PURCHASING AND SERVICES AGREEMENT

This Purchasing and Services Agreement (the "***Agreement***") is entered into on June 26, 2020 by and between WatchGuard, Inc., a Delaware corporation with offices located at 415 Century Parkway, Allen, TX 75013 ("***WatchGuard***", "***we***", or "***us***") and the City of Costa Mesa, a California municipal corporation ("***Agency***", or "***you***"). WatchGuard and the Agency may be referred to individually as a "***Party***" and collectively as the "***Parties***."

WHEREAS, WatchGuard sells in-car and body-worn camera systems, components and peripheral devices and related evidence management software and support services for use by law enforcement agencies (collectively, the "***WatchGuard Products and Services***"); and

WHEREAS, the Agency wishes to purchase from WatchGuard the WatchGuard Products and Services listed on the schedules and Scope of Work attached to this Agreement, and WatchGuard desires to provide the WatchGuard Products and Services to the Agency in accordance with, and subject to, the terms and conditions set forth in this Agreement.

I. DEFINITIONS

"***Action***" means any claim, action, cause of action, demand, lawsuit, arbitration, inquiry, audit, notice of violation, proceeding, litigation, citation, summons, subpoena or investigation of any nature, civil, criminal, administrative, regulatory or other, whether at law, in equity, or otherwise.

"***Agency Content***" means information, data, and other content, in any form or medium, that is collected, downloaded, compiled or processed by the Agency using the Software, by or through the Services or that incorporates or is derived from the processing of such information, data, or content by or through the Software or the Services.

"***Agreement***" means this agreement, including any Schedule, Scope of Work and/or Amendment attached hereto and incorporated herein from time to time.

"***Amendment***" means a modification or change to this Agreement that is mutually agreed upon by WatchGuard and the Agency in writing.

"***Confidential Information***" means information in any form or medium (whether oral, written, electronic, or other) that a Party considers confidential or proprietary, including information consisting of or relating to the disclosing Party's Intellectual Property Rights (defined below) technology, trade secrets, know-how, business operations, plans, strategies, customers, and pricing, and information with respect to which the disclosing Party has contractual or other confidentiality obligations, in each case whether or not marked, designated, or otherwise identified as "confidential".

"***Effective Date***" means June 26, 2020.

"***Hardware***" means the camera systems, connectors, components and peripheral devices, and related device licenses, listed in Schedule 1 to this Agreement.

"***Hardware Maintenance Plan***" means our agreement to maintain and support the Hardware, as set forth in Schedule 2 to this Agreement.

"***Intellectual Property Rights***" means all intellectual and proprietary rights, including but not limited to, invention and patents for inventions, know-how, trade secrets, copyrights and trademarks.

"***Losses***" means any and all losses, damages, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

"***Project Manager***" means, for each of WatchGuard and the Agency, the person designated as the Party's principal point of contact for administering and coordinating such Party's responsibilities under this Agreement, including management and oversight of the day-to-day work required of such Party.

"***Scope of Work***" means the Scope of Work prepared by WatchGuard and agreed to by the Agency, and attached to this Agreement as Schedule 1, plus all exhibits, appendices, and Amendments thereto, and the implementation, technical, and functional specifications set forth therein.

"***Services***" means all work described in Schedule 1 required to be performed by WatchGuard to deploy, install, configure, integrate, and render operational the Hardware and the Software.

"***Software***" means the WatchGuard proprietary evidence management platform described in Schedule 1. Software does not include any Third-Party Materials, software applications or commercially available software application, package or platform developed by the Agency or licensed to the Agency directly from a third party.

"***Software Maintenance Plan***" means our agreement to maintain and support the Software, as set forth in Schedule 3 to this Agreement.

"***Specifications***" means all specifications describing the features, functionality, and performance of the System, and identifying the Software and Hardware functions and capabilities needed to implement such features, functionality, and performance.

"***Subcontractor***" means any person or entity, other than an employee or affiliate of WatchGuard, that contracts with WatchGuard to perform Services.

"***Support Services***" has the meaning set forth in Section 2.5.

"***System***" means the Hardware and the Software together as configured, integrated, interconnected and implemented as described in the Scope of Work attached as Schedule 1 to this Agreement.

"***Term***" shall have the meaning set forth in Article VIII.

"***Third-Party Materials***" means materials, information, software, equipment, or components of or relating to the Services that are not proprietary to WatchGuard, or not otherwise approved by WatchGuard for use with the WatchGuard Products and Services, the Software, the Hardware, or the System.

"***Warranties***" means the warranties for the Hardware and Software listed on Schedule 2 and Schedule 3 to this Agreement, respectively, and as described in Article V of this Agreement.

"***WatchGuard Materials***" means the Services, Specifications, and Systems and any and all other information, data, documents, materials, works, and other content, devices, methods, processes, hardware, software, and other technologies and inventions, including any deliverables, technical or functional descriptions, requirements, plans, or reports, that are provided or used by WatchGuard or any Subcontractor in connection with the Services or otherwise comprise or relate to the WatchGuard Products and Services or Systems.

"***WatchGuard Products and Services***" means the camera hardware systems and components, the software, and the support services listed and described in Schedules 1, 2, 3, and 4 attached hereto and incorporated herein.

II. WatchGuard Obligations

2.1. System Delivery. According to the Specifications, and in accordance with the requirements set forth in Schedule 1 we will provide or cause to be provided, either (i) on-site or remote installation of the System, including without limitation, the Hardware and Software, by our employees or by a Subcontractor reasonably acceptable to you; or (ii) the Software, for your installation and configuration on your computer systems and infrastructure, without our provision of Services.

2.2. WatchGuard Work. Where called for in Schedule 1 we will plan, design, develop, deliver, install, render operational, implement and support the System, and provide the Agency with all related deliverables and Services necessary to fulfill our obligations under this Agreement. Without limiting the foregoing, we will provide, or provide through a Subcontractor reasonably acceptable to the you, all labor, equipment, accessories, tools, and other items and do all work required to meet the Specifications and fulfill the requirements of the Scope of Work, where the same are not expressly set forth in this Agreement as being your responsibility.

2.3. Designation of Project Manager. We will designate an employee to serve as Project Manager; provided, that we may replace our Project Manager at any time, and from time to time, upon prior notice to you, with one or more employees having similar knowledge, skills and abilities.

2.4. Training. We will provide designated Agency personnel on-site and/or remote training reasonably required to ensure that such personnel are capable of properly and efficiently operating and maintaining the System. The training program is more specifically described in the Scope of Work.

2.5. Maintenance and Support Services. We will make available to you ongoing maintenance and support services as described in the Scope of Work and/or the Warranties, the Hardware Maintenance Plan, and the Software Maintenance Plan. Such support may include, but may not be limited to, updates to the Software or Hardware necessary for the Software or Hardware to continue to meet Warranty requirements and/or the Specifications.

2.6. Insurance. While performing the Services and during the Term, we will maintain in force and effect Commercial General Liability Insurance, Workers Compensation Insurance, and Commercial Automobile Insurance in amounts specified by you, and will furnish you with certificates of insurance prior to providing the Services, in a form acceptable to you. The Commercial General Liability insurance policy shall include an endorsement naming the Agency as an additional insured.

III. Agency Obligations

3.1. Approval. You agree to confer, coordinate and cooperate with us to approve and accept the WatchGuard Products and Services, the System and the Specifications prior to us beginning to perform the Services. Notwithstanding the foregoing, your approval shall not operate as a waiver by you of any rights you may have under this Agreement, the Warranties, the Hardware Maintenance Plan, or the Software Maintenance Plan with regard to any non-conforming or defective WatchGuard Products and Services.

3.2. Designation of Project Manager. You agree to designate an employee to serve as Project Manager; provided, that you may replace your Project Manager at any time, and from time to time, upon prior notice to us with one or more employees having similar knowledge, skills and abilities.

3.3. Access. You agree to provide our employees and approved Subcontractors access to Agency premises and equipment sufficient to allow us to perform the Services according to the Specifications, and to make Agency personnel, including your Project Manager, available at reasonable times and upon our prior request, to facilitate our access to Agency premises and equipment.

3.4. Operation of the System. You will be responsible for (a) use of the WatchGuard Products and Services by your employees, agents, contractors, and end-users; (b) Agency Content or the combination of Agency Content with

other applications, content or processes, including any claim involving alleged infringement or misappropriation of third party rights by Agency Content or the use of Agency Content; (c) disputes between you and any third party over your use of the WatchGuard Products and Services or the collection or use of Agency Content; and (d) any hardware or networks that we do not authorize, approve or provide that you connect to or use in connection with the Software or Hardware following performance of the Services.

3.5. Payment of Fees. The fees for the Services, Warranties, and Support services are set forth in the Mobile Video System Combined Proposal attached as Schedule 4 to this Agreement. You agree to pay us the fees set forth in any invoice we submit to you for the Services, or in the Statement of Work, as it may be amended or supplemented by agreement of the Parties from time to time, within thirty (30) days of receipt of an invoice. Each invoice shall detail services rendered, time spent and fee.

IV. Indemnification

4.1. Indemnification by WatchGuard. We will indemnify and defend you and your elected officials, officers, directors, employees, agents, permitted successors and permitted assigns (each, an "***Agency Indemnitee***") from and against any and all Losses incurred by the Agency or an Agency Indemnitee resulting from any Action by a third party alleging (i) that your use of the Software (excluding Agency Content and Third-Party Materials) in accordance with this Agreement (including the Specifications) infringes or misappropriates such third party's U.S. Intellectual Property Rights; or (ii) negligent acts, errors or omissions, or willful misconduct of WatchGuard under or related to this Agreement, or performance of the Services. The foregoing obligation does not apply to the extent that the Action arises from:

(i) Third-Party Materials or Agency Content;

(ii) access to or use of the WatchGuard Materials in combination with any hardware, system, software, network, or other materials or service that we did not provide or that was not specified for Agency use in the Scope of Work or Specifications;

(iii) modification of the WatchGuard Materials other than: (a) by or on behalf of us; or (b) with our written approval in accordance with the Specifications;

(iv) failure to timely implement any modifications, upgrades, replacements, or enhancements made available to you by or on behalf of us.

V. Warranties

5.1. Hardware Warranty. We will provide you with warranty coverage for the Hardware upon the terms set forth in Schedule 2.

5.2. Software Warranty. We will provide you with the warranty coverage for the Software as set forth in Schedule 3.

5.3. Warranty Limitations. Except for the express warranties set forth in the WatchGuard Warranties, all WatchGuard Products and Services are provided "as is." All Third-Party Materials are provided "as is" and any representation or warranty of or concerning any Third-Party Materials is strictly between you and the third-party owner or distributor of the Third-Party Materials.

5.4 Performance of Services. We warrant and represent to you that all of the WatchGuard Products and Services to be performed or provided pursuant to this Agreement shall be performed and provided with care, expertise, skill, and diligence generally consistent with prevailing industry standards and expertise by companies providing or performing similar products and services.

VI. Intellectual Property Rights

6.1. WatchGuard Materials. We hereby grant to you a nonexclusive, perpetual, royalty-free license to use the Software consistent with the purposes of this Agreement. Except for the license rights in the Software expressly granted to you under this Agreement, we retain all right, title, and interest in and to the WatchGuard Materials, including all Intellectual Property Rights therein. With respect to Third-Party Materials, the applicable third-party providers own all right, title, and interest, including all Intellectual Property Rights, in and to the Third-Party Materials. You have no right, license, or authorization with respect to any of the WatchGuard Materials except as expressly set forth in this Agreement. We expressly retain all rights in and to the WatchGuard Materials not expressly granted herein.

6.2. Agency Content. As between you and us, you are and will remain the sole and exclusive owner of all right, title, and interest in and to all Agency Content, including all Intellectual Property Rights relating thereto. Notwithstanding the foregoing, you hereby grant all such rights and permissions in or relating to the Agency Content as are necessary or useful to us or our Subcontractors, to (a) provide the Services, (b) enforce this Agreement, and (c) exercise such rights as we or our Subcontractors may require to perform our obligations hereunder.

VII. Confidential Information

7.1. Disclosure. In connection with this Agreement each Party may disclose or make available Confidential Information to the other Party. Each Party will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of the other Party's Confidential Information. Except as required by applicable law, neither Party will disclose the other Party's Confidential Information during the Term or at any time during the five-year period following expiration of the Term without the prior written consent of the other Party.

VIII. Term and Termination

8.1. Initial Term. (a) If this Agreement is for the provision of WatchGuard Products and Services with no ongoing licenses, fees, or Services (as set forth in Schedule 1), the term shall commence as of the Effective Date and terminate without renewal upon completion of the Services; provided that provisions of this Agreement that are intended by their nature to survive termination or expiration shall remain in force and effect until they are satisfied or expire; (b) If this Agreement is for provision of WatchGuard Products and Services with ongoing licenses, fee or Services (as set forth in Schedule 1), the initial term of this Agreement shall commence as of the Effective Date and, unless earlier terminated pursuant to any of this Agreement's express provisions, will continue in effect until five (5) years from such date (the "***Initial Term***").

8.2. Renewal. Upon expiration of the Initial Term this Agreement may be renewed for successive one (1) year terms by written agreement of the Parties (each a "***Renewal Term***" and, collectively, together with the Initial Term, the "***Term***").

8.3. Termination. In addition to any other express termination right set forth elsewhere in this Agreement:

(a) we may terminate this Agreement, effective on written notice to you, if you: (i) fail to pay any amount when due hereunder, and such failure continues more than 30 days after we provide you with written notice thereof; or

(b) either Party may terminate this Agreement, effective on 30 days written notice to the other Party, if the other Party materially breaches this Agreement, and such breach: (i) is incapable of cure; or (ii) being capable of cure, remains uncured 30 days after the non-breaching Party provides the breaching Party with written notice of such breach; or

(c) you may terminate this Agreement if you fail to obtain or appropriate budgeted funds, or if funds are not otherwise legally available to pay the fees required under this Agreement such that your continued performance

of your obligations under this Agreement is not possible, in which case you agree to provide us with written notice of termination at least 90 days prior to the end of your then-current fiscal year, or as soon as is reasonably practical under the circumstances.

