SERVICES CONTRACT
Between
FRANKLIN COUNTY BOARD OF COMMISSIONERS
And
WatchGuard Video, Inc.

This Services Contract entered into by and between WatchGuard Video, Inc., a Corporation having its principal place of business located at 415 E. Exchange Parkway, Allen, Texas 75002 ("WatchGuard") and the Franklin County Board of Commissioners on behalf of the Franklin County Sheriff's Office ("County") for the procurement of the WatchGuard Solution (defined below) pursuant to, and under the authority of Resolution No.________ dated ___________, 2022.

The scope of this Contract and the SaaS Agreement attached hereto as Exhibit 2, is based on the offerings available under the Sourcewell contract #010720 awarded to WatchGuard Video, Inc effective February 24, 2020, as amended effective September 8, 2020 and collectively referred to herein as "Sourcewell Contract". This Sourcewell Contract is effective through February 21, 2024.

For the mutual considerations herein specified, County and WatchGuard have agreed and do hereby agree as follows:

Section 1 Definitions

- **"Contract," "Services Contract"** means this Services Contract.
- **"Configuration"** means processes by which WatchGuard will install and configure the WatchGuard Solution to the County's requirements.
- **"Data"** means those terms as defined in Section 2.03.1 of the SaaS Agreement.
- "**Defect"** means a failure of the Watchguard hardware or Watchguard Solution to conform to the Functional Descriptions, or their functional equivalent. Future functionality may be updated, modified, or otherwise enhanced through Watchguard's future releases as available or identified in Product Newsletters.
- **"Disaster"** means an event that causes an unrecoverable failure of an operations center, such as fire, flood, etc. A system outage does not constitute a Disaster.
- **"Documentation"** means any online or written documentation related to the use or functionality of the WatchGuard Solution that is provided or otherwise made available to the County, including instructions, user guides, manuals, and other training or self-help documentation.
- **"Effective Date"** means the last signature date set forth in the signature block.
- **"Equipment"** means the hardware provided by WatchGuard.
- **"Final Acceptance"** means the timeline set forth in Section 8.04 of the Services Contract.
- **"Force Majeure"** means an event beyond the reasonable control of the County or WatchGuard, including, without limitation, governmental action, war, riot or civil commotion, fire, natural disaster, pandemic, epidemic, or any other cause that could not with reasonable diligence be foreseen or prevented by the County or WatchGuard.
- **"Functional Description"** means the technical and functional specifications as set forth in Exhibit 1 to the Services Contract, and technical and functional specifications as may be updated, modified and enhanced through WatchGuard's future releases as available or identified in Product Newsletters.
- **"Hosting Solution"** means a WatchGuard Solution provided to and used by the County as a service that includes at least one mobile video product(s) and WatchGuard Software hosted in a data center.

- **"Integrations"** means the connection of new and existing systems to the WatchGuard Software to facilitate the exchange of Data, developed by WatchGuard and identified in the Statement of Work and Investment Summary.
- **"Investment Summary"** means the agreed upon cost proposal for the products and services attached to the Services Contract as Exhibit 1.
- **"Licensed Software"** means the software which is either pre-installed on Equipment or installed on County-provided equipment and licensed to County by WatchGuard for a perpetual or other defined licensed term.
- **"Product"** means, collectively, the Equipment, Licensed Software and Subscription Software.
- **"Product Newsletters"** means technical information relating to the Product, including product releases, cancellations, training and other information as more specifically set forth at the following website: https://www.motorolasolutions.com/en_us/support/technical-product-newsletter.html.
- **"Proper Invoice"** is defined as an itemized invoice that states which WatchGuard deliverable(s) in the milestone payment schedule in Exhibit 1 are being billed, and is otherwise free of defects, discrepancies, errors, or other improprieties. A Proper Invoice should include the invoice remittance address, as designated in the Contract, as well as the name and address of WatchGuard, the billing period, and the cost of the deliverables completed.
- **"SaaS Agreement"** means the Software as a Service Agreement attached to the Services Contract as Exhibit 2.
- **"SaaS Fees"** means the fees for the SaaS Services identified in Exhibit 1 to the Services Contract.
- **"SaaS Services"** means software as a service consisting of system administration, system management, and system monitoring activities that WatchGuard performs for the WatchGuard Software, and includes the right to access and use the WatchGuard Software, receive maintenance and support on the WatchGuard Software, including downtime resolution under the terms of the SLA, and Data storage and archiving pursuant to the terms of the SaaS Agreement. SaaS Services do not include support of an operating system or hardware, support outside of WatchGuard normal business hours, or training, consulting, or other professional services.
- **"Services"** means one-time services (implementation and configuration services as more specifically set forth in Exhibit 1 to this Contract). Services does not include SaaS Services.
- **"SLA"** means the service level agreement, which details certain responsibilities of the parties related to the WatchGuard Solution and the Hosting Solution. The SLA is attached hereto as Exhibit A to the SaaS Agreement.
- **"Solution Host"** means the data center where WatchGuard Software is hosted.
- **"Statement of Work"** means the Services and SaaS Services as governed by the Services Contract and SaaS Agreement, respectively, and outlined in Exhibit 1 to the Services Contract.
- **"Subscription Software"** means licenses of cloud-based software as a service products and other software which is either preinstalled on Equipment or installed on County-provided equipment, but licensed to County by WatchGuard on a subscription basis for the County's own use in accordance with the SaaS Agreement.
- **"Support Call Process"** means the support call processes available to the County and all Authorized Users (as defined in the SaaS Agreement) who access and use the WatchGuard Solution. WatchGuard's current Support Call Process is attached as Exhibit B to the SaaS Agreement.
- **"WatchGuard Software"** means WatchGuard's Subscription Software, including any Integrations, or other related interfaces identified in the Investment Summary that is hosted in a data center and provided to the County as a Service. The WatchGuard Software may also include embedded third-party software that WatchGuard is licensed to embed in WatchGuard proprietary software and sublicense to the County.
- **"WatchGuard Solution"** means the WatchGuard Software and the Hosting Solution on which the software is installed, as designed and implemented by WatchGuard.

