard with 5 or more CALs
 - Microsoft SQL Server 2014 Standard with 5 or more CALs

SVR 08-Configure Operating System

(Optional) Install the following features or roles on the Operating System. These roles are installed at installation of the Evidence Library Software

- .NET Framework 4.5 features
- (AD/LDS) Active Directory Lightweight Directory Services
- Web Server
 - Management Tools
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service
 - FTP Server
 - FTP Service
 - FTP Extensibility
- Application Server
 - .NET Framework 4.5
 - TCP Port Sharing
 - Windows Process Activation Support
 - HTTP Activation
- Files Services

SVR-09-Setup and Perform Backups:

WatchGuard Video does not perform backup of the “operating system” or “video storage” on the server, this is the responsibility of the agency.

SVR-10-Setup Recommended Disk Configuration (virtual and physical)

Drive partition	Volume contents	Recommended storage size	Preferred RAID type	Preferred disk type
1	Windows operating system, SQL Server application, Evidence Library application/installation directory	50 - 200 GB	RAID 5	HDD or SSD
2	SQL Server database, Evidence Library working directory (video staging: Import and Export storage locations), processing tier (Online Video first tier)	200 GB - 1 TB	RAID 5 or RAID 10	SSD
3	Video and case storage	2 - 30 TB	RAID 5, RAID 6, or RAID 10	HDD or cloud (Microsoft® Azure)
Other	Optional backup or additional storage	TBD	TBD	TBD

*Video and Case Storage volume will vary based on the number of cameras, video quality, and video retention. Contact a WatchGuardVideo Project Manager to receive a proper storage estimate.

SVR-11-Install TeamViewer

Teamviewer can be installed and made available to WatchGuard Video to provide remote support. Other remote applications can be used. Teamviewer is the preferred choice for remote access by WatchGuardVideo.

AP-01-Access Point Wiring and Installation

This section will cover the Access Point (AP) installation and wiring. Some items in this section are specific to the “Ubiquiti” or “MikroTik” product. If using a different Access Point or In Car wireless Radio, some sections may not apply. Contact the WatchGuard Video Project Manager for details if using a different wireless solution. The party responsible for the Access Point wiring and installation needs to have the following completed:

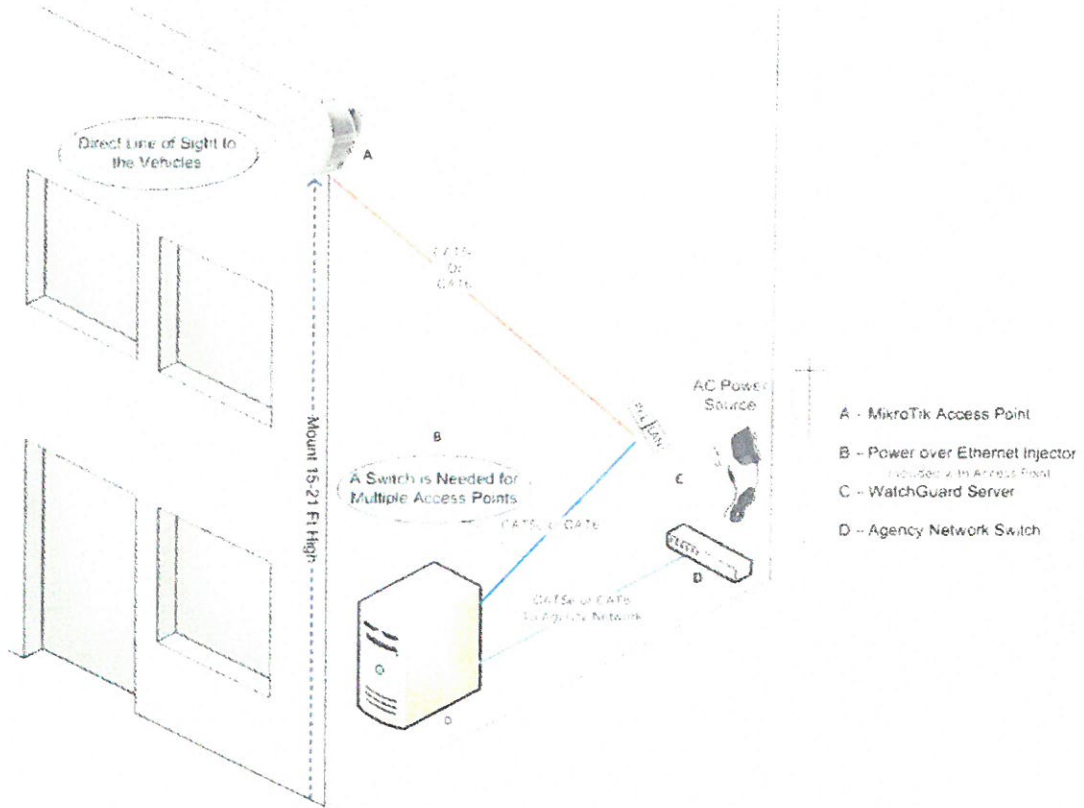
AP-02 Cabling

- Party will provide CAT5E or CAT6 Cable for the Access Point. **NOTE:** If mounting the Access Point on the exterior of a building, ensure the cable is protected. Protecting the cable can happen in 2 forms:
 - Supply an External grade CAT5E/CAT6 cable
 - Supply a conduit for the internal grade CAT5E or CAT6 cable
- Terminate the CAT5E or CAT6 cable at ALL ends to ensure there is a good connection.
- Test Connection with a cable tester or verify through AP web interface
- If using a VLAN to connect the AP to the server, ensure there is connectivity from AP to server through the managed switch.