IX. MISCELLANEOUS

9.1. Further Assurances. Upon a Party's reasonable request, the other Party shall, at the requesting Party's sole cost and expense, execute and deliver all such documents and instruments, and take all such further actions, as may be necessary to give full effect to this Agreement.

9.2. Relationship of the Parties. The relationship between the Parties is that of independent contractors. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, employment, or fiduciary relationship between the Parties, and neither Party shall have authority to contract for or bind the other Party in any manner whatsoever.

9.3. Notices. Any notice, request, consent, claim, demand, waiver, or other communications under this Agreement have legal effect only if in writing and addressed to a Party as follows (or to such other address or such other person that such Party may designate from time to time in accordance with this Section 9.3):

If to Provider: 415 Century Parkway, Allen, TX 75013
Facsimile: (214) 383-9661
Email: brian.greene@motorolasolutions.com
Attention: Brian Greene

If to Customer: City of Costa Mesa Police Department
99 Fair Drive, Costa Mesa, CA 92626
Facsimile: (714) 754-4911
Email: jlapointe@costamesaca.gov
Attention: Joyce LaPointe, Lieutenant

Copy to: City of Costa Mesa
77 Fair Drive
Costa Mesa, CA 92626
Attn: Finance Dept. | Purchasing

Notices sent in accordance with this Section 9.3 will be deemed effectively given: (a) when received, if delivered by hand, with signed confirmation of receipt; (b) when received, if sent by a nationally recognized overnight courier, signature required; (c) when sent, if by facsimile or email, (in each case, with confirmation of transmission), if sent during the addressee's normal business hours, and on the next business day, if sent after the addressee's normal business hours; and (d) on the third day after the date mailed by certified or registered mail, return receipt requested, postage prepaid.

9.4. Entire Agreement. This Agreement, together with any other documents incorporated herein by reference, constitutes the sole and entire agreement of the Parties with respect to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Agreement, the related exhibits, schedules, and attachments and any other documents incorporated herein by reference, the following order of precedence governs: (a) first, this Agreement, excluding its exhibits, schedules, and attachments; (b) second, the exhibits, schedules, and attachments to this Agreement as of the Effective Date; and (c) third, any other documents incorporated herein by reference.

9.5. Assignment. Neither Party may assign or transfer this Agreement or its rights or obligations hereunder without the prior written consent of the other party; provided, that we may assign or transfer this Agreement or any of our rights or obligations hereunder without your consent in connection with (a) the sale of all or substantially all of our stock or assets; (b) a merger or acquisition, whether we are the surviving or disappearing entity; (c) a corporate reorganization; or (d) transfer to a subsidiary or affiliate entity. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective successors and permitted assigns.

9.6. Force Majeure.

(a) No Breach or Default. In no event will either Party be liable or responsible to the other Party, or be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement, (except for any obligations to make payments), when and to the extent such failure or delay is caused by any circumstances beyond such Party's reasonable control (a "***Force Majeure Event***"), including acts of God, flood, fire, earthquake or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Agreement, national or regional emergency, plague, epidemic, pandemic, outbreaks of infectious disease or any other public health crisis, including quarantine or other government-imposed restrictions, strikes, labor stoppages or slowdowns or other industrial disturbances, passage of law or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota, or other restriction or prohibition or any complete or partial government shutdown, or national or regional shortage of adequate power or telecommunications or transportation. Either Party may terminate this Agreement if a Force Majeure Event affecting the other Party continues substantially uninterrupted for a period of 30 days or more.

(b) Affected Party Obligations. In the event of any failure or delay caused by a Force Majeure Event, the affected Party shall give prompt written notice to the other Party stating the period of time the occurrence is expected to continue and use commercially reasonable efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

9.7. No Third-Party Beneficiaries. This Agreement is for the sole benefit of the Parties hereto and their respective successors and permitted assigns and nothing herein, express or implied, is intended to or shall confer upon any other person any legal or equitable right, benefit, or remedy of any nature whatsoever under or by reason of this Agreement.

9.8. Amendment and Modification; Waiver. No amendment to or modification of or rescission, termination, or discharge of this Agreement is effective unless it is in writing and signed by each Party. No waiver by any Party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the Party so waiving. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Agreement will operate or be construed as a waiver thereof; nor shall any single or partial exercise of any right, remedy, power, or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

9.9. Severability. If any term or provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the Parties hereto shall negotiate in good faith to modify this Agreement so as to effect the original intent of the Parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

9.10. U.S. Government Rights. The Services are provided to the U.S. government as "commercial items", "commercial computer software", commercial computer software documentation", and "technical data", with the same rights and restrictions generally applicable to the Services. If you are using the Services on behalf of the U.S.

government and these terms fail to meet the U.S. government's needs or are inconsistent in any respect with federal law, you agree to immediately discontinue use of the Services. The terms as "commercial items", "commercial computer software", commercial computer software documentation", and "technical data" as used in this Section 9.10 have the same meaning as in the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement.

9.11. Equal Opportunity Compliance. In performing the Services we agree to abide by all applicable laws, regulations, and executive orders pertaining to equal employment opportunity, including federal laws and the laws of the State in which its primary place of business is located. In accordance with such laws, regulations, and executive orders, we agree that no person shall, on the grounds of race, color, religion, national origin, sex, age, veteran status or handicap, be excluded from employment with or participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity we perform in connection with this Agreement. If we are found to be non-compliant with these requirements in performing the Services or during the term of the Agreement, we agree to take appropriate steps to correct these deficiencies. Upon request, and as required by applicable law, we will furnish information regarding our nondiscriminatory hiring and promotion policies, as well as specific information on the composition of our principals and staff, including the identification of minorities and women in management or other positions with discretionary or decision-making authority.

9.12. Governing Law. This Agreement is governed by and construed in accordance with the internal laws of the state in which the Agency is physically located, without reference to conflict of laws rules. The United Nations Convention for International Sale of Goods does not apply to this Agreement.

9.13. Counterparts. This Agreement may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. A signed copy of this Agreement delivered by facsimile, email, or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

(Signature Page Follows)

IN WITNESS WHEREOF, the Parties hereto have executed this Purchases and Services Agreement as of the Effective Date.

CITY OF COSTA MESA

By: Lori Ann Farrell Harrison

Name Printed: Lori Ann Farrell Harrison

Title: City Manager

WATCHGUARD, INC.

By: Troy Montgomery

Name Printed: TROY MONTGOMERY

Title: DIRECTOR OF SALES

ATTEST:

Brenda Green 7-17-2020

Brenda Green
City Clerk

APPROVED AS TO FORM:

Kimberly Hall Barlow

Kimberly Hall Barlow
City Attorney

SCHEDULE 1

SCOPE OF WORK

(*SEE ATTACHED*)

Date: June 26, 2020 ("Effective Date")

Service Provider:
WatchGuard, Inc. a corporation incorporated in the state of Texas

Client:
City of Costa Mesa Police Department
Attn: STEPHANIE URUETA
77 Fair Drive Costa Mesa CA 92626

Principal Address of Service Provider:
415 E. Exchange Parkway
Allen, Texas 75002
Telephone Number: (866) 325-2836

WatchGuard, Inc. Federal Tax Identification Number:
11-3717781

1. **Scope of Work.** Service Provider will perform certain services and provide deliverables for Costa Mesa Police Department as described in the Statement of Work attached hereto as Schedule 1 (the "Initial Services"). During the term of the Agreement, Costa Mesa Police Department may request Service Provider to perform additional services, which shall be outlined in an additional description of services acknowledged in writing by both parties. 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 Statement of Work as the "Services". All Schedules and Exhibits attached hereto are hereby incorporated by this reference.

2. **Agency Provided Services and Equipment.** Costa Mesa Police Department 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. Costa Mesa Police Department acknowledges that these tasks or equipment are required and the Agency's failure to perform or deliver these tasks may result in additional costs and or delays.

3. **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. Costa Mesa Police Department may audit such records during normal business hours upon prior notice to Service Provider.

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

Schedule 1
Initial Services Statement of Work

Under the terms and conditions of the Purchasing and Services Agreement dated June 23, 2020 by and between Service Provider and Costa Mesa Police Department, the Service Provider shall provide and deliver the Initial Services and Deliverables set forth below.

Provided Services:
WatchGuard, Inc. will provide to Costa Mesa Police Department services resulting in the successful and satisfactory installation and configuration of the WatchGuard 4RE High Definition In-Car Video System with Integrated V300 body worn camera 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, Inc. is responsible for that particular task. If an "X" is listed under the "Agency" column, then Costa Mesa Police Department 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	**NA**		**Installation of Server in Equipment Rack (if applicable)**
SVR-02	**NA**		Provide a suitable Rack
SVR-03	**NA**		Mounting or Racking the Server
SVR-04	**NA**		Connecting the server (120V Power connector), KVM, Network Cabling and switches, JBOD, UPS)
SVR-05	**NA**		**Provide a physical or Virtual Server that meets the specified Server Requirements**
SVR-06	**NA**		**Installation and configuration of Windows Operating System and disk storage systems**
SVR-07	**NA**		Provide Operating System License
SVR-08	**NA**		Install and configure Operating System (Includes current patches)
SVR-09	**NA**		Setup and perform backups
SVR-10	**NA**		Setup recommended disk configuration
SVR-11	**NA**		Install and configure for remote access
SVR-12	**NA**		Installation of Mikrotik Access Points
SQL-01	**NA**		**Installation of Microsoft SQL Server**
SQL-02	**NA**		Provide SQL Server Licenses
SQL-03	**NA**		Install and configure SQL Server
SQL-04	**NA**		SQL Backup and Maintenance plan
SQL-05	**N/A**		Setup SQL Instance (if shared database server),
EL-01	**X**		**Installing and configuration of Evidence Library (CLOUD)**
EL-02	**X**		Install and configure Base Software

EL-03	X	X	Add or Sync Security Groups and Users
EL-04	X		Configure Evidence Library
EL-05	N/A		Install and configure Upload Servers (if applicable)
EL-06	X	X	**Installation of Evidence Library agent on Agency computers**
EL-07		X	Provide client computers that meet client Hardware and Software requirements.
EL-08		X	Connect client computers to Agency Network and Active Directory Domain
EL-09	X		Installation of Evidence Library Cloud Environment
EL-10	X	X	Installation and Configuration of Redactive machine (if applicable)
4RE-01	X	X	**Configuring available 4RE DVR units**
4RE-02	X		Create Configuration USB
4RE-03	X		Configure Each DVR as installs are completed
4RE-04	X	X	Change DVR IP configuration (if required)
4RE-05	NA		**MDC Application (if required)**
4RE-06	NA		Provide client computers that meet client Hardware and Software requirements for the MDC Application.
4RE-07	NA		Install and configure MDC application on each computer.
4RE-08	NA		Setup or configure in-car network for DVR to Computer connectivity which includes modifying Computer policy systems (i.e. NetMotion)
4RE-09	X	X	**4RE System In-Car Installation**
4RE-10	NA		**4RE Interview Room setup**
4RE-11	NA		**4RE-M 4RE Motorcycle System Installation**
V300-01	NA		**Configuring available V300 body worn cameras**
V300-02	NA		Create Configuration
V300-03	NA		Configure Each V300 body worn camera
V300-04	NA		Install/Configure Smart PoE Switch in Vehicle (if applicable)
V300-05	NA		Install and Configure Transfer Station (if applicable)
V300-06	NA		Install, Connect, Configure Transfer Station Racks
TEST-01	X		**Finish Testing Function of WatchGuard System**
TEST-02	X		Complete Testing Checklist
TRAIN-01	X		**Training**
TRAIN-02	X		4RE DVR Installation Training
TRAIN-03	X		4RE and V300 End User Training (Officers)
TRAIN-05	X		Evidence Library User Training (Officers/Supervisors)
TRAIN-06	X		Evidence Library Administrative Training
TRAIN-07	X		Redactive Training
Close-01	X	X	**Project Sign-Off**

Appendix A Reference
This appendix references the page number that include detailed actions and instructions for each "short description" in Table 1. See Appendix A, for details on each reference number.

Table of Contents

Appendix A

Scope: This document covers the "Statement of Work" for deploying the Evidence Library/4RE/V300 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

If purchasing a 3U Rack-mount server or additional JBOD unit from WatchGuard Video, 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

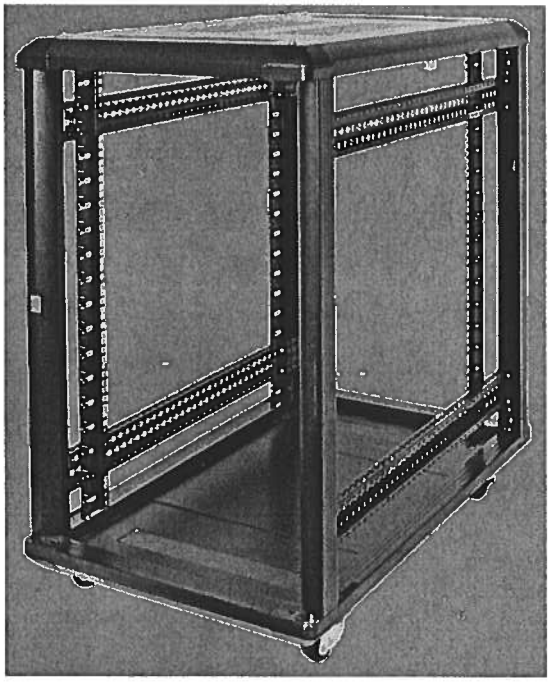
You will need a standard four post server rack with the following specifications

- 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

Components	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

Components	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	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 Preform 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 - 50 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 WatchGuard Video 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 WatchGuard Video.