Section 2 Administrative Requirements

This Contract consists of the terms and conditions contained herein, the exhibits listed below, and any resolutions and purchase orders made pursuant to this Contract.

Any inconsistency in this Contract shall be resolved by giving precedence in the following order:

(1) The signed Contract;
(2) Exhibit 1 – Statement of Work and Investment Summary; Exhibit 2 – SaaS Agreement, including all exhibits attached thereto; Exhibit 3 - Non-Discrimination / Equal Opportunity Affidavit; Exhibit 4 – Delinquent Personal Property Tax Affidavit; and Exhibit 5 – Franklin County Board of Commissioners Travel Policy;
(3) Sourcewell contract #010720 and any amendments or addenda thereto, included herein by reference.

Section 3 Contract Pricing and Delivery of Services

The total cost of the Contract is not to exceed $158,102.17. Any changes to the requirements of the specifications or need for additional funding must be mutually agreed to by both parties and approved under a contract modification by the Franklin County Board of Commissioners.

Each party's performance shall be in accordance with the terms and conditions of this Contract.

WatchGuard shall provide the Services and training on the WatchGuard Solution as more fully described in Exhibits 1-5 attached hereto. WatchGuard shall advise the County to ensure that the County can configure the County's infrastructure, hardware, and software so it is compatible with the WatchGuard Solution as further described in the SaaS Agreement. Within a timeframe agreed to by both parties following Contract award, WatchGuard and the County shall complete the project plan that is mutually acceptable to both parties. WatchGuard will provide the key personnel positions/roles identified in Exhibit 1. The County shall have the opportunity to meet and provide input on proposed WatchGuard project manager and key personnel. WatchGuard shall make reasonable efforts to collaborate with any third party vendors contracted by the County.

Each party agrees it shall make reasonable efforts to complete the work for the services in accordance with the project plan referenced in Exhibit 1. In any circumstance, WatchGuard shall immediately inform the County Project Manager in writing of any delays and any assistance needed from the County to address any such delay.

In providing the Services, WatchGuard agrees to commit the time and efforts of the key personnel and the key personnel shall work closely with the County's project team as further outlined in Exhibit 1. Issues related to personnel and staffing shall be addressed through the escalation process established through the Project Management Plan. Notwithstanding the provisions set forth in Exhibit 1, the parties recognize that diversions of key personnel may occur either for reasons within the control of WatchGuard or for reasons beyond the reasonable control of WatchGuard. In either case, WatchGuard must replace diverted key personnel in a timely manner reasonably acceptable to the County, subject to the following:

(a) Diversion for Reasons within the Control of WatchGuard

Prior to diversion of any key personnel, WatchGuard shall notify the County's Project Manager in writing reasonably in advance and shall submit the justification for such diversion, as well as resumes of proposed substitutes in sufficient detail to enable the County to evaluate the impact on the project and provide the County's Project Manager with an opportunity to interview the proposed replacement. The County has the right to approve the replacement of key personnel, and such approval shall not be unreasonably withheld or delayed. The replacement shall be engaged with the project a minimum of 10 business days before the diverted key personnel actually leaves. Said overlap period is intended to provide for the continuity of WatchGuard's installation work. WatchGuard further agrees that in no event shall the departure of the key personnel impact the price due hereunder.