AP-03 Mounting the Access Points

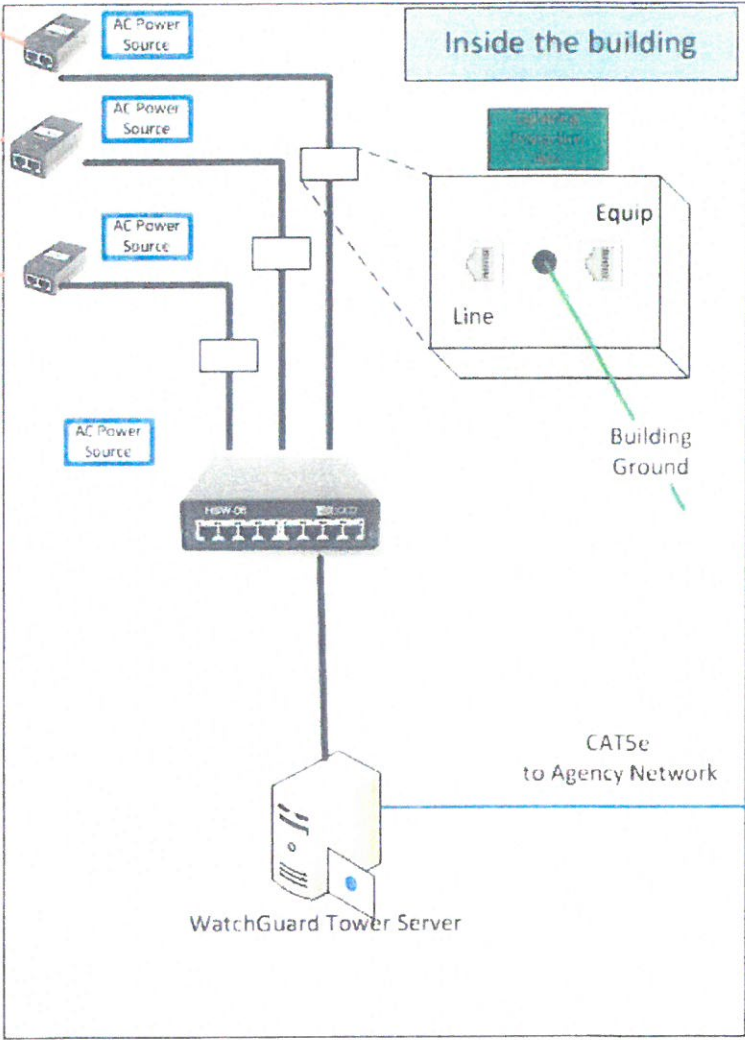
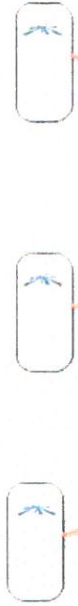
- Guidelines to mount the Access Point:
 - The AP height should be 15-21 ft. high from the ground. (any higher and the signal can overshoot the vehicles)
 - The AP needs to have direct line of sight to the vehicles with the DVR systems.
 - The AP needs to be mounted vertically.
- Ensure there is a 3 to 6 inch "Drip Loop" for the CAT5E or CAT6 cable. The drip loop prevents water from going into the RJ45 port and damaging the AP.

Access Point Wiring Diagram



Access Point
 Mounted approx 15-21 ft high
 Direct line of sight to the vehicles

Multiple Access Point Wiring Diagram



Legend:

- Cat5e PoE —
- Cat5e AP network —
- Cat5e LAN —

NOTE: Also a PoE Switch can be used that can gives 24 volts of power.

AP-05-Access Point and Radio Configuration

This section will cover the Statement of Work for the software configuration of the Access Points and Wireless radios.

AP-06- Provide Access Points

Provide Access Points that can communicate with the specifications below:

AP-07- Configure Access Points:

- Access Point should be configured to the following:
 - SSID (hidden)
 - Security: WPA2 – AES
 - Pre-shared Key (PSK)
 - Agency specified Network (e.g. 192.168.2.X/24)
- Access Points (Ubiquiti or other manufacturer) need to use the following channels if using the Ubiquiti Bullet for the in car wireless solution:
NOTE: The FCC is requiring wireless radio manufactures in the US to limit the 5Ghz frequencies to the following channels:
 - 5805 (freq. 161)
 - 5785 (freq. 157)
 - 5765 (freq. 153)
 - 5745 (freq. 149)
- Ubiquiti AP's should be used on the approved firmware versions (contact Customer service for up to date versions)
- WatchGuardVideo recommends the Wireless Radio(s) AP and in Car radio should be on the 5Ghz Range (more available channels, higher throughput). WatchGuard Video systems ship defaulted to the 5Ghz range unless otherwise specified
- If the Access Points are from a Manufacturer other than Ubiquiti, please ensure the following ports are not blocked anywhere from the AP connection to the WatchGuard server:
 - 5001
 - ICMP (ping)
 - 21
 - 20

AP-08- Configure In-Car Wireless Radio configuration:

- The in-car radios need to match the Access Point configuration
 - Refer to IP address network excel document
(document created by WGV with supplied information from Agency)
 - Same subnet (statically assigned IP addresses)
 - Same SSID
 - Same PSK
 - Same Security WPA2- AES
 - Enable NAT

- For a complete configuration guide, please contact WatchGuard Video Customer Service, or contact an IT person with knowledge on configuring the Ubiquiti or MikroTik wireless radios with the WatchGuard Video DVR.

AP-09-MDC Configuration

- If using the MDC/MDT application, the in-car wireless radio and the MDC will need to be configured to give out a specified DHCP address: from: 10.1.100.22 to 10.1.100.22 Subnet: 255.0.0.0
- Contact Customer Service for a configuration guide to configure the Bullet to give a DHCP address to the DVR.
- The Police Agency needs to have purchased the MDC application to have it installed on the MDC/MDT (In car laptop/computer)

SQL-01-Installing Microsoft SQL Server (Full Version)

Provides services and utilities to support and manipulate the Evidence Library database.

Prerequisites on SQL Server

- Microsoft Windows 7 Professional 64-bit SP2, Windows Server 2008 R2 64-bit SP2, Windows Server 2012 64-bit, Windows Server 2012 R2 64-bit or Windows Server 2014 64-bit.
NOTE: Some versions of SQL are not fully compatible with all Microsoft Operating systems. Check with Microsoft to find the compatible versions
- 64-bit processor, 1.4 GHz CPU, 2GB RAM minimum.
- *The Server hosting the WatchGuard Database must **NOT** be operating as a Domain Controller.*
- Before starting the installation of SQL, decide the storage paths for the Evidence Library database and other SQL Program files. If the server has a single volume, the default paths are probably fine.
- Logged on user must have local administrator rights on the server, and Full Control of all volumes on the server that will contain WatchGuard information.