AP-01-Access Point Wiring and Installation

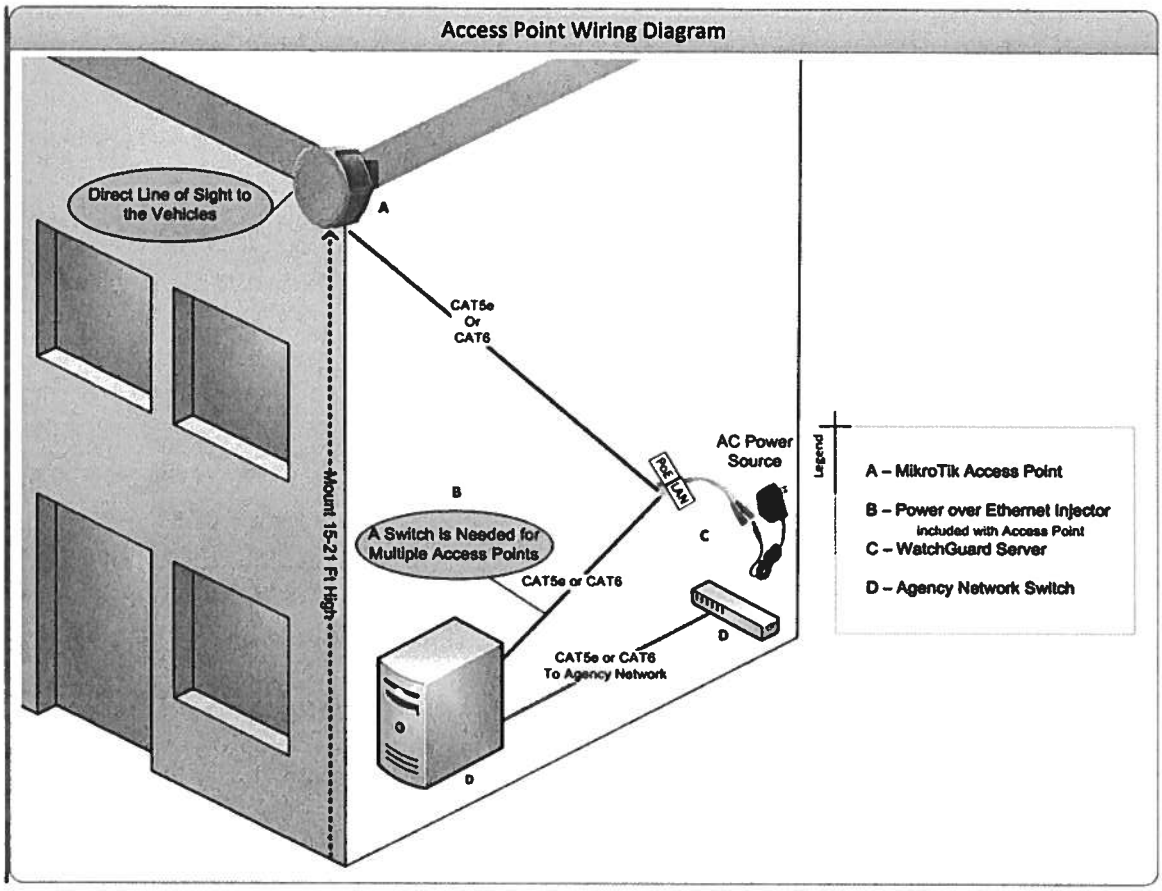
This section will cover the Access Point (AP) installation and wiring. Some items in this section are specific to the "Ubiquiti" or "MikroTik" product. If using a different Access Point or In Car wireless Radio, some sections may not apply. Contact the WatchGuard Video Project Manager for details if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

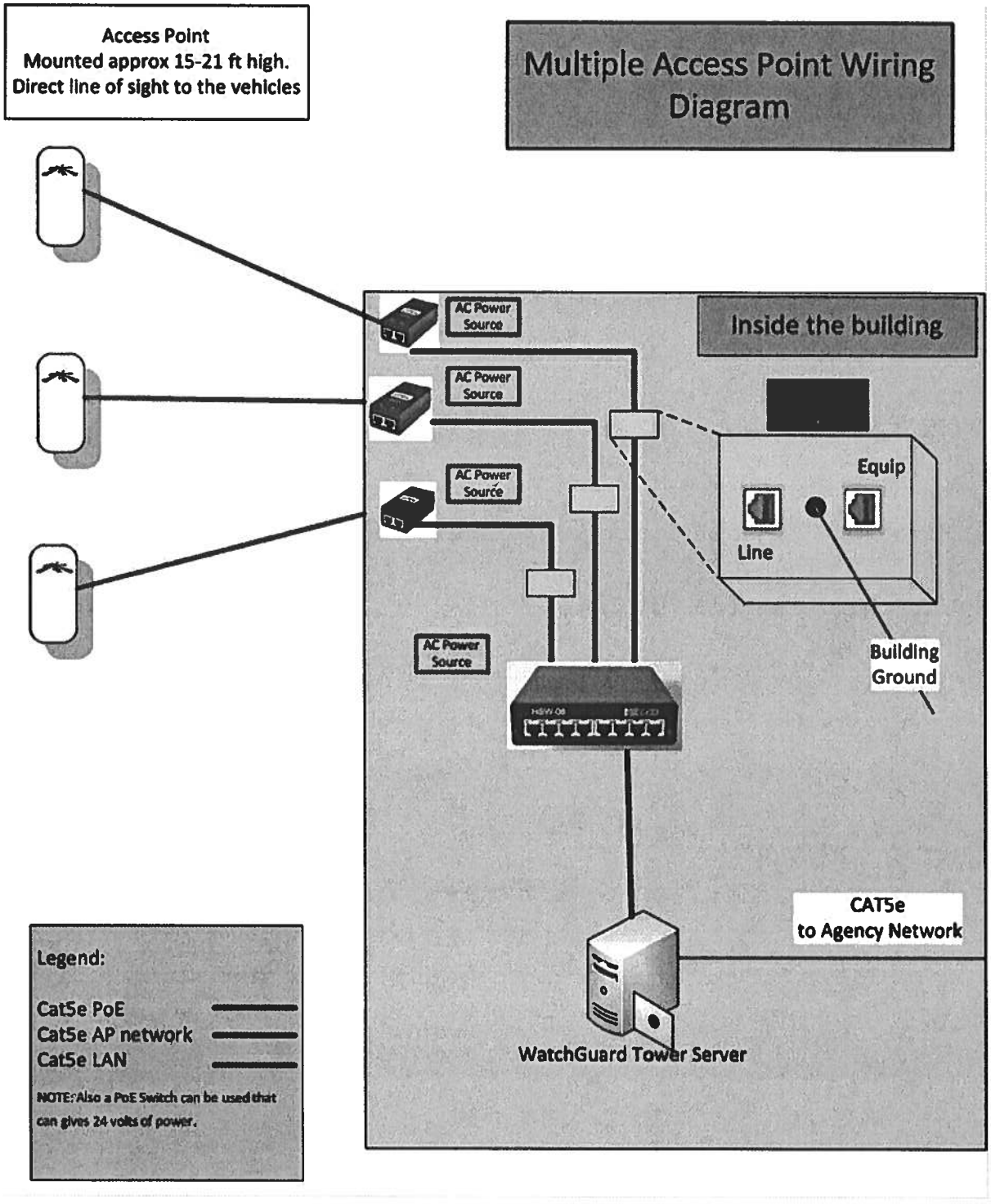
AP-02-Cabling

- 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
Direct Line of Sight to the Vehicles
A
CAT5e Or CAT6
Mount 15-21 Ft High
AC Power Source
PoE / LAN
B
A Switch is Needed for Multiple Access Points
C
CAT5e or CAT6
D
CAT5e or CAT6 To Agency Network
D
Legend
A – MikroTik Access Point
B – Power over Ethernet Injector
Included with Access Point
C – WatchGuard Server
D – Agency Network Switch


Access Point
Mounted approx 15-21 ft high.
Direct line of sight to the vehicles
Multiple Access Point Wiring Diagram
Inside the building
AC Power Source
AC Power Source
AC Power Source
AC Power Source
Equip
Line
Building Ground
CAT5e to Agency Network
WatchGuard Tower Server
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)
- WatchGuard Video 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.

Evidence Library Cloud System (if applicable)

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

- The Evidence Library server has been fully provisioned by WatchGuard engineers according to customer sizing requirements, and all required Server Roles and SQL are present.
- If the customer wishes to use Active Directory to authenticate their users, we will assist the customer with the setup and configuration of either an on-premise AD synchronization, or connect the customer's Office 365 Active Directory environment to EvidenceLibrary.com in order to access the current user base. Any required management Security Groups have 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.
- Any systems designated as Upload Appliances are online and meet the minimum requirements for that role.
- Internet access to the cloud is currently available and meets the minimum upload/download requirements as established or meets the previously determined connection speeds as determined by the customer at the time of contract discussions.
- At least one department user has been assigned the role as administrator for the purpose of management of the system.

Evidence Library On-Premise System (if applicable)

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 or Synchronize Active Directory Groups

The IT Point of contact would create (or use existing) AD Security Groups for the Evidence Library application to assign permissions to those groups (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). WatchGuard will demonstrate and assist with creation of those groups and demonstrate the permission assignments within Evidence Library.

EL-04-Configure Evidence Library Settings

- Configure the Evidence Library application for use.
- Add storage locations and folder shares and permissions to system (if applicable)
- Set all automatic retention policies on evidence and the cleanup intervals.

EL-05-Remote Upload Server/Appliance (if applicable)

Install the services and software necessary to receive video evidence from WatchGuard devices at either local or remote (well-connected) location, and configure the server to send all uploads to the WatchGuard Video server, whether on-premise or cloud hosted.

- The WatchGuard Upload Service is installed, binding the service to the appropriate network adapter on the server, and the service is started and tested for performance.

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 V300 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 V300 WiFi cameras.
- The agency will assist with the V300 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 El website) is a wrapped version containing the WatchGuard TransferAgent, TransferService and V300Driver with install choices embedded.

It can accept a /Q switch for unattended install.

TransferAgent.exe (also included on ISO) has TransferService and V300 Driver as pre-reqs, which limits our ability to control their behavior.

TransferAgent accepts the following parameters

/s which silently installs V300 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"="PDServer"
"HOST_SERVER"="PDServer"
"WEB_API_PORT"="9034"
"UI_URL"=https://PDServer.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 /l*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)

- 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 may provide hybrid cloud storage. The type of cloud storage supported depends on the Evidence Library software version. Contact WatchGuard 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"

Obtain required Cloud storage account information (i.e. Azure, endpoint suffix, account key)

- Enter in required information in Evidence Library "Evidence Management"

EL-10- Redactive

The agency or WatchGuard Video may provide the appropriate machine to run Redactive. If a WatchGuard Redactive server is purchased, the Watchguard onsite representative may install and connect the server to the agency network. WatchGuard will demonstrate and install the Redactive software on the appropriate machine. If an Enterprise version of Redactive is purchased, WatchGuard

will demonstrate and assist the setup of users and group permissions so that agency personnel are familiar with the fundamental functions of Redactive user and group permissions.

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 8.1/10 64-bit (Pro recommended)
- .NET Framework 4.0 minimum

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.

4RE-10-Interview Room setup

If using an interview room for the 4RE system, the agency must provide the following for each 4RE system (future 4RE software versions may support DHCP).

Soft items:

1. Static IP address
2. Subnet mask
3. Gateway

Physical items:

1. Ethernet connection on a 100 Mbps network or better (4RE must be able to connect to the network where the Evidence Library server is on)
2. Physical location to store 4RE, 4RE display, microphone(s) and camera(s)

WatchGuard Video highly recommends a professional CCTV installer is used to install the equipment. Also each interview room should have a dedicated 4RE system (not required, but highly recommended for improved search ability).

If using "WatchCommander" for live streaming and using more than 1 network card, the interview rooms need to be on the same network where the WatchCommander is bound to.

4RE-11-4REM 4RE Motorcycle System Installation

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

V300-01-Configuring V300 WiFi cameras

Prior to first use, each V300 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

V300-02-Create a Configuration

- Through the Evidence Library Administrator you will access V300 Management to complete the following steps.
  - Set up V300 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 V300 with newest firmware (contact customer service for the latest version)
  - Confirm the configuration settings, save each configuration then close V300 Management.

V300-03-Configure V300 Cameras

- Ensure the V300 cameras have the latest firmware version (contact WatchGuard Video Customer Service)
- Connect the V300 USB base into the computer where your Evidence Library agent is located or set up the V300 Transfer Station to connect to your Evidence Library server.
- Dock V300 into the USB base or V300 Transfer Station connected to your Evidence Library software.
- Using Evidence Library software, create and /or assign a configuration and an officer to the docked V300 body camera.

V300-04-Install/Configure Smart PoE Switch in Vehicle (if applicable)

- Applicable if using the V300 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

V300-05-Install Transfer Station (if applicable)

- V300 Transfer Stations are typically shipped preconfigured by the factory based on information provided by the agency. If not see included instructions to configure each.
- Installation of V300 Transfer Station
  - Connect Ethernet cable
  - Connect power cable
  - Attach the Rack mount bracket (if used)

TEST-01- Test Function of WatchGuard system

Test functions of the V300 and Evidence Library system.

TEST-02-Checklist

	Test 4RE USB upload to server via transfer agent on a 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 V300 Wireless upload to server
	Test V300 video upload to server via USB dock and/or V300 Transfer Station
	Validate V300 has correct configuration applied
	Test Evidence Library Login
	Test Evidence Library Video playback
	Test Evidence Library Audio
	Test Exporting Evidence Library video to USB
	Test Exporting Evidence Library video to CD/DVD
	Test Exporting Evidence Library video to Cloudshare

TRAIN-01-Training

WatchGuard Video provides training on the Evidence Library and V300 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 V300 WiFi End User Training (Officers)

WatchGuard Video will provide training (if needed) to parties who will be using the 4RE and V300 WiFi cameras. This will cover how to use the system on a daily basis and how to get through a shift using 4RE and V300 WiFi. Online Training is also available.

This onsite training can be completed in the following scenarios:

- 4RE Basic 5 minutes
- 4RE Full 1 hour
- V300 Basic 5 minutes
- V300 Full 45 minutes
- 4RE/V300 Basic 7 minutes
- 4RE/V300 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 in duration.