(b) Diversion for Reasons beyond the Control of WatchGuard

For key personnel who resign, become ill, or otherwise leave the project for reasons beyond the control of WatchGuard, WatchGuard shall notify the County Project Manager in writing as far in advance as possible and shall submit a justification for such diversion, as well as resumes of proposed substitutes, in sufficient detail to enable the County to evaluate the impact on the project and provide the County's Project Manager with an opportunity to telephonically interview the proposed replacement. The County has the right to approve of the replacement for the key personnel, such approval not to be unreasonably withheld or delayed. WatchGuard will make diligent efforts to place a substitute key personnel as soon as possible. WatchGuard further agrees that in no event shall the departure of the key personnel impact the price due hereunder.

Section 4 Term of Contract

The term of this Contract shall begin upon the Effective Date and remain in effect until the Contract is fully performed and Final Acceptance of the project is completed in accordance with the mutually agreed timeline in Exhibit 1, or until terminated by either party in accordance with the termination language in this Contract; provided, however, that the agreement(s) attached as Exhibit 1-5, and attachments thereto, shall continue in effect in accordance with their respective terms.

Except as provided in the SaaS Agreement (Exhibit 2), there are no extension options provided under this Contract, nor are any price increases permitted.

Section 5 Miscellaneous Terms

Section 5.01 Standard of Care

WatchGuard shall discharge its respective obligations under the Contract with that level of reasonable care which a similarly situated business would exercise under similar circumstances and for any transactions involving monies due the County. WatchGuard represents and warrants the following to the County:

(a) It (1) is duly incorporated, organized, and validly existing under the laws of, and in good standing with its state of incorporation; (2) has full authority to grant the County the rights granted in this Contract; and (3) has all requisite power and authority to execute and deliver, and to perform all of its obligations under this Contract.

(b) It shall execute any and all documents or contracts with third parties in its name and shall not represent itself as conducting business on behalf of the County or any of its agencies.

(c) It has filed all tax returns (federal, state, and local) required to be filed and has paid all taxes shown thereon to be due and all property taxes due, including interest and penalties, if any.

(d) It is in compliance in all material respects with all laws, regulations, and requirements applicable to its business and has obtained all authorizations, consents, approvals, orders, licenses, exemptions from, and has accomplished all filings or registrations or qualifications with, any court or governmental authority that are necessary for the transaction of its business.

(e) Subject to the disclaimers and exclusions below, WatchGuard represents and warrants that (a) Services will be provided in a good and workmanlike manner and will conform in all material respects to the Functional Descriptions in Exhibit 1; and (b) for a period of ninety (90) days commencing upon the Service completion date for one-time Services, the Services will be free of material defects in materials and workmanship. Other than as set forth in subsection (a) above, recurring Services are not warranted but rather will be subject to the requirements of the SaaS Agreement. WatchGuard provides other express warranties for WatchGuard-manufactured equipment, WatchGuard-owned software products, and certain Services. Such express warranties are included in the Exhibit 1. Such representations and warranties will apply only to the applicable product or service that is the subject of such SaaS Agreement.

(f) Warranty Claims; Remedies. To assert a warranty claim, County must notify WatchGuard in writing of the claim prior to the expiration of any warranty period set forth in this Contract. Upon receipt of such claim, WatchGuard will investigate the claim and use commercially reasonable efforts to repair or replace any confirmed materially non-conforming Product or re-perform any non-conforming Service, as agreed to by the parties. Such remedies are County's sole and exclusive remedies for WatchGuard's breach of a warranty. WatchGuard's warranties are extended by WatchGuard to County only, and are not assignable or transferrable.

(g) Pass-Through Warranties. Notwithstanding any provision of this Contract to the contrary, WatchGuard will have no liability for third-party software or hardware provided by WatchGuard; provided, however, that to the extent offered by third-party providers of software or hardware and to the extent permitted by law, WatchGuard will pass through express warranties provided by such third parties. To the extent that pass-through warranties exist under this Contract, Watchguard shall assist the County in making any pass-through warranty claim or will make the claim on behalf of the County, as needed.

(h) WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS AND PASS-THROUGH WARRANTIES IN THIS CONTRACT, PRODUCTS AND SERVICES PURCHASED HEREUNDER ARE PROVIDED "AS IS". WARRANTIES SET FORTH IN THE CONTRACT ARE THE COMPLETE WARRANTIES FOR THE PRODUCTS AND SERVICES AND WATCHGUARD DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND QUALITY. WATCHGUARD DOES NOT REPRESENT OR WARRANT THAT USE OF THE PRODUCTS AND SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR FREE OF SECURITY VULNERABILITIES.