SQL-02-Provide License Key

- Provide SQL Server license key for one of the following versions:
 - SQL Server 2008 R2
 - SQL Server 2012
 - SQL Server 2014

SQL-03- Install and Configure SQL Server:

- Execute **Setup.exe** from the SQL installation folder. Click "Next" through the initial pre-setup screens.
- Choose **Feature Installation** and select **ONLY** the following Instance Features:
 - Database Engine Services
 - Client Tools Connectivity
 - Client Tools SDK
 - SQL Server Books Online
 - Management Tools – Basic
 - Management Tools – Complete
 - SQL Client Connectivity SDK
- Select the predetermined path for the Shared Feature Directories, or use the defaults, and click "Next".
- The **Instance Configuration** screen allows the installer to specify the name of the SQL instance and the instance file path (where the actual database will be stored). The default (non-named) instance is MSSQLSERVER. If a new "Named instance" is used, it must be referred to explicitly (ServerName\NamedInstance) during all Evidence Library component installations. Choose and click Next.

- On the **Server Configuration** screen, the SQL Service Account settings are defined. Configure the following settings for each, then click Next.
 - SQL Server Agent...NT AUTHORITY\SYSTEM...Automatic Startup
 - SQL Server Database Engine.....NT AUTHORITY\NETWORK SERVICE...Automatic Startup
 - SQL Server Brower...NT AUTHORITY\LOCALSERVICE...Automatic Startup
- The **Database Engine Configuration** screen allows the installer to configure the allowed SQL authentication methods, and access permissions to the instance.
 - Select Mixed Mode (mixed mode not required, however windows authentication is required)
 - Create the SQL Server Administrator password
 - Click **Add Current User**, and then **Add**, and add the **Administrators** group from the local server to the SQL Server Administrators box, and click "Next."
 - Review settings on the Installation Summary page, and click **Install** to perform the installation.
- Once the **SQL Server Installation complete** message is displayed, click OK, then open **SQL 2008 R2 Management Studio** and login into the new SQL instance one time to verify that authentication is working.

SQL-04- Setup SQL Backup and Maintenance Plan:

- Setup a SQL Maintenance Plan to back up the following Databases (after Evidence Library is installed) every day at 11:00pm or 1:00am (avoid backup at 12:00am or during the same time as the Evidence Library cleanup schedule):
 - master
 - WGEvidenceLibrary

SQL-05-Special Considerations:

- If using a preexisting SQL server, WatchGuard recommends that the WGEvidenceLibrary database be put on a separate SQL instance
 - The **Instance Configuration** screen allows the installer to specify the name of the SQL instance and the instance file path (where the actual database will be stored). The default (non-named) instance is MSSQLSERVER. If a new "Named instance" is used, it must be referred to explicitly (ServerName\NamedInstance) during all Evidence Library component installations. Choose and click "Next."

EL-01-Installing and Configuring Evidence Library Server components

This section outlines the requirements for installing the Evidence Library core server services and components and the configuration of all tertiary settings needed for effective system reliability and function. Please get up to date instructions to installing the software from the Project Manager.

System Requirements

The following conditions are expected to be in place when considering this stage of the deployment:

- The primary Evidence Library server (either physical or virtual) has been fully provisioned according to the WatchGuard Video system requirements, and all required Server Roles are present.
- If the server is a domain member, the Active Directory account that will run the WatchGuard services already exists, is a member of the local server's Administrators' group, the required additional management Security Groups have already been created in Active Directory, and the user groups have been populated with at least some of the users that will be using the software.
- The SQL server software to host the primary Evidence Library database has been installed and correctly permissioned for the type of Evidence Library installation chosen.
- Any systems designated as Remote Upload Servers are online and meet the minimum requirements for that role.

EL-02- Evidence Library Server Installation

Install the services and software to collect, process, view, modify, store, and export video evidence collected from the in-car DVR units.

- The installation software and pre-requisite software is copied to the local repository local on the server and shared to Authenticated Users with Full Control, and set Users to have the NTFS Write capability on the shared folder. Run the software from a local drive, not over the network.
- Install the WatchGuard Video Security Token Service, creating the Lightweight Directory Service instance that the software uses for authentication, and ensure the service is started
- Install the WatchGuard Video Hosted, and ensure the service is started
- Install the WatchGuard Web Server
- Install the WatchGuard Video Wireless Import Service, and ensure the service is started, binding the service to the appropriate network adapter on the server
- Install the WatchGuard Video Evidence Library Client, providing an interface to configure the remaining service settings.
- Install the WatchGuard Video JobQueueWork Service, and ensure the service is started.

EL-03-Add Active Directory Groups

The IT Point of contact would create (or use existing) AD security Groups, for the Evidence Library application to set permissions (e.g. Officer's AD group has permission to View video, but cannot make copies of video. Supervisors AD group has permission to view all video and can make copies of video)

EL-04-Configure Evidence Library Settings

- Configure the Evidence Library application for use.
- Add necessary storage locations and shares to system
- Set all automatic retention policies on evidence and cleanup interval.

EL-05-Remote Upload Server (if applicable)

Install the services and software necessary to receive video evidence from vehicle DVRs at a remote, well-connected location, and configure the server to send all uploads to the primary WatchGuard Video server.

- The WatchGuard Video Service is installed, binding the service to the appropriate network adapter on the server, and the service is started.

Remote Evidence Library Server Installation

A WatchGuard Technician will connect remotely to a provisioned server to install the services and software to collect, process, view, modify, store, and export video evidence collected from the 4RE and VISTA WiFi cameras.

- Remote connectivity must be provided to the server that has been designated as the primary WatchGuard Server.
- The WatchGuard Technician will connect remotely to the server over the Internet prior to the agreed upon time to verify the provided server is properly configured, and to copy any required files and folders to the server.
- At the agreed upon time, the WatchGuard technician will connect to the server again and perform the software installation.
- The WatchGuard technician will configure all desired settings and assist with configuring the 4RE and VISTA WiFi cameras.
- The agency will assist with the VISTA configuration and verify functionality.

EL-06-Installation of Evidence Library Transfer Agent on Agency Workstations

Party will be responsible for installing the Evidence Library Transfer Agent on specified computers.