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.

SCHEDULE 2

HARDWARE WARRANTY

(*SEE ATTACHED*)

IN-CAR HARDWARE WARRANTY – 5 YEAR PLAN

5 YEAR LIMITED IN-CAR HARDWARE WARRANTY

WatchGuard, Inc., in recognition of its responsibility to provide quality systems, components, and workmanship, 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. A defective component that is repaired or replaced under this limited warranty will be covered for the remainder of the original warranty period. With the purchase of this 5 Year Extended Warranty, where defects in material or workmanship may occur, the following warranty terms and conditions apply:

WARRANTOR – This warranty is granted by WatchGuard, Inc., 415 E. Exchange, Allen, TX 75002-2616, 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.

PARTS AND COMPONENTS COVERED – All parts and components and repair labor of the warranted unit manufactured and/or installed by WatchGuard are covered by this warranty, except those parts and components excluded below.

PARTS AND COMPONENTS NOT COVERED – The Limited Warranty excludes normal wear-and-tear items such as frayed or broken cords, broken connectors, and scratched or broken displays. WatchGuard reserves the right to charge for damages resulting from abuse, improper installation, or extraordinary environmental damage (including damages caused by spilled liquids) to the unit during the warranty period at rates normally charged for repairing such units not covered under the Limited Warranty. In cases where potential charges would be incurred due to said damages, the agency submitting the system for repairs will be notified. Altered, damaged, or removed serial numbers results in voiding this Limited Warranty. If while under the warranty period, it is determined that the WatchGuard system was internally changed, modified, or repair attempted, the system warranty will become null and void.

LIMITED LIABILITY – WatchGuard's liability is limited to the repair or replacement of components found to be defective by WatchGuard. WatchGuard 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. WatchGuard will not be responsible for any removal or re-installation cost of the unit or for damages caused by improper installation.

REMEDY – If, within the duration of this warranty, a unit or component covered by this warranty is determined by WatchGuard to be defective in material or workmanship, WatchGuard shall replace any defective components. Replacement of a defective component(s) pursuant to this warranty

415 E. Exchange • Allen, TX • 75002-2616
Toll Free (800) 605-6734 • Main (972) 423-9777 • Fax (972) 423-9778
www.WatchGuardVideo.com

shall be warranted for the remainder of the warranty period applicable to the system warranty period. WatchGuard will advance ship a replacement unit, or at the request of the customer, ask for the unit to be sent in for repair. In the case of an advanced shipment replacement, WatchGuard will supply a return label with the advance unit, and the customer must return the defect within thirty days.

SHIPPING – When an advanced replacement is sent out, the unit will ship via ground shipping, and WatchGuard will provide a prepaid shipping label to return any defective unit for end users in the continental United States. A serial number is required to be submitted with the request in order to receive an advanced replacement unit. The customer will need to contact WatchGuard's Customer Service Department to request a return material authorization (RMA) number. Failure to return the unit within the thirty-day window will result in the customer being billed the full purchase price of the advance shipped unit.

If the customer requests the unit be sent in for repair, the end user will be responsible for any shipping charges to WatchGuard. WatchGuard will return ship the product to a customer within the continental United States by prepaid ground shipping only. 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'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.

SUPPORT CONTACT INFORMATION

WatchGuard, Inc.

Attn: Customer Service Department
415 E. Exchange
Allen, Texas 75002-2616
(800) 605-6734 Toll Free Main Phone
(972) 423-9777 Main
(972) 423-9778 Fax
www.watchguardvideo.com
support@watchguardvideo.com

415 E. Exchange • Allen, TX • 75002-2616
Toll Free (800) 605-6734 • Main (972) 423-9777 • Fax (972) 423-9778
www.WatchGuardVideo.com

V300 NO-FAULT EXTENDED HARDWARE WARRANTY – 3 YEAR PLAN

WatchGuard, Inc., 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. Any and all No-Fault warranties must be purchased with the initial purchase of the V300 unit, and the V300 No-Fault warranty must also be purchased for all V300 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 V300 Camera Warranty:

WARRANTOR – This warranty is granted by WatchGuard, Inc., 415 E. Exchange, Allen, TX 75002, Telephone: 972-423-9777, Facsimile: 214-383-9661.

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.

PARTS AND COMPONENTS COVERED – The V300 No-Fault warranty covers all parts and components of the V300 Standard, and the V300 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 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 system was internally changed, modified, or repaired.

LIMITED LIABILITY – WatchGuard's liability is limited to the repair or replacement of components. WatchGuard 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.

415 E. Exchange• Allen, TX • 75002
Toll Free (800) 605-6734 • Main (972) 423-9777 • Fax (214) 383-9661
www.WatchGuardVideo.com

REMEDY – If, within the duration of this warranty, a unit or component covered by this warranty is damaged in any way, WatchGuard 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 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, Inc.
Attn: Customer Service Department
415 E. Exchange
Allen, Texas 75002
(800) 605-6734 Toll Free Main Phone
(866) 384-8567 Toll Free Queued Customer Service
(972) 423-9777 Main
(214) 383-9661 Fax
www.watchguardvideo.com
support@watchguardvideo.com

415 E. Exchange• Allen, TX • 75002
Toll Free (800) 605-6734 • Main (972) 423-9777 • Fax (214) 383-9661
www.WatchGuardVideo.com

SCHEDULE 3

SOFTWARE WARRANTY

(*SEE ATTACHED*)

Agreement No. _____

SOFTWARE AS A SERVICE SUBSCRIPTION AGREEMENT
For
EVIDENCELIBRARY.COM

This Software as a Service Agreement (this "**Agreement**"), effective as of June 26, 2020 (the "**Effective Date**"), is by and between WatchGuard, Inc., a Delaware corporation with offices located at 415 Century Parkway, Allen, TX 75013 ("**Provider**", "**we**" or "**us**") and the City of Costa Mesa, a California municipal corporation ("**Customer**" or "**you**").

WHEREAS, Provider provides access to its software-as-a-service offerings to its customers;

WHEREAS, Customer desires to access certain software-as-a-service offerings described herein, and Provider desires to provide Customer access to such offerings, subject to the terms and conditions set forth in this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions.

"**Access Credentials**" means any user name, identification number, password, license or security key, security token, PIN, or other security code, method, technology, or device used, alone or in combination, to verify an individual's identity and authorization to access and use the Services.

"**Action**" means any claim, action, cause of action, demand, lawsuit, arbitration, inquiry, audit, notice of violation, proceeding, litigation, citation, summons, subpoena or investigation of any nature, civil, criminal, administrative, regulatory or other, whether at law, in equity, or otherwise.

"**Affiliate**" of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. The term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract or otherwise/ownership of more than 50% of the voting securities of a Person.

"**Authorized User**" means Customer's employees, consultants, contractors, and agents (i) who are authorized by Customer to access and use the Services under the rights granted to Customer pursuant to this Agreement and (ii) for whom access to the Services has been purchased hereunder.

"**Confidential Information**" has the meaning set forth in Section 9.1.

"**Customer Data**" means information, data, and other content, in any form or medium, that is collected, downloaded, or otherwise received, directly or indirectly from Customer or an Authorized User by or through the Services or that incorporates or is derived from the Processing of such information, data, or content by or through the Services. For the avoidance of doubt, Customer Data does not include Resultant Data or any other information reflecting the access or use of the Services by or on behalf of Customer or any Authorized User.

"**Customer Failure**" has the meaning set forth in Section 4.2.

"**Customer Indemnitee**" has the meaning set forth in Section 12.1.

"**Customer Systems**" means the Customer's information technology infrastructure, including computers, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Customer or through the use of third-party services.

"**Disclosing Party**" has the meaning set forth in Section 9.1.

"**Documentation**" means any manuals, instructions, or other documents or materials that the Provider provides or makes available to Customer in any form or medium and which describe the functionality, components, features, or requirements of the Services or Provider Materials, including any aspect of the installation, configuration, integration, operation, use, support, or maintenance thereof.

"**Fees**" has the meaning set forth in Section 8.1.

"**Force Majeure Event**" has the meaning set forth in Section 15.9.

"**Harmful Code**" means any software, hardware, or other technology, device, or means, including any virus, worm, malware, or other malicious computer code, the purpose or effect of which is to (a) permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner any (i) computer, software, firmware, hardware, system, or network or (ii) any application or function of any of the foregoing or the security, integrity, confidentiality, or use of any data Processed thereby, or (b) prevent Customer or any Authorized User from accessing or using the Services or Provider Systems as intended by this Agreement. Harmful Code does not include any Provider Disabling Device.

"**Indemnitee**" has the meaning set forth in Section 12.3.

"**Indemnitor**" has the meaning set forth in Section 12.3.

"**Initial Term**" has the meaning set forth in Section 14.1.

"**Intellectual Property Rights**" means any and all registered and unregistered rights granted, applied for, or otherwise now or hereafter in existence under or related to any patent, copyright, trademark, trade secret, database protection, or other intellectual property rights laws, and all similar or equivalent rights or forms of protection, in any part of the world.

"**Law**" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree, or other requirement of any federal, state, local, or foreign government or political subdivision thereof, or any arbitrator, court, or tribunal of competent jurisdiction.

"**Losses**" means any and all losses, damages, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

"**Permitted Use**" means any use of the Services by an Authorized User for the benefit of Customer in the ordinary course of its internal business operations.

"**Person**" means an individual, corporation, partnership, joint venture, limited liability entity, governmental authority, unincorporated organization, trust, association, or other entity.

"**Process**" means to take any action or perform any operation or set of operations that the Services are capable of

taking or performing on any data, information, or other content, including to collect, receive, input, upload, download, record, reproduce, store, organize, compile, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate, or make other derivative works or improvements, process, retrieve, output, consult, use, perform, display, disseminate, transmit, submit, post, transfer, disclose, or otherwise provide or make available, or block, erase, or destroy . "**Processing**" and "**Processed**" have correlative meanings.

"**Provider Disabling Device**" means any software, hardware, or other technology, device, or means used by Provider or its designee to disable Customer's or any Authorized User's access to or use of the Services automatically with the passage of time or under the positive control of Provider or its designee.

"**Provider Indemnitee**" has the meaning set forth in Section 12.2.

"**Provider Materials**" means the Services, Specifications, Documentation, and Provider Systems and any and all other information, data, documents, materials, works, and other content, devices, methods, processes, hardware, software, and other technologies and inventions, including any deliverables, technical or functional descriptions, requirements, plans, or reports, that are provided or used by Provider or any Subcontractor in connection with the Services or otherwise comprise or relate to the Services or Provider Systems. For the avoidance of doubt, Provider Materials include Resultant Data and any information, data, or other content derived from Provider's monitoring of Customer's access to or use of the Services, but do not include Customer Data.

"**Provider Personnel**" means all individuals involved in the performance of Services as employees, agents, or independent contractors of Provider or any Subcontractor.

"**Provider Systems**" means the information technology infrastructure used by or on behalf of Provider in performing the Services, including all computers, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Provider or through the use of third-party services.

"**Receiving Party**" has the meaning set forth in Section 9.1.

"**Renewal Term**" has the meaning set forth in Section 14.2.

"**Representatives**" means, with respect to a party, that party's and its Affiliates' employees, officers, directors, consultants, agents, independent contractors, service providers, sublicensees, subcontractors, and legal advisors.

"**Resultant Data**" means data and information related to Customer's use of the Services and/or information compiled from Customer Data that is used by Provider in an aggregate and anonymized manner, for one or more of the following purposes: (i) to compile statistical and performance information related to the provision and operation of the Services; (ii) to provide routine or Customer-requested maintenance, repairs, analytical or diagnostic services related to the Services, Provider Systems or Customer Data; (iii) to ensure compliance with, or provide updates or revisions to, this Agreement, Service Level performance metrics, or the Services, and policies and protocols related thereto; or (iv) to compile analytical and statistical information for purposes of developing and improving our products and services.

"**Scheduled Downtime**" has the meaning set forth in Exhibit B.

"**Service Allocation**" has the meaning set forth in Section 3.4.

"**Service Credit**" has the meaning set forth in Exhibit B.

"**Service Level Failure**" has the meaning set forth in Exhibit B.

"**Services**" means the software-as-a-service offering described in Exhibit A.

"**Specifications**" means the specifications for the Services set forth in Exhibit B.

"**Subcontractor**" has the meaning set forth in Section 2.7.

"**Support Services**" has the meaning set forth in Section 5.4.

"**Term**" has the meaning set forth in Section 14.2.

"**Third-Party Materials**" means materials and information, in any form or medium, including any open-source or other software, documents, data, content, specifications, products, equipment, or components of or relating to the Services that are not proprietary to Provider.

2. Services.

2.1 Access and Use. Subject to and conditioned on your and your Authorized Users' compliance with the terms and conditions of this Agreement, we hereby grant to you a non-exclusive, non-transferable (except in compliance with Section 15.8) right to access and use the Services during the Term, solely for use by Authorized Users in accordance with the terms and conditions herein. Such use is limited to your internal use. We will provide you with Access Credentials as of the Effective Date.

2.2 Documentation License. We hereby grant you a non-exclusive, non-sublicenseable, non-transferable (except in compliance with Section 15.8) license to use the Documentation during the Term solely for your internal business purposes in connection with its use of the Services.

2.3 Service and System Control. Except as otherwise expressly provided in this Agreement, as between the parties:

(a) We have and will retain sole control over the operation, provision, maintenance, and management of the Provider Materials; and

(b) You have and will retain sole control over the operation, maintenance, and management of, and all access to and use of, the Customer Systems, and sole responsibility for all access to and use of the Provider Materials by any Person by or through the Customer Systems or any other means controlled by you or any Authorized User, including any: (i) information, instructions, or materials provided by any of them to the Services or us; (ii) results obtained from any use of the Services or Provider Materials; and (iii) conclusions, decisions, or actions based on such use.