Section 5.02 Affirmative Covenants

Until the termination or expiration of this Contract, WatchGuard shall:

(a) Maintain its existence and continue to be a duly incorporated legal entity that is organized and validly existing under the laws of its incorporation and duly qualified to do business in the State of Ohio to the extent required by applicable law.

(b) Give notice to the County, within ten days of WatchGuard learning thereof, of any litigation involving a claim for damages in excess of $100,000 affecting or relating to WatchGuard's performance hereunder or the services required under this Contract.

(c) Promptly notify the County if:

(i) WatchGuard learns of the occurrence of any material event which constitutes, or, with the passage of time, the giving of notice or otherwise, will constitute, a default under this Contract together with a detailed statement by a duly authorized representative specifying the nature thereof and what action WatchGuard is taking or proposes to take with respect thereto;

(ii) WatchGuard receives any notice of default from, or the taking of any other action by, the holder(s) of any promissory note, debenture or other evidence of indebtedness of WatchGuard, together with a detailed statement by WatchGuard's duly authorized representative specifying the notice given or other action taken by such holder(s) and the nature of the claimed default and what action WatchGuard is taking or proposes to take with respect thereto;

(iii) WatchGuard learns of the existence of any legal, judicial, or regulatory proceedings affecting WatchGuard or any of its properties or assets in which the amount involved is material and is not covered by insurance or which, if adversely determined, would cause a material adverse change in the business, prospects, profits, properties, assets, or condition (financial or otherwise) of WatchGuard; or

(iv) There shall occur or exist any other event or condition causing a material adverse change in the business, prospects, profits, properties, assets, or condition (financial or otherwise) of WatchGuard.

Section 5.03 General Indemnification

WatchGuard will defend, indemnify, and hold harmless the County's and the County's agents, officials, and employees from and against any and all third party claims, losses, liabilities, damages, costs, and expenses (including reasonable attorney's fees and costs) for (1) personal injury, death or direct damage to tangible property to the extent caused by WatchGuard's negligence, gross negligence or willful misconduct, or (2) WatchGuard's violation of a law applicable to WatchGuard's performance under this Contract. The County must notify WatchGuard promptly in writing of the claim and give WatchGuard sole control over the defense of the suit and all negotiations for its settlement or compromise. The County agrees to provide WatchGuard with reasonable assistance, cooperation, and information in defending the claim at WatchGuard's expense.

Section 5.04 Intellectual Property Infringement.

WatchGuard will defend County against any third-party claim alleging that a WatchGuard-developed or manufactured Product or Service (the "**Infringing Product**") infringes a United States patent, copyright, or trade secret of any third party ("**Infringement Claim**"), and WatchGuard will pay all damages finally awarded against County by a court of competent jurisdiction for an Infringement Claim, or agreed to in writing by WatchGuard in settlement of an Infringement Claim. WatchGuard's duties under this **Section 5.04 – Intellectual Property Infringement** are conditioned upon: (a) County promptly notifying WatchGuard in writing of the Infringement Claim; (b) WatchGuard having sole control of the defense of the suit and all negotiations for its settlement or compromise; and (c) County cooperating with WatchGuard and, if requested by WatchGuard, providing reasonable assistance in the defense of the Infringement Claim at WatchGuard's expense.

5.04.1 If an Infringement Claim occurs, or in WatchGuard's opinion is likely to occur, WatchGuard may at its option and expense: (a) procure for County the right to continue using the Infringing Product; (b) replace or modify the Infringing Product so that it becomes non-infringing; or (c) grant County (i) a pro-rated refund of any amounts pre-paid for the Infringing Product (if the Infringing Product is a software Product, i.e., Licensed Software or Subscription Software) or (ii) a credit for the Infringing Product, less a reasonable charge for depreciation (if the Infringing Product is Equipment, including Equipment with embedded software).