The Transfer Agent can be installed remotely with SCCM or other like software. *Contact Project Manager or WatchGuard Support representative to verify the instructions below are up to date:*

Transfer_Agent.exe (installed with EI website) is a wrapped version TransferAgent, TransferService and VistaDriver with install choices embedded.

It only accepts a /Q switch for unattended install

TransferAgent.exe (also included on ISO) has TransferService and Vista Driver as pre-reqs, which limits our ability to control their behavior.

TransferAgent accepts the following parameters

/s which silently installs vista driver and transfer service (only valid if upgrade or TransferService registry is pre-populated as below)

CL_HOST_SERVER=computer name (default 'localhost' if Host service detected) computer name where Host service is installed

CL_INSTALLDIR=directory (defaults to C:\Program Files (x86)\WatchGuard Video\
Installation directory

CL_OPERATIONS_DIRECTORY=directory (defaults to C:\WatchGuardVideo\)

CL_STS_SERVER=computer name (default 'localhost' if STS service detected) computer name where STS

/qb quiet basic interface (skipping user inputs with progress bar)

/qn quiet no interface

/l*v drive:\directory\file.log manually specify install log location defaults to

Examples:

Minimum silent install command line (only useful for upgrades or if registry pre-populated with answers) :

TransferAgent.exe /s /v/qn

All Parameters:

TransferAgent.exe /s /v/"qn CL_HOST_SERVER=localhost CL_STS_SERVER=localhost"
/v"CL_INSTALLDIR="C:\Program Files\WGV\"" /v"CL_OPERATIONS_DIRECTORY="C:\WGV\""

TransferService.exe (as a pre-req of TransferAgent) can only be configured at install through the use of 32-bit registry keys

[HKEY_LOCAL_MACHINE\SOFTWARE\WatchGuard Video\Transfer Service]

"STS_SERVER"="JSAVONAWIN7VM"

"HOST_SERVER"="JSAVONAWIN7VM"

"WEB_API_PORT"="9034"

"UI_URL"=<https://jsavonawin7vm.watchguardvideo.local>

Please note if you are directly entering into registry on 64-bit systems root key changes to

[HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\WatchGuard Video\Transfer Service]

Instructions for rebuilding Transfer_Agent.exe on webserver for changes to certificate either 1) or 2) below

1) Re-generate Transfer_Agent.exe package with updated certificate.

a) Copy new certificate to C:\ProgramData\WatchGuard Video\EvidenceLibraryWeb.cer (on Web server)

b) Run "C:\Program Files\WatchGuard Video\Evidence Library Web\WebRoot\Client\buildTA.cmd" 1 (from admin command prompt on Web server)

c) For deployment run new Transfer_Agent.exe /Q

--OR--

2) Use TransferAgent.exe from ISO after pre-populating answers in registry.

a) Create reg file with answers for Transfer Service. (or re-use existing C:\Program Files\WatchGuard Video\Evidence Library Web\WebRoot\Client\TransferAnswer.reg)

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\WatchGuard Video]

[-HKEY_LOCAL_MACHINE\SOFTWARE\WatchGuard Video\Transfer Agent]

[HKEY_LOCAL_MACHINE\SOFTWARE\WatchGuard Video\Transfer Service]

"STS_SERVER"="JSAVONAWIN7VM"

"HOST_SERVER"="JSAVONAWIN7VM"

"WEB_API_PORT"="9034"

"UI_URL"=<https://jsavonawin7vm.watchguardvideo.local>

b) Deploy reg answer file to target machine (unneeded if upgrading a previous installation of EL4 Transfer Agent)

reg.exe IMPORT TransferAnswer.reg /reg:32

c) Add cert to target machines (certutil -addstore "Root" EvidenceLibraryWeb.cer) or use group policy...

d) Deploy TransferAgent.exe /S /V"/qn /!*"v %TEMP%\WatchGuard_Video_Transfer_Agent.log"

EL-07-Minimum Workstation Hardware Requirements

Verify the following minimum hardware requirements

- 1.7 gigahertz (GHz) Dual core comparable or faster processor
- 1 gigabyte (GB) or more of RAM
- 160 megabytes (MB) or more of available hard disk space
- DVD-RW optical drive (if exporting to a DVD disc)
- 1 available USB 2.0 port
- Super VGA video adapter capable of 1024 x 768 resolution or higher
- 100 Mbps Network Card or better

EL-08-Domain / Network Connectivity

- Agencies using a Domain Network
 - Log into the workstation using a domain user login and password
- Agencies using a NON-Domain Network
 - Log into the workstation with a valid user login and password
- Verify the Evidence Library server is visible to the workstation using the ping command

Workstation OS & Browser Requirements

Verify one of the following operating systems is installed on the workstation(s)

- Window 7
- Windows 8.1
- Windows 10

Verify one of the following browsers is installed on the workstation

- Google Chrome v45 or Higher
- Internet Explorer 10
- Internet Explorer 11
- Microsoft Edge

User Permissions

Ensure all Evidence Library users have right to access the workstation and Evidence Library server.

EL-09- Cloud Storage

The agency or WatchGuard Video could provide cloud storage. The type of cloud storage supported depends on the Evidence Library software version. Contact WatchGuard Video Project Manager to get up to date supported cloud storage systems.

- Obtain required Cloud storage account information (i.e. Azure, endpoint suffix, account key)
- Enter in required information in Evidence Library "Evidence Management"

4RE-01-Configuring 4RE DVR units

Prior to first use, each 4RE DVR must be configured. This process involves adding each vehicle to Evidence library, generating a configuration file and deploying this configuration to the DVR using a USB drive. This process is generally shared between the Evidence Library administrator or Fleet Manager Role and the vehicle installer. If On-site services are purchased the technician will assist in creating the Vehicles in Evidence Library from an agency provided list and create the USB Configuration drive for the installer.