2.4 Reservation of Rights. Nothing in this Agreement grants any right, title, or interest in or to (including any license under) any Intellectual Property Rights in or relating to, the Services, Provider Materials, or Third-Party Materials, whether expressly, by implication, estoppel, or otherwise. All right, title, and interest in and to the Services, the Provider Materials, and the Third-Party Materials are and will remain with us and the respective rights holders in the Third-Party Materials.

2.5 Service Management. Each party shall, throughout the Term, maintain within its organization a service manager to serve as such party's primary point of contact for day-to-day communications, consultation, and decision-making regarding this Agreement. Each service manager shall be responsible for providing all day-to-day consents and approvals on behalf of such party under this Agreement. Each party shall ensure its service manager has the requisite organizational authority, skill, experience, and other qualifications to perform in such capacity.

2.6 Changes. (a) Changes to the Services. We reserve the right, in our sole discretion, to make any changes to the Services and Provider Materials that we deem necessary or useful to: (1) maintain or enhance (i) the quality or delivery of our services to our customers, (ii) the competitive strength of or market for our services, or (iii) the Services' cost efficiency or performance; or (2) to comply with applicable Law. We will notify you of any material change to the Services or Provider Materials.

(b) Changes to this Agreement. We may revise, update or supplement this Agreement from time to time. Any such revision, update or supplement shall become effective immediately. We will notify you of any changes to this Agreement, and your continued use of the Services following your receipt of notice means that you agree to the terms and conditions of this Agreement as revised, updated or supplemented.

2.7 Subcontractors. We may from time to time in our discretion engage third parties to perform Services (each, a "**Subcontractor**").

2.8 Suspension or Termination of Services. We may, directly or indirectly, and by use of a Provider Disabling Device or any other lawful means, suspend, terminate, or otherwise deny your, any Authorized User's, or any other Person's access to or use of all or any part of the Services or Provider Materials, without incurring any resulting obligation or liability, if: (a) we receive a judicial or other governmental demand or order, subpoena, or law enforcement request that expressly or by reasonable implication requires us to do so; or (b) we reasonably believe that: (i) you or any Authorized User have failed to comply with any material term of this Agreement, or accessed or used the Services beyond the scope of the rights granted or for a purpose not authorized under this Agreement or in any manner that does not comply with any material instruction or requirement of the Specifications; (ii) you or any Authorized User are, have been, or are likely (in our reasonable judgment) to be involved in any fraudulent, misleading, or unlawful activities relating to or in connection with any of the Services; or (iii) this Agreement expires or is terminated. If we suspend your right to access the Services you will remain responsible for payment of Fees you incur during the period of suspension and you will not be entitled to Service Credits during the period of suspension. This Section 2.8 does not limit any of our other rights or remedies, whether at law, in equity, or under this Agreement.

3. Use Restrictions; Service Usage and Data Storage.

3.1 Use Restrictions. You shall not, and shall not permit any other Person to, access or use the Services or Provider Materials except as expressly permitted by this Agreement and, in the case of Third-Party Materials, the applicable third-party license agreement. For purposes of clarity and without limiting the generality of the foregoing, you shall not, except as this Agreement expressly permits:

(a) copy, modify, or create derivative works or improvements of the Services or Provider Materials;

(b) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make available any Services or Provider Materials to any Person, including on or in connection with the internet or any time-sharing, service bureau, software-as-a-service, cloud, or other technology or service;

(c) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code of the Services or Provider Materials, in whole or in part;

(d) bypass or breach any security device or protection used by the Services or Provider Materials or access or use the Services or Provider Materials other than by an Authorized User through the use of his or her own then valid Access Credentials;

(e) input, upload, transmit, or otherwise provide to or through the Services or Provider Systems, any information or materials that are unlawful or injurious, or contain, transmit, or activate any Harmful Code;

(f) damage, destroy, disrupt, disable, impair, interfere with, or otherwise impede or harm in any manner the Services, Provider Systems, or Provider's provision of services to any third party, in whole or in part;

(g) remove, delete, alter, or obscure any trademarks, Specifications, Documentation, warranties, or disclaimers, or any copyright, trademark, patent, or other intellectual property or proprietary rights notices from any Services or Provider Materials, including any copy thereof;

(h) access or use the Services or Provider Materials in any manner or for any purpose that infringes, misappropriates, or otherwise violates any Intellectual Property Right or other right of any third party (including by any unauthorized access to, misappropriation, use, alteration, destruction, or disclosure of the data of any other Provider customer), or that violates any applicable Law;

(i) access or use the Services or Provider Materials for purposes of competitive analysis of the Services or Provider Materials, the development, provision, or use of a competing software service or product or any other purpose that is to our detriment or commercial disadvantage; or

(j) otherwise access or use the Services or Provider Materials beyond the scope of or is inconsistent with the authorization granted under this Section 3.1.

3.2 Service Usage. Exhibit A sets forth the subscription terms and Fees for the designated levels of usage and data storage available for Customer Data (each a "**Service Allocation**"). We will use commercially reasonable efforts to notify you in writing if your use of the Services exceeds the storage limits or other use parameters of the Service Allocation set forth in Exhibit A, at which point we may mutually agree to adjust your Service Allocation and corresponding Fee obligations in accordance with applicable Specifications. You acknowledge that exceeding your then-current Service Allocation may result in service degradation for you and other of our customers, and you therefore agree that (a) we have no obligation to allow you to exceed your then-current Service Allocation; and (b) you are not entitled to any Service Level Credits for periods during which your use of the Services exceeds your then-current Service Allocation, regardless of whether the Services fail to meet the availability requirements (as defined in Exhibit B) during such period.

3.3 Data Storage. The Customer Data will be stored in a secure, general purpose storage account in a Microsoft Azure data center ("**Microsoft**" and "**MS Data Center**") that is located within the United States and that will be compliant with the FBI's Criminal Justice Information Services ("**CJIS**") requirements. You agree that we may transfer the Customer Data to the MS Data Center; provided, however, that except as otherwise provided in this Agreement, you shall retain all right, title and interest in and to the Customer Data at all times, wherever located or stored, and whether in transit or at rest.

4. Customer Obligations.

4.1 Customer Systems and Cooperation. You shall at all times during the Term: (a) set up, maintain, and operate in good repair and in accordance with the Specifications all Customer Systems on or through which the Services are accessed or used; (b) provide Provider Personnel with such access to your premises and Customer Systems as is necessary for Provider to perform the Services in accordance with the Availability Requirement and Specifications; (c) provide all cooperation and assistance as we may reasonably request to enable us to exercise our rights and perform our obligations under and in connection with this Agreement; (d) ensure that your use of the Services is in compliance with applicable laws, rules and regulations; (e) set up and enable any hardware or networks that connect to the Services and ensure that all such hardware and networks properly interact with the Services and its hardware and software component parts; (f) maintain responsibility for the Customer Data before it is uploaded to the Services platform; and (g) establish any security settings you deem necessary and appropriate for your network and Customer Data .

4.2 Effect of Customer Failure or Delay. We are not responsible or liable for any delay or failure of performance caused in whole or in part by your delay in performing, or failure to perform, any of your obligations under this Agreement (each, a "**Customer Failure**").

4.3 Corrective Action and Notice. If you become aware of any actual or threatened activity prohibited by Section 3.1, you shall, and shall cause your Authorized Users to, immediately: (a) take all reasonable and lawful measures within your or their respective control that are necessary to stop the activity or threatened activity and to mitigate its effects (including, where applicable, by discontinuing and preventing any unauthorized access to the Services and Provider Materials and permanently erasing from their systems and destroying any data to which any of them have gained

unauthorized access); and (b) notify us of any such actual or threatened activity.

5. Service Levels and Credits.

5.1 Service Levels. Subject to the terms and conditions of this Agreement, we will use commercially reasonable efforts to make the Services Available as set forth in Exhibit B.

5.2 Service Level Failures and Remedies. In the event of a Service Level Failure, we shall issue a credit to you according to the process specified in Exhibit B.

5.3 Scheduled Downtime. We will use commercially reasonable efforts to schedule Scheduled Downtime at the times and according to the processes set forth in Exhibit B.

5.4 Service Support. The Services include our standard customer support services (**"Support Services"**) in accordance with our service support schedule then in effect from time to time.

6. Data Backup and Redundancy. We will take reasonable measures to provide for Customer Data redundancy by providing for three (3) copies of the Customer Data to be maintained in locally redundant storage (**"LRS"**) within the MS Data Center in which the Customer Data resides. At your request, we may provide for geo-redundant storage (**"GRS"**) for replication of the Customer Data in a secondary MS Data Center that is geographically distant from the first MS Data Center. A GRS election is considered an upgrade of the standard LRS account and will require payment of additional Fees and execution of an addendum to this Agreement. You are responsible for implementing and maintaining all such Customer Data backup and disaster recovery processes you deem appropriate for your local computer systems and information technology infrastructure.

7. Security.

7.1 Provider Systems and Security Obligations. Without limiting the representations, warranties and disclaimers in Section 11 or your obligations under Sections 6, 7.4 and 7.5, we will implement reasonable and appropriate measures designed to help you secure the Customer Data against unlawful loss, access or disclosure. However, (i) we are not responsible for the accuracy, completeness or success of any efforts for replication, restoration, or recovery of Customer Data that you or Microsoft may take; and (ii) we are not liable for damage to, or loss or corruption of Customer Data from any cause, including failure of any storage, replication or redundancy capabilities of any MS Data Center(s) in which Customer Data may be located.

7.2 Data Privacy. Subject to the rights granted to us in Section 10.3, we will not access or use Customer Data except as necessary to maintain or provide the Services, or as necessary to comply with applicable Law or a binding order of a court or governmental agency. We will not (a) disclose Customer Data to any government, government agency or third party, or (b) subject to Section 3.2, move Customer Data except as necessary to comply with applicable Law or a binding order of a court or governmental agency. Unless we are prohibited from doing so by applicable Law, we will give you notice of any such legal requirement or order.

7.3 Prohibited Data. You acknowledge that the Services are not designed with security and access management for Processing the following categories of information: (a) data that is classified and or used on the U.S. Munitions list, including software and technical data; (b) articles, services, and related technical data designated as defense articles or defense services; and (c) International Traffic in Arms Regulations (**"ITAR"**) related data (each of the foregoing, **"Prohibited Data"**). You shall not, and shall not permit any Authorized User or other Person to, provide any Prohibited Data to, or Process any Prohibited Data through, the Services, the Provider Systems, or any Provider Personnel. You are solely responsible for reviewing all Customer Data and shall ensure that no Customer Data constitutes or contains any Prohibited Data.

7.4 Customer Control and Responsibility. (a) You have and will retain sole responsibility for: (1) all Customer Data,

including its content and use; (2) all information, instructions, and materials provided by or on your behalf or by or on behalf of any Authorized User in connection with the Services; (3) your information technology infrastructure, including computers, software, databases, electronic systems (including database management systems), and networks, whether operated directly by you or through the use of third-party services ("**Customer Systems**"); (4) the security and use of Access Credentials by you and your Authorized Users; and (5) all access to and use of the Services and Provider Materials directly or indirectly by or through the Customer Systems or your or your Authorized Users' Access Credentials, with or without your knowledge or consent, including all results obtained from, and all conclusions, decisions, and actions based on, such access or use.

(b) You understand and agree that all transactions you undertake using the Services are between you and the parties with which you are transacting. Certain features and capabilities of the Services may link you to or provide you with access to third-party content such as networks, websites, and information databases that we do not operate or control ("**Third-Party Services**"). We are not responsible for your contact with, access to or use of any Third-Party Services or any losses or damage you may experience from such contact, use or access, unless such losses or damages directly resulted from our material breach of our obligations under this Agreement.

7.5 Access and Security. You agree to employ all physical, administrative, and technical controls, screening and security procedures and other safeguards necessary to: (a) securely administer the distribution and use of all Access Credentials and protect against any unauthorized access to or use of the Services; and (b) control the content and use of Customer Data, including the uploading or other provision of Customer Data for Processing by the Services.

8. Fees and Payment

8.1 Fees. You agree to pay us the fees set forth in Exhibit A ("**Fees**") in accordance with this Section 8.

8.2 Taxes. All Fees and other amounts payable by you under this Agreement are exclusive of taxes and similar assessments. Without limiting the foregoing, you are responsible for all sales, use and excise taxes, and any other similar taxes, duties, and charges of any kind imposed by any federal, state, or local governmental or regulatory authority on any amounts payable by you hereunder, other than any taxes imposed on our income.

8.3 Late Payment. If you fail to make any payment when due, then, in addition to all other remedies that may be available:

(a) you shall reimburse us for all costs we incur in collecting any late payments, including attorneys' fees, court costs, and collection agency fees; and

(b) if such failure continues for thirty (30) days following written notice thereof, we may suspend performance of the Services until all past due amounts and interest thereon have been paid, without incurring any obligation or liability to you or any other Person by reason of such suspension.

8.4 No Deductions or Setoffs. All amounts payable to us under this Agreement shall be paid by you in full without any setoff, recoupment, counterclaim, deduction, debit, or withholding for any reason (other than Service Credits issued pursuant to Section 5.2 or any deduction or withholding of tax as may be required by applicable Law).

9. Confidentiality.

9.1 Confidential Information. In connection with this Agreement each party (as the "**Disclosing Party**") may disclose or make available Confidential Information to the other party (as the "**Receiving Party**"). Subject to Section 9.2, "**Confidential Information**" means information in any form or medium (whether oral, written, electronic, or other) that

the Disclosing Party considers confidential or proprietary, including information consisting of or relating to the Disclosing Party's technology, trade secrets, know-how, business operations, plans, strategies, customers, and pricing, and information with respect to which the Disclosing Party has contractual or other confidentiality obligations, in each case whether or not marked, designated, or otherwise identified as "confidential".