5.04.2 In addition to the other damages disclaimed under this Contract, WatchGuard will have no duty to defend or indemnify County for any Infringement Claim that arises from or is based upon: (a) County Data, County-Provided Equipment (as defined in Section 2.12(d) of the SaaS Agreement), Non-WatchGuard Content (as defined in Section 5 of the SaaS Agreement), or third-party equipment, hardware, software, data, or other third-party materials; (b) the combination of the Product or Service with any products or materials not provided by WatchGuard; (c) a Product or Service designed, modified, or manufactured in accordance with County's designs, specifications, guidelines or instructions and not otherwise approved by WatchGuard; (d) a modification of the Product or Service by a party other than WatchGuard; (e) use of the Product or Service in a manner for which the Product or Service was not designed or that is inconsistent with the terms of this Contract; or (f) the failure by County to use or install an update to the Product or Service that is intended to correct the claimed infringement, except to the extent that WatchGuard is responsible for making or publishing such update to the Product or Service. In no event will WatchGuard's liability resulting from an Infringement Claim extend in any way to any payments due on a royalty basis, other than a reasonable royalty based upon revenue derived by WatchGuard from County from sales or license of the Infringing Product.

5.04.3 This **Section 5.04 – Intellectual Property Infringement** provides County's sole and exclusive remedies and WatchGuard's entire liability in the event of an Infringement Claim. For clarity, the rights and remedies provided in this Section are subject to, and limited by, the restrictions set forth in **Section 9.04 – Limitation of Liability** below.

Section 5.05 Ethics

WatchGuard agrees that it shall take reasonable steps to ensure that its owners, and employees do not voluntarily acquire any personal interest, direct or indirect, which is incompatible or in conflict with the discharge and fulfillment of his or her functions and responsibilities with respect to the carrying out of said work and shall comply with the applicable provisions of the Ohio ethics laws.

Section 5.06 Subcontracting

WatchGuard confirms that it will be the primary contractor who will be performing the work under the Contract. WatchGuard may use subcontractors for portions of the work under the Contract, but WatchGuard will remain the primary contractor and will remain liable for all work performed hereunder regardless of whether performed directly by it or by a subcontracted entity. Prior to the Effective Date, WatchGuard provided the County with a list of subcontractors it currently uses.

WatchGuard shall not use any subcontractor who has been subject to action that limits the subcontractor's right to do business with the local, state, or federal government. The County reserves the right to deny use of a subcontractor(s) if the County determines that WatchGuard will not be the primary contractor who will be performing the work under the Contract.

Section 5.07 Binding Effect/No Assignment

This Contract shall be binding on, and shall be for the benefit of, either County or WatchGuard successor(s) or permitted assign(s). Neither party will assign any of its rights under this Contract without the other party's prior written consent. Except WatchGuard may, without the prior written consent of the County, assign the Contract in its entirety to the surviving entity of any merger or consolidation or to any purchaser of substantially all of WatchGuard's assets. Following any such assignment, the County may enter into a novation agreement with assignee acceptable to the County. The parties hereto understand that the County is legally prohibited from making payment to any entity other than WatchGuard unless the aforementioned novation contract is executed by the County and assignee. The County may assert against an assignee any claim or defense County had against WatchGuard under this Contract.

WatchGuard shall notify the County as soon as possible, but no later than 60 days, after converting into, merging, or consolidating with or selling or transferring substantially all of its assets or business to another corporation, person, or entity.

Section 5.08 Record Keeping

WatchGuard will keep all financial records consistent with Generally Accepted Accounting Principles (GAAP) during the period covered by the Contract and is required to provide the Franklin County Purchasing Department, Franklin County Board of Commissioners, or their designated representative, authorized representatives (for the Contractor), and any person or agency instrumentally involved in providing financial support for the Contract work access and the right to examine any directly pertinent books or records for the purpose of verifying performance in accordance with the terms of this Contract ("WatchGuard Records"). In no circumstances will WatchGuard be required to create or maintain documents not kept in the ordinary course of WatchGuard's business operations, nor will WatchGuard be required to disclose any information, including but not limited to product cost data, which it considers confidential or proprietary to WatchGuard.

The County may audit WatchGuard's Records relating directly to the Contract once per year on ten business (10) days' advance notice.

Section 5.09 Insurance Requirements

(a) During the course of performing services under this Contract, WatchGuard agrees to maintain the following levels of insurance:

(i) Commercial General Liability of $5,000,000 per occurrence with $5,000,000 general aggregate;

(ii) Automobile Liability of $1,000,000 combined single limit;

(iii) Professional Liability including Cyber Insurance of $5,000,000 per claim and aggregate. Throughout the contract period, WatchGuard must maintain cyber breach insurance that shall include; third party liability coverage for loss or disclosure of data, including electronic data, network security failure, unauthorized access and/or use or other intrusions, infringement of any intellectual property rights (except patent infringement and trade secret misappropriation) unintentional breach of contract, negligence or breach of duty to use reasonable care, breach of any duty of confidentiality, invasion of privacy, or violation of any other legal protections for personal information, defamation, libel, slander, commercial disparagement, negligent transmission of computer virus, ransomware, worm, logic bomb, or Trojan horse or negligence in connection with denial of service attacks, or negligent misrepresentation. WatchGuard will notify the County immediately if WatchGuard's insurance coverage is reduced or terminated;