4RE-02- Create a Configuration USB

- Adding Vehicle to Evidence library
 - Vehicles are added to Evidence Library by an administrator or user with the Device Management role.
 - Open Device Management and select Edit configuration
 - Click the All Vehicles Node and select New to add a new vehicle.
 - Enter in a "Vehicle ID" (unique name that easily identifies each vehicle)
 - Select the appropriate "Configuration" Group
- Generating a USB configuration drive
 - Open Device Management and select Deploy Configurations Manually
 - Select the Vehicles to be configured or use the Select All function
 - Click the Export Configuration button and select a USB drive

4RE-03-Configure 4RE DVR's

- Press and hold the STOP button for 3 seconds to safely eject the current USB drive.
- Open the USB vault, remove the USB drive and place the USB Configuration drive in the unit
- On the display select the correct Vehicle ID and press the LOAD button
- Replace the original USB drive and close the vault
- Power cycle (reboot) the DVR

- Test configuration
 - Confirm that the agency name appears in the bottom right corner of the display
 - Press Menu and select Officer and verify that an appropriate list of officers is displayed
- Configure the DVR's as they are available.

4RE-04-Change IP Address on DVR (if applicable)

In some instances the DVR IP address parameters may need to be changed from the default settings. When this is required a detail list of assigned addresses will be created and provided to the Agency along with instructions on how to manually change these parameters.

The default IP address of the DVR is

10.1.100.20
255.0.0.0
10.1.0.1

The secondary IP standard is:

10.1.100.20
255.255.255.0
10.1.100.1

4RE-05-MDC Application (if applicable)

The MDC Application requires compatible hardware and software as well as several tasks need to be completed for proper operation. These tasks which include installing the application, configuring network rules and firewalls, require the support and assistance of the Agency's IT department to be involved to have a successful implementation.

4RE-06-MDC Application Requirements

- 2GHz Intel Core processor minimum (2.27 GHz recommended)
- 1GB Memory minimum (2GB recommended)
- 100 MB free hard disk space
- 800x600 screen resolution minimum (1024x768 recommended; up to 1900x1600 supported)
- Touch screen
- Available 100 Mb/s Ethernet port
- Comparable notebook PC: Panasonic Toughbook CF-31

Software Requirements:

An account with Administrative level permissions is required to install the MDC application. Additionally the system requires the following software components.

- Operating System
 - Windows XP SP3, 32-bit minimum
 - Windows 7 Pro recommended

- .NET Framework 4.0

4RE-07-Install MDC application

To install the application, please contact WatchGuard Customer Service to get software and up to date instructions

4RE-08-Setup MDC Network

There are several potential network components that may need to be configured to allow the MDC application to function correctly in your environment. WatchGuard will assist in determining the required changes but it is the Agencies responsibility to make the changes.

- A WatchGuard provided switch is needed.
- Auto configuration of the Laptop's Ethernet port.
 - Another option is to configure the Wireless Radio to provide a DHCP address
- Configure NetMotion or similar product to allow local networking
 - Configure firewalls and anti-virus software to allow operations
 - Ports: TCP 25810, UDP 25843, UDP 25845, UDP 25855

4RE-09-4RE In-Car System Installation

Follow up to date instructions that are provided in the DVR box.

VISTA-01-Configuring VISTA WiFi cameras

Prior to first use, each VISTA WiFi camera must be configured. This process is called "Checkout" and involves connecting each camera to Evidence library to assign a configuration and officer name. This process can be done each time the officer needs to be assigned a camera, or can be done in scenarios where officers are assigned a Body Camera to use on a more permanent basis

VISTA-02-Create a Configuration

- Through the Evidence Library Administrator you will access VISTA Management to complete the following steps.
 - Set up VISTA default officer preferences.
 - Create initial default configuration(s).
 - Assign enrollments (user groups) to each configuration(s).
 - Set up system event tags if not already done.
 - Set the recording properties for each configuration.
 - Set the device properties for each configuration.
 - Apply VISTA with newest firmware (contact customer service for the latest version)
 - Confirm the configuration settings, save each configuration then close VISTA Management.

VISTA-03-Configure VISTA Cameras

- Ensure the VISTA cameras have the latest firmware version (contact WatchGuardVideo Customer Service)
- Connect the VISTA USB base into the computer where your Evidence Library software is located or set up the VISTA Transfer Station to connect to your Evidence Library software.
- Dock VISTA in the USB base or VISTA Transfer Station connected to your Evidence Library software.
- Using Evidence Library software, create and /or assign a configuration and an officer to the docked VISTA.

VISTA-04-Install/Configure Smart PoE Switch in Vehicle (if applicable)

- Applicable if using the VISTA WiFi in the vehicle with or without 4RE.
 - Install Smart PoE Switch in the vehicle. Use up to date instructions.
 - Install the WiFi Base. Use up to date instructions.
 - If not using the factory default IP address from the 4RE Configure the Smart PoE switch. See the default 4RE IP address below:
10.1.100.20
255.0.0.0
10.1.0.1

TEST-01- Test Function of WatchGuard system

Test functions of the VISTA and Evidence Library system.

TEST-02-Checklist

	Test 4RE USB upload to server via Import Scanner on remote PC client
	Test 4RE Wireless upload to server
	Test Evidence Library Client Audio (Cabin microphone)
	Test Evidence Library Client Audio (Wireless microphone)
	Test wireless configuration changes
	Create a "Test" Case in Case Management
	Test Distributed Multi-Peer recording
	Test VISTA Wireless upload to server
	Test VISTA video upload to server via USB dock and/or VISTA Transfer Station
	Validate VISTA has correct configuration applied
	Test Evidence Library WEB Client Login
	Test Evidence Library WEB Client Video playback
	Test Evidence Library WEB Client Audio
	Test Exporting Evidence Library video to USB
	Test Exporting Evidence Library video to CD/DVD

TRAIN-01-Training

WatchGuard Video provides training on the Evidence Library and VISTA cameras. Online Training is covered as long as the customer is under warranty. Contact the WatchGuard Video Project Manager to setup online training for you agency.

TRAIN-02-4RE and VISTA WiFi End User Training (Officers)

WatchGuard Video will provide training (if needed) to parties who will be using the 4RE and VISTA WiFi cameras. This will cover how to use the system on a daily basis and how to get through a shift using 4RE and VISTA WiFi. Online Training is also available.

This onsite training can be completed in the following scenarios:

- 4RE Basic 5 minutes
- 4RE Full 1 hour
- VISTA/VISTA WiFi Basic 5 minutes
- VISTA/VISTA WiFi Full 45 minutes
- 4RE/VISTA Basic 7 minutes
- 4RE/VISTA Full 1 hour and 30 minutes

TRAIN-03-Evidence Library User Training (Officers/Supervisors)

WatchGuard Video will provide training (if needed) to parties who will be using the Evidence Library system on a computer. This will cover how to use the system on a daily basis, view video and make copies, make necessary changes in the system. This onsite training is typically 1 hour.