9.2 Exclusions. Confidential Information does not include information that the Receiving Party can demonstrate by written or other documentary records: (a) was rightfully known to the Receiving Party without restriction on use or disclosure prior to such information's being disclosed or made available to the Receiving Party in connection with this Agreement; (b) was or becomes generally known by the public other than by the Receiving Party's or any of its Representatives' noncompliance with this Agreement; (c) was or is received by the Receiving Party on a non-confidential basis from a third party that, to the Receiving Party's knowledge, was not or is not, at the time of such receipt, under any obligation to maintain its confidentiality; or (d) the Receiving Party can demonstrate by written or other documentary records was or is independently developed by the Receiving Party without reference to or use of any Confidential Information.

9.3 Protection of Confidential Information. As a condition to being provided with any disclosure of or access to Confidential Information, the Receiving Party shall:

(a) not access or use Confidential Information other than as necessary to exercise its rights or perform its obligations under and in accordance with this Agreement;

(b) except as may be permitted by and subject to its compliance with Section 9.4, not disclose or permit access to Confidential Information other than to its Representatives who: (i) need to know such Confidential Information for purposes of the Receiving Party's exercise of its rights or performance of its obligations under and in accordance with this Agreement; (ii) have been informed of the confidential nature of the Confidential Information and the Receiving Party's obligations under this Section 9.3; and (iii) are bound by confidentiality and restricted use obligations at least as protective of the Confidential Information as the terms set forth in this Section 9;

(c) safeguard the Confidential Information from unauthorized use, access, or disclosure using at least the degree of care it uses to protect its similarly sensitive information and in no event less than a reasonable degree of care;

(d) promptly notify the Disclosing Party of any unauthorized use or disclosure of Confidential Information and take all reasonable steps to prevent further unauthorized use or disclosure; and

(e) ensure its Representatives' compliance with, and be responsible and liable for any of its Representatives' non-compliance with, the terms of this Section 9.

(f) notwithstanding any other provisions of this Agreement, the Receiving Party's obligations under this Section 9 with respect to any Confidential Information that constitutes a trade secret under any applicable Law will continue until such time, if ever, as such Confidential Information ceases to qualify for trade secret protection under one or more such applicable Laws other than as a result of any act or omission of the Receiving Party or any of its Representatives.

9.4 Compelled Disclosures. If the Receiving Party or any of its Representatives is compelled by applicable Law to disclose any Confidential Information then, to the extent permitted by applicable Law, the Receiving Party shall: (a) promptly, and prior to such disclosure, notify the Disclosing Party in writing of such requirement so that the Disclosing Party can seek a protective order or other remedy or waive its rights under Section 9.3; and (b) provide reasonable assistance to the Disclosing Party in opposing such disclosure or seeking a protective order or other limitations on disclosure. If the Disclosing Party waives compliance or, after providing the notice and assistance required under this Section 9.4, the Receiving Party remains required by Law to disclose any Confidential Information, the Receiving Party shall disclose only that portion of the Confidential Information that, on the advice of the Receiving Party's legal counsel, the Receiving Party is legally required to disclose.

10. Intellectual Property Rights.

10.1 Provider Materials. We retain all right, title, and interest in and to the Provider Materials, including all Intellectual Property Rights therein and, with respect to Third-Party Materials, the applicable third-party providers own all right, title, and interest, including all Intellectual Property Rights, in and to the Third-Party Materials. You have no right, license, or authorization with respect to any of the Provider Materials except as expressly set forth in Section 2.1 or the applicable third-party license, in each case subject to Section 3.1. We expressly retain all other rights in and to the Provider Materials. In furtherance of the foregoing, you hereby unconditionally and irrevocably grant to us an assignment of all right, title, and interest in and to the Resultant Data, including all Intellectual Property Rights relating thereto.

10.2 Customer Data. As between you and us, you are and will remain the sole and exclusive owner of all right, title, and interest in and to all Customer Data, including all Intellectual Property Rights relating thereto, subject to the rights and permissions granted in Section 10.3.

10.3 Consent to Use Customer Data. You hereby irrevocably grant all such rights and permissions in or relating to Customer Data as are necessary or useful to us, our Subcontractors, and Provider Personnel to (a) provide the Services, (b) enforce this Agreement, (c) compile the Resultant Data, and (d) exercise such rights as we, our Subcontractors, and Provider Personnel may require to perform our obligations hereunder.

11. Representations and Warranties.

11.1 Provider Representations, Warranties, and Covenants. We represent, warrant, and covenant to you that we will perform the Services using personnel of required skill, experience, and qualifications and in a professional and workmanlike manner in accordance with generally recognized industry standards for similar services and will devote adequate resources to meet our obligations under this Agreement.

11.2 Customer Representations, Warranties, and Covenants. You represent, warrant, and covenant to us that you own or otherwise have and will maintain the necessary rights and consents in and relating to the Customer Data so that, as received by us and Processed in accordance with this Agreement, they do not and will not infringe, misappropriate, or otherwise violate any Intellectual Property Rights, or any privacy or other rights of any third party or violate any applicable Law.

11.3 DISCLAIMER OF WARRANTIES. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN SECTIONS 11.1 AND 11.2, ALL SERVICES AND PROVIDER MATERIALS ARE PROVIDED "AS IS." WE SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, WE MAKE NO WARRANTY OF ANY KIND THAT THE SERVICES OR PROVIDER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET YOUR OR ANY OTHER PERSON'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR FREE. ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN YOU AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

12. Indemnification.

12.1 Provider Indemnification. We agree to indemnify, defend, and hold harmless you and your elected officials, officers, directors, employees, agents, permitted successors, and permitted assigns (each, a "**Customer Indemnitee**") from and against any and all Losses incurred by you or a Customer Indemnitee resulting from any Action by a third party (other than your Affiliate) that your use or an Authorized User's use of the Services (excluding Customer Data and Third-Party Materials) in accordance with this Agreement (including the Specifications) infringes or misappropriates such third party's U.S. Intellectual Property Rights. The foregoing obligation does not apply to the extent that the alleged infringement arises from:

(a) Third-Party Materials or Customer Data;

(b) access to or use of the Provider Materials in combination with any hardware, system, software, network, or other materials or service that we did not provide or that was not specified for your use in the Documentation;

(c) modification of the Provider Materials other than: (i) by or on behalf of us; or (ii) with our written approval in accordance with our written specification;

(d) failure to timely implement any modifications, upgrades, replacements, or enhancements made available to you by or on behalf of us; or

(e) act, omission, or other matter described, in Section 12.2(a), Section 12.2(b), Section 12.2(c), or Section 12.2(d), whether or not the same results in any Action against or Losses by any Provider Indemnitee.

12.2 Customer Indemnification. You agree to indemnify, defend, and hold harmless us and our Subcontractors and Affiliates, and each of our and their respective officers, directors, employees, agents, successors, and assigns (each, a "**Provider Indemnitee**") from and against any and all Losses incurred by such Provider Indemnitee resulting from any Action by a third party (other than an Affiliate of a Provider Indemnitee) to the extent that such Losses arise out of or result from, or are alleged to arise out of or result from:

(a) Customer Data, including any Processing of Customer Data by us or on our behalf in accordance with this Agreement;

(b) any other materials or information (including any documents, data, specifications, software, content, or technology) provided by you or on behalf of you or any Authorized User, including our compliance with any specifications or directions provided by or on behalf of you or any Authorized User to the extent prepared without any contribution by us;

(c) allegation of facts that, if true, would constitute your breach of any of your representations, warranties, covenants, or obligations under this Agreement; or

(d) gross negligence or more culpable act or omission (including recklessness or willful misconduct) by you, any Authorized User, or any third party on behalf of you or any Authorized User, in connection with this Agreement.

12.3 Indemnification Procedure. Each party shall promptly notify the other party in writing of any Action for which such party believes it is entitled to be indemnified pursuant to Section 12.1 or Section 12.2, as the case may be. The party seeking indemnification (the "**Indemnitee**") shall cooperate with the other party (the "**Indemnitor**") at the Indemnitor's sole cost and expense. The Indemnitor shall promptly assume control of the defense and shall employ counsel reasonably acceptable to the Indemnitee to handle and defend the same, at the Indemnitor's sole cost and expense. The Indemnitee may participate in and observe the proceedings at its own cost and expense with counsel of its own choosing. The Indemnitor shall not settle any Action on any terms or in any manner that adversely affects the rights of any Indemnitee without the Indemnitee's prior written consent, which shall not be unreasonably withheld or delayed. If the Indemnitor fails or refuses to assume control of the defense of such Action, the Indemnitee shall have the right, but no obligation, to defend against such Action, including settling such Action after giving notice to the Indemnitor, in each case in such manner and on such terms as the Indemnitee may deem appropriate.

12.4 Mitigation. If any of the Services or Provider Materials are, or in our opinion are likely to be, claimed to infringe, misappropriate, or otherwise violate any third-party Intellectual Property Right, or if you or any Authorized User's use of the Services or Provider Materials is enjoined or threatened to be enjoined, we may, at our option and sole cost and expense:

(a) obtain the right for you to continue to use the Services and Provider Materials materially as contemplated by this Agreement;

(b) modify or replace the Services and Provider Materials, in whole or in part, to seek to make the Services and Provider Materials (as so modified or replaced) non-infringing, while providing materially equivalent features and functionality, in which case such modifications or replacements will constitute Services and Provider Materials, as applicable, under this Agreement; or

(c) by written notice to you, terminate this Agreement with respect to all or part of the Services and Provider Materials, and require that you immediately cease any use of the Services and Provider Materials or any specified part or feature thereof.

12.5 Sole Remedy. THIS SECTION 12 SETS FORTH YOUR SOLE REMEDIES AND OUR SOLE LIABILITY AND OBLIGATION FOR ANY ACTUAL, THREATENED, OR ALLEGED CLAIMS THAT THE SERVICES AND PROVIDER MATERIALS OR ANY SUBJECT MATTER OF THIS AGREEMENT INFRINGES, MISAPPROPRIATES, OR OTHERWISE VIOLATES ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

13. Limitations of Liability.

13.1 EXCLUSION OF DAMAGES. IN NO EVENT WILL WE OR ANY OF OUR LICENSORS, SERVICE PROVIDERS, OR SUPPLIERS BE LIABLE UNDER OR IN CONNECTION WITH THIS AGREEMENT OR ITS SUBJECT MATTER UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, FOR ANY: (a) LOSS OF PRODUCTION, USE, BUSINESS, REVENUE, OR PROFIT OR DIMINUTION IN VALUE; (b) IMPAIRMENT, INABILITY TO USE OR LOSS, INTERRUPTION OR DELAY OF THE SERVICES, OTHER THAN FOR THE ISSUANCE OF ANY APPLICABLE SERVICE CREDITS PURSUANT TO SECTION 5.2, (c) LOSS, DAMAGE, CORRUPTION OR RECOVERY OF DATA, OR BREACH OF DATA OR SYSTEM SECURITY, (d) LOSS OF GOODWILL OR REPUTATION, OR (e) CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED, OR PUNITIVE DAMAGES, REGARDLESS OF WHETHER SUCH PERSONS WERE ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE, AND NOTWITHSTANDING THE FAILURE OF ANY AGREED OR OTHER REMEDY OF ITS ESSENTIAL PURPOSE.

13.2 CAP ON MONETARY LIABILITY. IN NO EVENT WILL OUR AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER ARISING UNDER OR RELATED TO BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR ANY OTHER LEGAL OR EQUITABLE THEORY, EXCEED THE TOTAL AMOUNTS PAID TO US UNDER THIS AGREEMENT IN THE 12-MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM. THE FOREGOING LIMITATIONS APPLY EVEN IF ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

14. Term and Termination.

14.1 Initial Term. The initial term of this Agreement commences as of the Effective Date and, unless terminated earlier pursuant any of this Agreement's express provisions, will continue in effect until three (3) years from such date (the "**Initial Term**").

14.2 Renewal Term. Upon expiration of the Initial Term this Agreement will renew for successive one (1) year terms upon written agreement of the parties (each a "**Renewal Term**" and, collectively, together with the Initial Term, the "**Term**").

14.3 Termination. In addition to any other express termination right set forth elsewhere in this Agreement:

(a) we may terminate this Agreement, effective on written notice to you, if you: (i) fail to pay any amount when

due hereunder, and such failure continues more than 30 days after we provide you with written notice thereof; or (ii) breach any of your obligations under Section 3.1, Section 7.3, or Section 9;

(b) either party may terminate this Agreement, effective on 30 days written notice to the other party, if the other party materially breaches this Agreement, and such breach: (i) is incapable of cure; or (ii) being capable of cure, remains uncured 30 days after the non-breaching party provides the breaching party with written notice of such breach; and

(c) either party may terminate this Agreement, effective immediately upon written notice to the other party, if the other party: (i) becomes insolvent or is generally unable to pay, or fails to pay, its debts as they become due; (ii) files or has filed against it, a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency Law; (iii) makes or seeks to make a general assignment for the benefit of its creditors; or (iv) applies for or has appointed a receiver, trustee, custodian, or similar agent appointed by order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business.

14.4 Effect of Termination or Expiration. Upon any expiration or termination of this Agreement, except as expressly otherwise provided in this Agreement:

(a) all rights, licenses, consents, and authorizations granted by either party to the other hereunder will immediately terminate;

(b) we agree to immediately cease all use of any Customer Data or your Confidential Information and (i) promptly return to you, or at your written request destroy, all documents and tangible materials containing, reflecting, incorporating, or based on Customer Data or your Confidential Information; and (ii) subject to Section 14.5, permanently erase all Customer Data and your Confidential Information from all systems we directly or indirectly control; provided that, for clarity, our obligations under this Section 14.4(b) do not apply to any Resultant Data;

(c) you agree to immediately cease all use of any Services or Provider Materials and (i) promptly return to us, or at our written request destroy, all documents and tangible materials containing, reflecting, incorporating, or based on any Provider Materials or our Confidential Information, and (ii) permanently erase all Provider Materials and our Confidential Information from all systems you directly or indirectly control;

(d) notwithstanding anything to the contrary in this Agreement, with respect to information and materials then in its possession or control: (i) the Receiving Party may retain the Disclosing Party's Confidential Information; (ii) we may retain Customer Data; and (iii) you may retain Provider Materials, in the case of each of subclause (i), (ii) and (iii), in its then current state and solely to the extent and for so long as required by applicable Law; (iv) we may also retain Customer Data in our backups, archives, and disaster recovery systems until such Customer Data is deleted in the ordinary course pursuant to Section 14.5; and (v) all information and materials described in this Section 14.4(d) will remain subject to all confidentiality, security, and other applicable requirements of this Agreement;

(e) we may disable your and your Authorized User's access to the Services and the Provider Materials;

(f) if you terminate this Agreement pursuant to Section 14.3(b), you will be relieved of any obligation to pay any Fees attributable to the period after the effective date of such termination and we will: (i) refund to you Fees paid in advance for Services that we have not performed as of the effective date of termination; and (ii) pay to you any unpaid Service Credits to which you may be entitled; and

(g) if we terminate this Agreement pursuant to Section 14.3(a) or Section 14.3(b), all Fees that would have become payable had the Agreement remained in effect until expiration of the Term will become immediately due and payable, and you agree to pay such Fees, together with all previously-accrued but not yet paid Fees on receipt of our invoice therefor.