(b) Workers' Compensation complying with applicable statutory requirements; and WatchGuard shall provide the County with a certificate of insurance identifying the County as a certificate holder within a commercially reasonable timeframe after the Effective Date. Additionally, WatchGuard shall include the County as an additional insured to its Commercial General Liability and Automobile Liability policies. That additional insured status will be reflected on the certificate of insurance WatchGuard provides the County after the Effective Date. WatchGuard agrees that the insurance will be primary on claims for which WatchGuard is responsible. Copies of WatchGuard's insurance policies are only available in the event of a disputed or litigated claim during discovery period. Watchguard's required insurance shall (i) apply as primary and non-contributory to any insurance or program of self-insurance that may be maintained by the County and (ii) contain waivers of subrogation on all coverage except Professional Liability/Cyber Liability insurance.

(c) During the term of this Contract and any renewal thereto, WatchGuard, and any agent of WatchGuard, at its sole cost and expense, shall maintain the required insurance coverage as described in the Contract. County may require WatchGuard to provide respective certificate(s) of insurance in order to verify coverage. Failure to provide a requested certificate within a seven (7) calendar day period may be considered as default.

Section 5.10 Performance Bond

WatchGuard shall provide and maintain a performance bond ("Bond") in the amount of 100% of the total cost of the Services Contract and the SaaS Agreement within ten (10) business days after execution of this Contract.

Section 5.11 County Assistance

The County acknowledges that the implementation of the WatchGuard Solution, and the ability to meet project deadlines and other milestones, is a cooperative effort requiring the time and resources of County personnel, as well as WatchGuard's personnel. The County agrees to use all good-faith efforts to cooperate with and assist WatchGuard as may be reasonably required to meet the agreed upon project deadlines and other milestones for implementation. This cooperation includes at least the County working with WatchGuard to schedule the implementation-related services outlined in this Contract.

Section 6 Reserved

Section 7 Fee Payment Schedule, Invoicing, Payment Due Date, and Taxes

Section 7.01 Fee Payment Schedule

WatchGuard will invoice the County in accordance with the milestone payment schedule set forth in the Investment Summary (Exhibit 1).

Section 7.02 Invoicing

The County agrees to set up an ACH payment account to ensure timely electronic payment to WatchGuard.

(a) WatchGuard will provide the County with electronic payment information within five (5) business days following the Effective Date.

(b) Not Used

(c) Not Used

(d) WatchGuard will provide a Proper Invoice upon completion and County's acceptance of mutually agreed upon deliverables and in accordance with the related milestone payment schedule outlined in Exhibit 1. WatchGuard will be required to submit invoices electronically, by mail, sent by courier, or sent as an attachment to an email to the bill to address identified in the purchase orders used to issue orders against this Contract. WatchGuard's Federal Tax Identification Number should appear on all statements and invoices. Failure to provide a Proper Invoice will be cause for rejection of the invoice with a written notice stating the deficiencies. Payment will be delayed until the deficiencies are corrected and a Proper Invoice is submitted, which will then be paid in accordance with Section 7.03.

Section 7.03 Payment Due Date

(a) The County only processes an invoice for payment after delivery and mutually agreed upon deliverables and related milestone payment schedule. The County will pay all invoices within thirty (30) days of the County's receipt of the invoice. The County will not pay late fees, interest, or other penalties for later payment. Any entity authorized to utilize this Contract, outside the responsibility of the County, is responsible for all orders, invoices, payment, and/or tracking.

(b) Upon the County's failure to make payment on undisputed invoices when due, WatchGuard shall notify the County in writing of its intent to stop work until all undisputed payments are made. The County shall have a period of 30 days to cure and make payment before WatchGuard can exercise its right, in addition to its other rights and remedies, to suspend, temporarily, further performance of this Contract without liability.

Section 7.04 Taxes

The fees in the Investment Summary do not include any taxes, including, without limitation, sales, use, or excise tax. The County is tax exempt and will provide a tax-exempt certificate to WatchGuard upon WatchGuard's request. WatchGuard is responsible for reporting and paying its income taxes, both federal and state, as applicable, arising from WatchGuard's performance of this Contract.

Section 8 Contract Administration and Reports

Section 8.01 Contract Administration

The Franklin County Sheriff's Office, with assistance from the Franklin County Purchasing Department, will be responsible for the administration of the Contract and will monitor WatchGuard's performance and compliance with the terms, conditions, and specifications of the Contract. If any agency observes any infraction(s), such shall be documented and conveyed to the Franklin County Purchasing Department for immediate remedy. Franklin County Purchasing Department shall be the point of contact for the County relative to any notices sent to or by the County pursuant to this Contract.