TRAIN-04- Evidence Library Administrative Training

WatchGuard Video will provide Administrative training to parties who will be using the Evidence Library on a computer. This will cover how to use administrative functions: Setting up permissions, set video retention policies, applying new configurations, and other management functions of Evidence Library. This onsite training is no longer than 3 hours, but typically can be completed in 1 hour.



VISTA NO-FAULT 3 YEAR EXTENDED HARDWARE WARRANTY

WatchGuard Video, in recognition of the high demands placed on all equipment worn, and used by Police Officers is offering the following No-Fault Warranty option. WatchGuard warrants each system, part, and component it manufactures first sold to an end user to be free from defects in material and workmanship for a period of **ONE-YEAR** from the date of purchase in its standard Limited Warranty.

The No-Fault 3 Year Extended Warranty may be purchased directly from WatchGuard Video. Any and all No-Fault warranties must be purchased with the initial purchase of the VISTA unit, and the VISTA No-Fault warranty must also be purchased for all VISTA units. Failure to purchase the No-Fault warranty at the time of purchase will require the covered unit to be physically inspected at the facility of the manufacturer and any repairs necessary to bring the unit back to full working order must be performed prior to the issuance of any new warranty. The customer will be responsible for the cost of the inspection (equal to 1 hour of labor) plus the standard costs associated with any required repairs. The following warranty terms and conditions apply with the purchase of the No-Fault VISTA Camera Warranty:

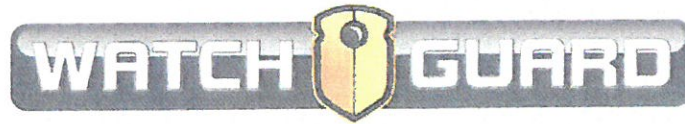
WARRANTOR – This warranty is granted by WatchGuard Video, 415 Century Parkway, Allen, TX 75013, Telephone: 972-423-9777, Facsimile: 972-423-9778.

PARTIES TO WHOM WARRANTY IS INTENDED – This warranty extends to the original end user of the equipment only and is not transferable. Any exceptions must be approved in writing from WatchGuard Video.

PARTS AND COMPONENTS COVERED – The VISTA No-Fault warranty covers all parts and components of the VISTA Standard, and the VISTA Extended capacity Body Worn Cameras. This also includes the base, cables, and battery replacements during the life of the extended warranty. Repair labor of the warranted unit manufactured and/or installed by WatchGuard Video are covered by this warranty, except those parts and components excluded below.

PARTS AND COMPONENTS NOT COVERED – The No-Fault Warranty will not include systems with intentionally altered or removed serial numbers, or it is determined that the WatchGuard Video system was internally changed, modified, or repaired.

LIMITED LIABILITY – WatchGuard Video's liability is limited to the repair or replacement of components. WatchGuard Video will not be liable for any direct, indirect, consequential, or incidental damages arising out of the use of or inability to use the system even if the unit proved to be defective.



REMEDY – If, within the duration of this warranty, a unit or component covered by this warranty is damaged in any way, WatchGuard Video shall replace the unit with an Advance Replacement unit. The Advance Replacement unit will ship via UPS ground and include a prepaid shipping label to return the defective or damaged unit. WatchGuard requires that any and all parts and pieces of the damage unit be returned. By contacting WatchGuard to send in a unit in for repair or replacement under the No-Fault Warranty, the customer agrees to return the damaged unit within 30 days. Failure to return the unit will result in the customer being billed the full purchase price for the new advance shipped unit. The Advance Replacement unit pursuant to this warranty shall be warranted for the remainder of the warranty period.

SHIPPING –Throughout the duration of the warranty period, WatchGuard Video will provide an Advance Replacement unit with a prepaid shipping label to return any defective unit for end users in the continental United States provided serial numbers are submitted during the Customer Service diagnostic process. In such event, contact WatchGuard’s Customer Service Department for troubleshooting and to start the diagnostic process. Any expedited shipping costs are the responsibility of the end user. Customers that are outside the continental United States will be responsible for all transportation costs both to and from WatchGuard Video’s factory for warranty service, including without limitation to any export or import fees, duties, tariffs, or any other related fees that may be incurred during transportation.

You may also obtain warranty service by contacting your local WatchGuard Authorized Service Center (ASC) for shipping instructions. A list of local ASCs may be obtained by contacting WatchGuard’s Customer Service Department. Customers will be responsible for all transportation costs to and from the local ASC for warranty service.

Should you have any further questions regarding the WatchGuard Video No-Fault warranty, please direct them to:

WatchGuard Video

Attn: Customer Service Department
415 Century Parkway
Allen, Texas 75013
(800) 605-6734 Toll Free Main Phone
(866) 384-8567 Toll Free Queued Customer Service
(972) 423-9777 Main
(972) 423-9778 Fax
www.watchguardvideo.com
support@watchguardvideo.com



EVIDENCE LIBRARY SOFTWARE MAINTENANCE PLAN

TERMS AND CONDITIONS

Your WatchGuard Software Maintenance Plan for Evidence Library (herein referred to as the "Software Maintenance Plan") is governed by these Terms and Conditions and constitutes your contract with WatchGuard as described below. Subject to these Terms and Conditions,

- (i) The Software Maintenance Plan applies to all customers who signed up for an active plan with WatchGuard Video after July 1, 2015.
- (ii) The Evidence Library Software ("Covered Software") first sold to an end user is guaranteed to be free defects in material and workmanship for the duration of the coverage period.
- (iii) The Software Maintenance Plan provides you with access to telephone technical support and web-based support resources for the Covered Software.
- (iv) The Software Maintenance Plan provides you with access to software service packs, minor software updates, major software upgrades, and 4RE/VISTA Firmware updates.
- (v) The Software Maintenance Plan includes the "Basic" level of CLOUD-SHARE.