14.5 Return of Customer Data.

(a) During the Term. You may retrieve Customer Data at any time during the Term.

(b) Upon Termination. We will not delete Customer Data for a period of 60 days following termination (the "**Post - Termination Retention Period**"). During the Post-Termination Retention Period you may retrieve Customer Data only if you have paid all amounts due under this Agreement. We will make the Customer Data available to you in a non-proprietary format and assist you with retrieval during the Post-Termination Retention Period. You agree to pay our reasonable expenses, on a time and materials basis, for the assistance we provide in assisting you with retrieval of the Customer Data. WE HAVE NO OBLIGATION TO MAINTAIN THE CUSTOMER DATA BEYOND THE POST-TEMINATION RETENTION PERIOD, AND WE MAY THEREAFTER DELETE THE CUSTOMER DATA, UNLESS LEGALLY PROHIBITED FROM DOING SO, OR UNLESS AN EXTENSION OF THE POST-TERMINATION RETENTION PERIOD IS AGREED TO. Upon your request and provided that you have paid all amounts due under this Agreement, we may agree to a reasonable extension of the Post-Termination Retention Period. If we are legally prevented from deleting the Customer Data beyond the Post-Termination Retention Period you agree to pay all costs associated with continued storage until the Customer Data is either deleted or retrieved by you.

14.6 Surviving Terms. The provisions set forth in the following sections, and any other right or obligation of the parties in this Agreement that, by its nature, should survive termination or expiration of this Agreement, will survive any expiration or termination of this Agreement: Section 3.1, Section 9, Section 11.4, Section 12, Section 13, Section 14.4, Section 14.5, this Section 14.6, and Section 15.

15. Miscellaneous.

15.1 Further Assurances. Upon a party's reasonable request, the other party shall, at the requesting party's sole cost and expense, execute and deliver all such documents and instruments, and take all such further actions, as may be necessary to give full effect to this Agreement.

15.2 Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, employment, or fiduciary relationship between the parties, and neither party shall have authority to contract for or bind the other party in any manner whatsoever.

15.3 Public Announcements. Neither party shall issue or release any announcement, statement, press release, or other publicity or marketing materials relating to this Agreement or, unless expressly permitted under this Agreement, otherwise use the other party's trademarks, service marks, trade names, logos, domain names, or other indicia of source, association, or sponsorship, in each case, without the prior written consent of the other party, which consent shall not be unreasonably withheld; provided, however, that we may, without your consent, include or display your name, logo and other indicia in our lists of current or former customers in promotional and marketing materials.

15.4 Notices. Any notice, request, consent, claim, demand, waiver, or other communications under this Agreement have legal effect only if in writing and addressed to a party as follows (or to such other address or such other person that such party may designate from time to time in accordance with this Section 15.4):

If to Provider:
415 Century Parkway, Allen, TX 75013
Facsimile: (214) 383-9661
Email: brian.greene@motorolasolutions.com
Attention: Brian Greene

If to Customer:	City of Costa Mesa Police Department 99 Fair Drive, Costa Mesa, CA 92626 Facsimile: (714) 754-4911 Email: jlapointe@costamesaca.gov Attention: Joyce LaPointe, Lieutenant
Copy to:	City of Costa Mesa 77 Fair Drive Costa Mesa, CA 92626 Attn: Finance Dept. | Purchasing

Notices sent in accordance with this Section 15.4 will be deemed effectively given: (a) when received, if delivered by hand, with signed confirmation of receipt; (b) when received, if sent by a nationally recognized overnight courier, signature required; (c) when sent, if by facsimile or email (in each case, with confirmation of transmission), if sent during the addressee's normal business hours, and on the next business day, if sent after the addressee's normal business hours; and (d) on the third day after the date mailed by certified or registered mail, return receipt requested, postage prepaid.

15.5 Interpretation. For purposes of this Agreement: (a) the words "include," "includes," and "including" are deemed to be followed by the words "without limitation"; (b) the word "or" is not exclusive; (c) the words "herein," "hereof," "hereby," "hereto," and "hereunder" refer to this Agreement as a whole; (d) words denoting the singular have a comparable meaning when used in the plural, and vice-versa; and (e) words denoting any gender include all genders. Unless the context otherwise requires, references in this Agreement: (x) to sections, exhibits, schedules, and attachments mean the sections of, and exhibits, schedules, and attachments attached to, this Agreement; (y) to an agreement, instrument, or other document means such agreement, instrument, or other document as amended, supplemented, and modified from time to time to the extent permitted by the provisions thereof; and (z) to a statute means such statute as amended from time to time and includes any successor legislation thereto and any regulations promulgated thereunder. The parties intend this Agreement to be construed without regard to any presumption or rule requiring construction or interpretation against the party drafting an instrument or causing any instrument to be drafted. The exhibits, schedules, and attachments referred to herein are an integral part of this Agreement to the same extent as if they were set forth verbatim herein.

15.6 Headings. The headings in this Agreement are for reference only and do not affect the interpretation of this Agreement.

15.7 Entire Agreement. This Agreement, together with any other documents incorporated herein by reference, constitutes the sole and entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Agreement, the related exhibits, schedules, and attachments and any other documents incorporated herein by reference, the following order of precedence governs: (a) first, this Agreement, excluding its exhibits, schedules, and attachments; (b) second, the exhibits, schedules, and attachments to this Agreement as of the Effective Date; and (c) third, any other documents incorporated herein by reference.

15.8 Assignment. Neither party may assign or transfer this Agreement or its rights or obligations hereunder without the prior written consent of the other party; provided, that we may assign or transfer this Agreement or any of our rights or obligations hereunder without your consent in connection with (a) the sale of all or substantially all of our stock or assets; (b) a merger or acquisition, whether we are the surviving or disappearing entity; (c) a corporate reorganization; or (d) transfer to a subsidiary or affiliate entity. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective successors and permitted assigns.

15.9 Force Majeure.

(a) No Breach or Default. In no event will either party be liable or responsible to the other party, or be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement, (except for any obligations to make payments), when and to the extent such failure or delay is caused by any circumstances beyond such party's reasonable control (a "**Force Majeure Event**"), including acts of God, flood, fire, earthquake or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Agreement, national or regional emergency, plague, epidemic, pandemic, outbreaks of infectious disease or any other public health crisis, including quarantine or other government-imposed restrictions, strikes, labor stoppages or slowdowns or other industrial disturbances, passage of Law or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota, or other restriction or prohibition or any complete or partial government shutdown, or national or regional shortage of adequate power or telecommunications or transportation. Either party may terminate this Agreement if a Force Majeure Event affecting the other party continues substantially uninterrupted for a period of 30 days or more.

(b) Affected Party Obligations. In the event of any failure or delay caused by a Force Majeure Event, the affected party shall give prompt written notice to the other party stating the period of time the occurrence is expected to continue and use commercially reasonable efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

15.10 No Third-Party Beneficiaries. This Agreement is for the sole benefit of the parties hereto and their respective successors and permitted assigns and nothing herein, express or implied, is intended to or shall confer upon any other Person any legal or equitable right, benefit, or remedy of any nature whatsoever under or by reason of this Agreement.

15.11 Amendment and Modification; Waiver. No amendment to or modification of or rescission, termination, or discharge of this Agreement is effective unless it is in writing and signed by each party. No waiver by any party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the party so waiving. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Agreement will operate or be construed as a waiver thereof; nor shall any single or partial exercise of any right, remedy, power, or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

15.12 Severability. If any term or provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the parties hereto shall negotiate in good faith to modify this Agreement so as to effect the original intent of the parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

15.13 U.S. Government Rights. The Services are provided to the U.S. government as "commercial items", "commercial computer software", commercial computer software documentation", and "technical data", with the same rights and restrictions generally applicable to the Services. If you are using the Services on behalf of the U.S. government and these terms fail to meet the U.S. government's needs or are inconsistent in any respect with federal law, you agree to immediately discontinue use of the Services. The terms as "commercial items", "commercial computer software", commercial computer software documentation", and "technical data" as used in this Section 15.13 have the same meaning as in the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement.

15.14 Governing Law. This Agreement is governed by and construed in accordance with the internal laws of the state in which your principal headquarters is located. The United Nations Convention for International Sale of Goods does not apply to this Agreement.

15.15 Dispute Resolution. Any dispute or claim relating in any way to this Agreement, your use of the Services, or the Provider Materials will be resolved by binding arbitration, rather than in court. The Federal Arbitration Act and federal

arbitration law apply to this Agreement. There is no judge or jury in arbitration, and court review of an arbitration award is limited. However, an arbitrator can award on an individual basis the same damages and relief as a court (including injunctive and declaratory relief or statutory damages), and must follow the terms of this Agreement as a court would. A party who intends to seek arbitration must first send to the other party a notice of dispute, which must include a description of the nature and basis of the claims that the party is asserting and the relief sought. If you and we are unable to resolve the claims described in the notice within 30 days after the notice is sent, you or we may initiate arbitration proceedings. To begin an arbitration proceeding, you must send a letter requesting arbitration and describing your claim to our registered agent Capitol Corporate Services, Inc., P.O. Box 1831, Austin, TX 78767. If we begin an arbitration proceeding, we will send notice to you at the address in Section 15.4. The arbitration will be conducted by the American Arbitration Association ("AAA") under its rules, which are available at www.adr.org or by calling 1-800-778-7879. Payment of filing, administration and arbitrator fees will be governed by the AAA's rules. Attorneys' fees and costs may be awarded by the arbitrator as provided by the AAA's rules. Arbitration will be conducted in the city in which your principal headquarters office is located or another location that we mutually agree to. If the relief sought is $10,000 or less you or we may elect to have the arbitration conducted by telephone or based solely on written submissions, subject to the arbitrator's discretion to require an in-person hearing. WE AND YOU AGREE THAT EACH OF US MAY BRING CLAIMS AGAINST THE OTHER ONLY ON AN INDIVIDUAL BASIS AND NOT AS A PLAINTIFF OR CLASS MEMBER OR REPRESENTATIVE IN ANY PURPORTED CLASS, AND THAT ANY DISPUTE RESOLUTION PROCEEDINGS WILL BE CONDUCTED ONLY ON AN INDIVIDUAL BASIS AND NOT IN A CLASS, CONSOLIDATED OR REPRESENTATIVE ACTION. If for any reason a claim proceeds in court rather than in arbitration we and you waive any right to a jury trial. We and you both agree that you or we may bring suit in court to enjoin infringement or other misuse of Intellectual Property Rights.

15.16. Counterparts. This Agreement may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. A signed copy of this Agreement delivered by facsimile, email, or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date first above written.

CITY OF COSTA MESA

By: _____

Name Printed: LoriAnn Farrell Harrison

Title: City Manager

WATCHGUARD, INC.

By: _____

Name Printed: TROY MONTGOMERY

Title: DIRECTOR OF SALES

ATTEST:

Brenda Green 7-17-2020

Brenda Green
City Clerk

APPROVED AS TO FORM:

Kimberly Hall Barlow
City Attorney

EXHIBIT A

SERVICES, SERVICE ALLOCATION and FEES

The Services: Cloud-based, software-as-a-service evidence management data storage platform using Microsoft Azure Government Cloud Storage services fully-hosted in one or more secure Microsoft data centers.

Service Allocations and Fees:

Plan I (Unlimited)

Unlimited Storage available for customers with data retention policies as follows:

- a one-year storage period for non-evidentiary recordings;
- a 10-year storage period for evidentiary recordings; and
- the video recording policy is event-based (i.e. policies that do not require officers to record entire shifts)

For purposes of this Plan, the term "evidentiary recordings" refers to data having relevance to a legal trial or regulatory hearing.

Plan costs are based on a per-device basis, which means that the Plan does not have a per-user fee, meaning that an unlimited number of users can access data using the Services.

This Plan also features unlimited data sharing, using the Company's CLOUD-SHARE on-premises software.

Plan cost is based upon the customer's choice of two options: (a) a per-device fee of $495 per contract year for assigned (i.e., individual use) devices, or (b) a per-device fee of $695 per contract year for pooled (i.e., shared) devices. There is also a $0.03 per GB per device per month for storage that does not meet these requirements.

When the actual usage across all devices averages less than 700 GB per device over a contract year, at the end of each calendar year the customer will be rebated an amount equal to $0.03 per GB per month ($0.36 per GB per calendar year) for each GB under 700 GB actually used per device. The rebate is offered in cash or as a credit against future charges for the Services.

EXHIBIT B

SERVICE LEVEL AGREEMENT

(See attached)

SERVICE LEVEL AGREEMENT
FOR
EVIDENCELIBRARY.COM

LAST UPDATED: February 14, 2019

This Service Level Agreement for EvidenceLibrary.com (this "SLA") is a part of the Software as a Service Agreement between WatchGuard, Inc. ("Company" "us" or "we") and users of EvidenceLibrary.com ("Customer" or "you") (the "Agreement" and the "Services"). Capitalized terms used but not defined in this SLA have the meaning given to them in the Agreement. This SLA applies to the Services, but not to any other services we provide to you or to any of our on-premises software that is a part of the Services, or any Third-Party Materials that you use in connection with the Services, unless specifically provided to the contrary in this SLA or the Agreement.