Section 8.02 Out of Scope Work and Change Order Process

(a) Out of Scope Work

WatchGuard is not allowed to perform any work that is out of scope. If WatchGuard believes that the work being requested to be performed is out of scope it must be brought to the attention of the Project Manager or the Franklin County Purchasing Department. Any work that is out of scope, if it is determined to be necessary by the County, must be added to the Statement of Work through a written contract modification provided to the County to be approved by the Franklin County Board of Commissioners, which has the sole discretion to authorize a modification to the Contract. Approval of a contract modification under this section by the Franklin County Board of Commissioners shall be at their sole and complete discretion. WatchGuard is not obligated to perform additional or out of scope work unless/until such work is mutually agreed upon in writing under via Contract addendum or Change Order and signed by both parties. If WatchGuard knowingly performs work that is out of scope and does so without the proper written authorization from the Franklin County Board of Commissioners, they do so at their own risk. The County will not be liable for any cost of the work performed that was out of scope and done without the proper authorization. The price quotes in the addendum or change order will be valid until Final Acceptance.

(b) Change Order Process

(i) In the event changes to the scope of the project and/or additional work become necessary or desirable to the parties, the parties shall follow the procedures set forth in this Section. A change or addition to the scope of work shall be effective only when documented by a Change Order, which shall be in writing, executed by both parties, and expressly reference this Contract. The Change Order shall set forth in detail: (1) the change requested; (2) the reason for the proposed change; (3) the cost of the change; (4) the impact of the change on time for completion of the project; and (5) technical changes to be considered. The parties will agree on the form to be used to document the Change Order and will mutually agree to procedures for submitting such Change Orders. Change Orders will be submitted for all changes to the specifications whether they involve a cost increase or are a no-cost Change Order.

(ii) Not Used.

Section 8.03 "Go-Live" Acceptance

The implementation of this Agreement shall occur in six phases as described in Exhibit 1. Each phase shall have its own Go-Live acceptance period. Implementation of a subsequent phase may commence during the Go-Live acceptance period of the preceding phase, but commencement of implementation of the subsequent phase shall not be a waiver of the Go-Live Acceptance requirements of this section for the preceding phase. For each phase, Go-Live shall be deemed accepted when the following criteria have been met:

(1) The WatchGuard Software conforms with the Functional Descriptions set forth in this Contract;

(2) completion of all required training outlined in the training plan included in Exhibit 1 and commencement of Go-Live acceptance period described below; and

(3) the WatchGuard Software for each County “Department Phase” operates in a production environment for 30 consecutive days (“Go-Live Acceptance Period”) without any Priority Level 1 or Priority Level 2 Defects, as such Defects are described in the Support Call Process Table (see Exhibit B to SaaS Agreement) In the event that a Priority Level 1 or Priority Level 2 Defect occurs during the Go-Live Acceptance Period, Watchguard shall remedy the Defect, and upon the Defect being remedied, the Go-Live Acceptance Period will restart and a new 30-day period shall be required without Priority Level 1 or 2 Defect in order for Go-Live acceptance to occur.

Upon the Go-Live Acceptance for the first phase as described in Exhibit 1, the parties shall execute a Go-Live

Acceptance certificate or other writing confirming Go-Live Acceptance for the first phase, and upon the execution of that certificate Watchguard shall invoice the County for one-half of the first year SaaS Fee as described in Exhibit 1.

Priority Level Defects 3 and 4 (see Exhibit B to SaaS Agreement) will not be subject to the Go-Live Acceptance Period. Go-Live Acceptance applies individually to each County "Department Phase" identified on the Investment Summary. When all Department Phases have achieved Go-Live Acceptance, Final Acceptance will be achieved in accordance with the requirements of Section 8.04 below.

Section 8.04 Final Acceptance

(a) Final Acceptance shall occur when the WatchGuard Software operates in a production environment for 30 consecutive days ("Final Acceptance Period") following Go-Live Acceptance for all County Department Phases without any Priority Level 1 or Priority Level 2 Defects. In the event that a Priority Level 1 or Priority Level 2 Defect occurs during the Final Acceptance Period, Watchguard shall remedy the Defect, and upon the Defect being remedied, the Final Acceptance Period will restart and a new 30-day period shall be required without Priority Level 1 or 2 Defect in order for Final Acceptance to occur.