The Software Maintenance Plan can be extended beyond the first year, provided payment for the annual Software Maintenance Plan for each year is made to WatchGuard prior to the end of the Coverage Period. The Software Maintenance Plan must be carried consecutively without any lapses in yearly coverage across all purchased 4RE In-Car, and VISTA units. WatchGuard will track the serial numbers of each unit and associate coverage with the Software Maintenance Plan respectively. All 4RE In-Car, VISTA and IT related hardware is excluded under the Software Maintenance Plan.

The duration of the Software Maintenance Plan ("Coverage Period") is for the period specified by any and all paid invoices related to the purchases of Software Maintenance Plans. WatchGuard may restrict service provided under this Software Maintenance Plan to the Covered Software's original country of purchase.

All Software Maintenance plans will have a "Common" expiration date that will be determined by the expiration of the original Software Maintenance from the initial purchase invoice. The common expiration date will be the same for all units. Any additional units purchased after the initial invoice, will not have Software Maintenance extended past the common expiration date unless additional years of Software Maintenance are purchased. All units must be extended at the same time and then the new expiration date will become the common expiration date for all current and future units purchased.



SERVICE OPTIONS

Remote Service which includes call center, on-line chat, email, will call, and remote desktop service, is provided free of charge for the Coverage Period. In instances where remote desktop capability is accessible, WatchGuard will make every reasonable effort to provide a solution remotely.

On-Site Technical Service must be scheduled in advance and is available at a minimum daily rate. Contact WatchGuard for further information regarding rates and availability.

TECHNICAL SUPPORT

TELEPHONE AND WEB SUPPORT

During the Coverage Period WatchGuard will provide you with access to telephone technical support and web-based technical support resources. Technical support may include the launch, configuration, troubleshooting, and recovery, interpreting system error messages, and determining when hardware repairs are required. WatchGuard will provide technical support for the Covered Software including software applications that are installed by WatchGuard or an Authorized Service Center. WatchGuard will provide support for the then-current version of the software.

SUPPORT LIMITATIONS

The Software Maintenance Plan does not cover:

- (i) Issues that could be resolved by upgrading the software to the then-current version.
- (ii) Your use of or modification to the Covered Software in a manner for which the Covered Software is not intended to be used or modified.
- (iii) Third-party products or their effects on or interactions with the Covered Software.
- (iv) Does not cover the services or time related to the installation of the software, training, or software upgrades.
- (v) Your use of a computer or operating system that is unrelated to Covered Software.
- (vi) Connectivity issues with the Covered Software over networks not built or supported by WatchGuard.
- (vii) Covered Software that has been deleted or uninstalled.
- (viii) Preventative maintenance on the Covered Software.
- (ix) Damage to, or loss of, any software or data residing or recorded on the same computer as the Covered Software. The contents of the hard drive may be deleted in the course of service. WatchGuard may install system software updates as part of your service that will prevent the software from reverting to an earlier version. Reinstallation of software programs and user data are not covered under this Plan.



- (x) Hardware Warranty coverage includes, but is not limited to, servers, computers, DVD burners, JBOD online storage devices, uninterruptable power supplies, building mounted antennas, and all related brackets and mounting hardware ("IT Equipment").
- (xi) On-Site technical service.
- (xii) Problems caused by the function of a network or viruses or other software problems introduced into the Covered Software or computer the Covered Software is running on.
- (xiii) Except as specifically provided herein, any other damages that do not arise from defects in materials and workmanship or ordinary and customary usage of the Covered Software.

Any Incident deemed out of scope as defined in this Software Maintenance Plan or any incident that occurs while no Software Maintenance Plan Agreement is in place, shall be subject to additional fees and/or charges. The Customer will be quoted applicable charges and rates prior to any service(s) being performed. Approved service(s) will commence upon receipt of a purchase order.

OBTAINING TECHNICAL SUPPORT

You may obtain technical support by calling (800) 605-6734. The Customer Service Representative will provide you technical support.

YOUR RESPONSIBILITY

To receive service or support under the Plan, you agree to comply with the following:

- (i) Provide your agency name and serial number (if required) of the Covered Software.
- (ii) Provide information about the symptoms and causes of the problems with the Covered Software.
- (iii) Respond to requests for information, including but not limited to the associated serial number of Covered Software, version, model, IT hardware, and software including operating system and database software, third-party software installed, any peripherals devices connected or installed with the Covered Software, any error messages displayed, actions taken before the Covered Software experienced the issue and steps taken to resolve the issue.
- (iv) You shall maintain all IT Equipment related to or required by the Covered Software. Any incident arising from inadequate maintenance of these systems shall be subject to additional per incident charges
- (v) Any changes to the hardware or software environment for both the Covered Software and IT Equipment made by Customer that results in any degradation in performance will be the responsibility of you including any related costs to correct the issue. Changes include, but are not limited to, in-car installation resulting in a non-approved



installation, damaged or misalignment of wireless antennas caused by the customer or weather, untrimmed trees or added obstacles that degrade wireless signal strength, added vehicles without regard for adding additional wireless access points that results in degraded performance, adding or changing video storage locations in an improper manner, adding or updating server software without the approval of WatchGuard, changes to the 4RE related network topology or architecture without consultation of WatchGuard.

GENERAL TERMS

- (i) WatchGuard may subcontract or assign performance of its obligations to third-parties but will not be relieved of its obligations to you in doing so.
- (ii) WatchGuard is not responsible for any failures or delays in performing under the Plan that are due to events outside WatchGuard's reasonable control.
- (iii) This Plan is offered and valid only in the United States of America. This Plan may not be available in all states, and is not available where prohibited by law.
- (iv) In carrying out its obligations WatchGuard may, at its discretion and solely for the purposes of monitoring the quality of WatchGuard's response, record part or all of the calls between you and WatchGuard.
- (v) WatchGuard is not obligated to renew the Software Maintenance Plan after termination. If a new Software Maintenance Plan is offered, WatchGuard will determine the price and terms.

LIMITATION OF LIABILITY

EXCEPT FOR THE LIMITED WARRANTIES AND REMEDIES CONTAINED HEREIN, THIS PRODUCT IS PROVIDED ON AN "AS IS" BASIS, WITHOUT ANY OTHER WARRANTIES OR CONDITIONS, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THOSE ARISING BY LAW, STATUTE, USAGE OF TRADE, OR COURSE OF DEALING.