We may change the terms of this SLA from time to time during the term of your subscription; however, we will provide you with prior notice of any material changes we make. If you renew your subscription the form of SLA that is current at the time will apply during the renewal term.

SERVICE COMMITMENT

We will use commercially reasonable efforts to make the Services available with the Monthly Uptime Percentage defined below during any Service Period (our "Service Level Commitment"). If we do not meet the Service Level Commitment for any Service Period you may be entitled to a Service Credit, as described below.

DEFINITIONS

"**Downtime**" means the total number of minutes in any Service Period during which the Services are Unavailable. Downtime does not include time during which the Services are unavailable for Scheduled Downtime or as the result of one or more Exclusions.

"**Incident**" means an event or series of events resulting in Downtime.

"**Maximum Available Minutes**" means the number of minutes during a Service Period, less Scheduled Downtime, that the Services are required to be available for your access and use in accordance with the Specifications.

"**Monthly Uptime Percentage**" means, for any Service Period, Maximum Available Minutes less Downtime, divided by the Maximum Available Minutes multiplied by 100, as follows:

Monthly Uptime Percentage = ((Maximum Available Minutes – Downtime)/Maximum Available Minutes)) x 100

If you have used the Services for only part of a Service Period, the Services are assumed to be 100% available for that part of the Service Period in which the Services were not used (for example, if you begin to use the Services in the middle of a month). Monthly Uptime Percentage calculations do not include downtime that results from Scheduled Downtime or an Exclusion.

"**Scheduled Downtime**" means any Downtime (a) of which you are notified at least three (3) days in advance, or (b) during a standard maintenance window, according to a maintenance schedule we will publish from time to time.

"Service Credit" means a dollar credit, as calculated herein, that we may credit back to your account under the conditions set forth below. A Service Credit is based on a percentage, as stated below, of the Service Fee for the Service Period for which the Service Credit is approved.

"Emergency Downtime" means any Downtime for which you may receive less than 24-hour notification period. This emergency maintenance may be performed at any time, with or without notice, as deemed necessary by us. Emergency Downtime falling outside of Scheduled or Planned Downtime may be eligible for Service Credit.

"Service Fee" means the fee that you actually pay for the Services during a Service Period.

"Service Level" means a performance metric that we agree to meet in the delivery of the Services. A **"Service Level Failure"** means a material failure of the Services to meet the Maximum Available Minutes requirement.

"Service Period" means one calendar month.

"Unavailable" means that all connection requests to the Services fail during a one (1) minute period such that you or your End Users cannot upload or access files.

"Low Priority" means a request for information or software defects with acceptable workaround.

"Medium Priority" means an isolated issue (one agency, small subset of events) that prevents import, search, or export of events or cases.

"High Priority" means a pervasive issue (multiple agencies, large subsets of events) that prevents import, search, or export of events or cases, missing events, system performance out of Customer SLA. Customer designated emergency.

"Response time" means the amount of time between when a Customer first creates an incident report (which includes leaving a phone message, sending an email, or using an online ticketing system) and when the provider actually responds.

"Resolution time" means the amount of time between when the Customer first creates an incident report and when that problem is actually solved, workaround provided, or for issues requiring software changes is placed in to the future development backlog.

SERVICE LEVELS AND SERVICE CREDITS

The following Service Levels apply to your use of the Services:

Monthly Uptime Percentage	Service Credit as Percentage of Service Fee
< 99.90%	10%
< 99.00%	25%

SERVICE ESCALATION PROCESS

The table below provides typical response time expectations for each support level (Tier 1, Tier 2, and Engineering Operations) based on the incident priority levels (Low, Medium, High):

Priority	Response (Minutes)	Tier 1 Support (Minutes)	Tier 2 Support (Minutes)	Engineering Operations(Minutes)	Total(Minutes)	Total Resolution (Hours)
Low	60	960	1440	2880	5340	**89**
Medium	60	480	720	1440	2700	**45**
High	60	240	240	720	1260	**21**

Below table provides the incident response and resolution targets based on service hours, priority, and support team involved.

Service hours	Origin	Support Team	Priority	Service Response	Resolution or Escalation
Business Hours	Direct Call/ Email/ Automated Alert	Tier 1	LOW	< 60 minutes of initial call	< 16 hours
Business Hours	Escalation	Tier 2	LOW	< 4 hours of escalation	< 24 hours
Business Hours	Escalation	Engineering Operations	LOW	< 8 hours of escalation	< 48 hours
Business Hours	Escalation	Engineering Hold	LOW		Entered in to Backlog
Business Hours	Direct Call/Email	Tier 1	MEDIUM	< 60 minutes of initial call	< 8 hours
Business Hours	Escalation	Tier 2	MEDIUM	< 2 hours of escalation	< 12 hours
Business Hours	Escalation	Engineering Operations	MEDIUM	< 4 hours of escalation	< 24 hours
Business Hours	Escalation	Engineering Hold	MEDIUM		Prioritized in to Backlog
Business Hours	Direct Call/ Email/ Automated Alert	Tier 1	HIGH	< 60 minutes of initial call	< 4 hours
Business Hours	Escalation	Tier 2	HIGH	< 4 hours of escalation	< 4 hours
Business Hours	Escalation	Engineering Operations	HIGH	< 2 hours of escalation	< 12 hours
Business Hours	Escalation	Engineering Hold	HIGH		Prioritized in to next release
After Hours	Direct Call	Tier 1	LOW	Deferred to Business Hours	
After Hours	Direct Call	Tier 1	MEDIUM, HIGH	< 70 minutes of initial call	< 4 hours
After Hours	Direct Call	Tier 2	MEDIUM HIGH	<4 hours of escalation	< 8 hours
After Hours	Direct Call	Engineering Operations	HIGH	<2 hours of escalation	< 12 hours

TERMS

I. SERVICE CREDITS

Service Credits are your only remedy for unavailability of the Services under this SLA and the Agreement. You may not offset a Service Fee for any performance or availability issues. Service Credits issued for any Service Period will not under any circumstances exceed the Service Fee for that Service Period.

To be eligible for a Service Credit, your claim must be received by us, in the required form, no later than the end of the second Service Period following the Service Period in which the incident(s) occurred. Your failure to make a timely request will disqualify you from receiving a Service Credit.

We will apply a Service Credit only against future Service Fees, and we will issue Service Credits only if the credit amount for the Service Fee is greater than one dollar (US$1). Service Credits do not entitle you to a refund or cash payment. Service Credits may not be applied against any other account or service you may have with us. You must be in compliance with the Agreement to receive a Service Credit.

II. SERVICE CREDIT CLAIMS AND PAYMENT

To apply for a Service Credit, you must open a support case by going to support.watchguardvideo.com or by contacting customer support at 1800-605-6734 and providing us with all of the information we need to investigate and validate your claim. The information we need will include, but may not be limited to, (i) the dates and times of the Unavailability incident(s); (ii) request logs documenting the incident(s) and corroborating the claimed Unavailability (any PII or CJI information contained or described in logs should be redacted prior to submission); and (iii) details of your efforts to resolve the incident(s) at the time of occurrence.

We will review the submitted information and make a good faith determination of whether a Service Credit is due. If we determine that a Service Credit is due, we will process your claim within thirty (30) days of our determination and apply the Service Credit to the next Service Fee.

III. EXCLUSIONS

For purposes of calculating Maximum Available Minutes, the following are Exclusions for which the Services shall not be considered Unavailable nor any Service Level Failure be deemed to occur in connection with any failure to meet Maximum Available Minutes for any Service Period, or your inability to access or use the Services that is due, in whole or in part, to any:

(a) act or omission by you to access or use the Services, or use of Access Credentials that does not strictly comply with the Agreement;
(b) Customer Failure;
(c) Internet connectivity failure;
(d) causes beyond our reasonable control, such as a Force Majeure Event, or the performance of any third-party hosting provider or communications or internet service provider;
(e) failure, interruption, outage, inadequate bandwidth, or other problem with any software, hardware, system, network, or facility that we have not provided or authorized pursuant to the Agreement (other than third-party software or equipment within our direct control);
(f) Scheduled Downtime or backups to the Services;
(g) disabling, suspension, or termination of the Services pursuant to Section 2.8 of the Agreement; or
(h) separate instances of unavailability of the Services of less than ten (10) minutes duration each.

REDACTIVE END USER LICENSE AGREEMENT

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 WatchGuard, Inc.

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;

415 E. Exchange Parkway • Allen, TX • 75002
Toll Free (800) 605-6734 • Main (972) 423-9777 • Fax (972) 423-9778
www.WatchGuardVideo.com

SCHEDULE 4

MOBILE VIDEO SYSTEM COMBINED COST PROPOSAL

(*SEE ATTACHED*)

415 E. Exchange Pkwy.
Allen, TX 75002
P - (972) 423-9777
F - (214) 383-9661

Mobile Video System Combined Cost Proposal

HARDWARE COST BREAKDOWN

Item #	Description	Qty.	Unit Price	TAX	Unit Price w/ Tax	Extended Price
IN-CAR CAMERA HARDWARE						
1	4RE High Definition In-Car Video System *Includes:* *Mini Zoom Camera* *Separate Back Seat Camera* *Integrated GPS* *Crash detection* *DVR with Integrated 200GB automotive grade hard drive* *16GB USB drive* *4.3" touch screen remote display control panel* *Cabin microphone* *4RE, V300, Smart PoE Switch*	60	$4,070.00	7.75%	$ 4,385.43	$263,125.50
2	MikroTik Configured Wireless Kit, 4RE In-Car 802.11n, 5GHz Includes: Radio, Antenna, PoE, 2-10' Ethernet Cables)	60	$200.00	7.75%	$ 215.50	$12,930.00
3	HD Panoramic Camera Upgrade Replaces the Zero Sightline Front Camera with a HD Panoramic	60	$200.00	7.75%	$ 215.50	$12,930.00
BODY CAMERA HARDWARE						
4	V300 Wearable Camera *Includes: One (1) Battery, Mounting Hardware and One (1) year warranty on*	100	$805.00	7.75%	$ 867.39	$86,738.75
5	V300 8 Bay Ethernet Transfer Station	13	$1,200.00	7.75%	$ 1,293.00	$16,809.00
6	V300 Rechargeable Battery	100	$95.00	7.75%	$ 102.36	$10,236.25
7	V300, USB Charge and Upload Docking Base	20	$95.00	7.75%	$ 102.36	$2,047.25
REDACTIVE SOFTWARE, HARDWARE & WARRANTIES						
8	Redactive Redaction Software, Enterprise, Single Seat License	1	$5,995.00	0.00%	$ 5,995.00	$5,995.00
9	Redactive Tower, Xeon 16 Core, 480GB SSD, Blu Ray DVDRW, 16GB RAM	1	$4,000.00	7.75%	$ 4,310.00	$4,310.00
10	Software Maintenance, REDACTIVE, 3-Year Bundle (Months 1-	1	$2,795.00	0.00%	$ 2,795.00	$2,795.00
11	Warranty, Redactive Tower Workstation, Extended Warranty to	1	$650.00	0.00%	$ 650.00	$650.00

WARRANTIES AND MAINTENANCE						
12	Warranty, 4RE, In-Car, 1st Year (Months 1-12)	60	$0.00	0.00%	$ -	$0.00
13	Warranty, 4RE, In-Car, 2nd Year (Months 13-24)	60	$25.00	0.00%	$ 25.00	$1,500.00
14	Warranty, 4RE, In-Car, 3rd Year (Months 25-36)	60	$75.00	0.00%	$ 75.00	$4,500.00
15	Warranty, 4RE, In-Car, 4th Year (Months 37-48)	60	$150.00	0.00%	$ 150.00	$9,000.00
16	Warranty, 4RE, In-Car, 5th Year (Months 49-60)	60	$275.95	0.00%	$ 275.95	$16,557.00
17	V300 Warranty, 1st Year (Months 1-12)	100	$0.00	0.00%	$ -	$0.00
18	Warranty, V300, 3 Year No-Fault *Replaces standard warranty and must be purchased up front*	100	$425.00	0.00%	$ 425.00	$42,500.00
IMPLEMENTATION SERVICES						
19	System Configuration - 1st Location *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*	1	$2,500.00	0%	$2,500.00	$2,500.00
20	4RE System Installation, In-Car (per Unit Charge) - QUOTED	60	$650.00	0%	$650.00	$39,000.00
21	Access Point Installation	3	$500.00	0%	$500.00	$1,500.00
			SOLUTION TOTAL			$535,623.75

FULLY HOSTED CLOUD STORAGE OPTION

Item #	Description	Qty.	Unit Price	TAX	Unit Price w/ Tax	Extended Price
22	WiFi Access Point, Configured, 802.11n, 5GHz, Sector (included	3	$250.00	7.75%	$ 269.38	$808.13
23	ELC Upload Applicance *1U Rack Mounted Chassis, Dual Power Supply, SM X11SSH-LN4F SOC 1151 C236 64G 4XGBE I210-AT 8XSATA3 M.2, Intel XEON E3-1225V67, 16GB (2X8GB), DDR4 2400 ECC, 2x256GB SSD, 6GB/s, RAID 1 array, 256GB usable, 4-4TB Hard Drives, 7,200 RPM Enterprise, RAID 10 array, 8TB usable, Microsoft Windows 10 IOT Enterprise. 5-Year Full Service (On-Site or reimbursed) Warranty*	1	$4,500.00	7.75%	$ 4,848.75	$4,848.75
24	Unlimited Plan - Assigned Devices	100	$495.00	0.00%	$ 495.00	$49,500.00
25	Unlimited Plan - Pooled Devices	60	$695.00	0.00%	$ 695.00	$41,700.00
					First Year Total	$96,856.88
					5-YEAR STORAGE TOTAL	**$461,656.88**

5-YEAR TOTAL COST OF OWNERSHIP	$997,280.63