NEITHER WATCHGUARD NOR ITS DEALERS OR SUPPLIERS WILL HAVE ANY LIABILITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO, LOSS OF REVENUE OR PROFIT, WHETHER RESULTING FROM THE USE, MISUSE OR INABILITY TO USE THIS PRODUCT OR FROM DEFECTS IN THE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR THEY ARE FORESEEABLE. WATCHGUARD IS ALSO NOT RESPONSIBLE FOR CLAIMS BY A THIRD PARTY. WATCHGUARD'S MAXIMUM AGGREGATE LIABILITY TO YOU, AND THAT OF ITS DEALERS AND SUPPLIERS, SHALL NOT EXCEED THE AMOUNT PAID BY YOU FOR THIS PRODUCT AS EVIDENCED BY YOUR PURCHASE RECEIPT.



This limited warranty gives you specific legal rights. You may also have other rights that may vary from state to state or from country to country. You are advised to consult applicable state or country laws for a full determination of your rights.

SUPPORT CONTACT INFORMATION

WatchGuard Video

Attn: Customer Service Department
415 Century Parkway
Allen, Texas 75013
(800) 605-6734 Toll Free Main Phone
(972) 423-9777 Main
(972) 423-9778 Fax
www.watchguardvideo.com
support@watchguardvideo.com



EVIDENCE LIBRARY END USER LICENSE AGREEMENT

CAREFULLY READ THE FOLLOWING LICENSE AGREEMENT. BY OPENING THE PACKAGE OR CLICKING ON THE "ACCEPT" BUTTON, YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "DO NOT ACCEPT" BUTTON, AND, IF APPLICABLE, RETURN THIS PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

LICENSE GRANT

The package contains software ("Software") and related explanatory written materials ("Documentation"). "Software" includes any upgrades, modified versions, updates, additions and copies of the Software. "You" means the person or company who is being licensed to use the Software or Documentation. "We" and "us" means Enforcement Video, LLC (dba WatchGuard Video).

We hereby grant you a perpetual license to use one copy of the Software on any single computer, provided the Software is in use on only one computer at any time. The Software is "in use" on a computer when it is loaded into temporary memory (RAM) or installed into the permanent memory of a computer—for example, a hard disk, CD-ROM or other storage device.

TITLE

We remain the owner of all right, title and interest in the Software and Documentation.

ARCHIVAL OR BACKUP COPIES

You may either:

- Make one copy of the Software solely for backup or archival purposes; or
- Transfer the Software to a single hard disk, provided you keep the original solely for backup or archival purposes.

THINGS YOU MAY NOT DO

The Software and Documentation are protected by United States copyright laws and international treaties. You must treat the Software and Documentation like any other copyrighted material—for example a book. You may not:

- Copy the Documentation;



- Copy the Software except to make archival or backup copies as provided above;
- Modify or adapt the Software or merge it into another program;
- Reverse engineer, disassemble, decompile or make any attempt to discover the source code of the Software;
- Place the Software onto a server so that it is accessible via a public network such as the Internet;
or
- Sublicense, rent, lease or lend any portion of the Software or Documentation.

TRANSFERS

You may transfer all your rights to use the Software and Documentation to another person or legal entity provided you transfer this Agreement, the Software and Documentation, including all copies, updates and prior versions to such person or entity and that you retain no copies, including copies stored on computer.

LIMITED WARRANTY

We warrant that for a period of ninety days after delivery of this copy of the Software to you:

- The physical media on which this copy of the Software is distributed will be free from defects in materials and workmanship under normal use; and
- The Software will perform in substantial accordance with the Documentation.

To the extent permitted by applicable law, THE FOREGOING LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, AND WE DISCLAIM ANY AND ALL IMPLIED WARRANTIES OR CONDITIONS, INCLUDING ANY IMPLIED WARRANTY OF TITLE, NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, regardless of whether we know or had reason to know of your particular needs. No employee, agent, dealer or distributor of ours is authorized to modify this limited warranty, nor to make any additional warranties.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

LIMITED REMEDY

Our entire liability and your exclusive remedy shall be:

- The replacement of any diskette(s) or other media not meeting our Limited Warranty which is returned to us or to an authorized Dealer or Distributor with a copy of your receipt; or



- If we or an authorized Dealer or Distributor are unable to deliver a replacement diskette(s) or other media that is free of defects in materials or workmanship, you may terminate this Agreement by returning the Software and Documentation and your money will be refunded.

IN NO EVENT WILL WE BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF OR THE INABILITY TO USE THE SOFTWARE (EVEN IF WE OR AN AUTHORIZED DEALER OR DISTRIBUTOR HAS BEEN ADVISED OF THE POSSIBILITY OF THESE DAMAGES), OR FOR ANY CLAIM BY ANY OTHER PARTY.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

TERM AND TERMINATION

This license agreement takes effect upon your use of the software and remains effective until terminated. You may terminate it at any time by destroying all copies of the Software and Documentation in your possession. It will also automatically terminate if you fail to comply with any term or condition of this license agreement. You agree on termination of this license to either return to us or destroy all copies of the Software and Documentation in your possession.

CONFIDENTIALITY

The Software contains trade secrets and proprietary know-how that belong to us and it is being made available to you in strict confidence. ANY USE OR DISCLOSURE OF THE SOFTWARE, OR OF ITS ALGORITHMS, PROTOCOLS OR INTERFACES, OTHER THAN IN STRICT ACCORDANCE WITH THIS LICENSE AGREEMENT, MAY BE ACTIONABLE AS A VIOLATION OF OUR TRADE SECRET RIGHTS.

GENERAL PROVISIONS

1. This written license agreement is the exclusive agreement between you and us concerning the Software and Documentation and supersedes any and all prior oral or written agreements, negotiations or other dealings between us concerning the Software.
2. This license agreement may be modified only by a writing signed by you and us.
3. In the event of litigation between you and us concerning the Software or Documentation, the prevailing party in the litigation will be entitled to recover attorney fees and expenses from the other party.
4. This license agreement is governed by the laws of the State of Texas.
5. You agree that the Software will not be shipped, transferred or exported into any country or used in any manner prohibited by the United States Export Administration Act or any other export laws, restrictions or regulations.