(b) Should a Priority Level 3 Incident affecting more than one user or as otherwise mutually agreed upon by the County and WatchGuard occur, the Final Acceptance Period shall be suspended. Upon resolution of the aforementioned Priority Level 3 event, the Final Acceptance Period shall resume on the next business day until either Final Acceptance or the occurrence of another Support Incident as described in Section 8.04.

(c) Upon Final Acceptance the parties shall execute a certificate or other writing confirming that Final Acceptance has occurred. Watchguard shall invoice County for the second one-half of the year 1 SaaS Fees upon Final Acceptance.

Section 8.05 Acceptance Not Waiver

The County's approval or acceptance of, or payment for any of the Services or Equipment to be provided under this Contract and related Contract documents, shall not be construed to operate as a waiver of any rights or benefits to the County under this Contract or cause of action arising out of the performance of this Agreement, nor shall it be construed to relieve WatchGuard of liability for any express warranties or responsibility for faulty materials, workmanship, or service as contained in this Contract.

Section 9 Contract Cancellation, Termination, Remedies

Section 9.01 Contract Cancellation

The County may cancel this Contract upon any one of the following events. The cancellation will be effective on the date delineated by the County as set forth below.

(a) 90-Day Notice Termination. The County reserves the right to terminate the Contract by giving WatchGuard 90-days prior written notification. Upon receipt of notice from the County, unless otherwise agreed by the parties, WatchGuard shall cease beginning the completion of any new phase of the Services and shall only complete Services in furtherance of winding down the Contract. In such event, the County agrees to pay Watchguard for Services performed up to the effective date of termination.

(b) Non-Appropriation of Funds. This Contract is contingent upon the County budgeting and appropriating the funds on an annual basis necessary for the continuation of this Contract in any contract year. In the event that the funds necessary for the continuation of this Contract are not approved for expenditure in any year, this Contract shall terminate on the last day of the fiscal year in which funding was approved, without penalty to the County. The County will provide WatchGuard with written notification within 10 business days after being notified that the funding of this Contract is no longer approved. The County will pay WatchGuard for all products and services delivered through the date of termination and will not be entitled to a refund or offset of previously paid, but unused SaaS Fees.

(c) Cancellation for Failure to Retain Certification. Pursuant to the requirements as stated in the Contract, all certifications and/or registrations must be maintained for the life of the Contract. Failures to renew certification(s) or the de-certification by certifying entity, may result in the termination of this Contract for Default.

(d) Cancellation for Financial Instability. The County may cancel this Contract by 30-day advanced written notice to WatchGuard if a petition in bankruptcy or similar proceeding has been filed by or against WatchGuard.

Section 9.02 Termination for Default

(a) County's Termination for Default by WatchGuard:

The County may, subject to the paragraphs below, by written notice of default to WatchGuard, terminate this Contract in whole or in part if WatchGuard fails to: (1) deliver the supplies or to perform the services within the time specified in this Contract or any extension and such failure is the sole fault of WatchGuard; or (2) make progress, so as to endanger WatchGuard's performance under this Contract.

Prior to any Notice of Default being issued, the County will provide WatchGuard with written notice of a perceived failure ("Perceived Failure Notice"). WatchGuard may, within seven business days following the Perceived Failure Notice, propose a written action plan acceptable to the County to remedy the perceived failures, infractions, or defaults ("Perceived Failure Plan"), or request a meeting by the parties to discuss the perceived failures, infraction, or defaults ("Perceived Failure Notice Meeting"). The Perceived Failure Notice Meeting shall occur not later than 45 days following the issuance of the Perceived Failure Notice. Following the Perceived Failure Notice Meeting, WatchGuard shall have 15 days to provide a Perceived Failure Plan. Should WatchGuard fail to provide a Perceived Failure Plan within the required timeframe, or should the County reasonably determine the Perceived Failure Plan is not acceptable, then the County shall have the right to issue a Notice of Default, in whole or in part, and may within ten business days following issuance of the Notice of Default terminate this Contract, in whole or in part, for default.

If the County terminates this Contract, in whole or in part, for default under this Section 9.02, it may acquire, under the terms and in the manner, the County considers appropriate, supplies or services similar to those terminated. In addition, the County may recover from WatchGuard reasonable costs incurred to complete the services to a capability not exceeding that specified in this Contract. However, WatchGuard shall continue the work not terminated.

If failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is beyond the control of WatchGuard and subcontractor, and without fault or negligence of either, WatchGuard shall not be liable for any excess costs for failure to perform, unless the subcontracted supplies or services were obtainable from other sources in sufficient time for WatchGuard to meet the required delivery schedule.

<u>Effect of Termination or Expiration</u>. Upon termination for any reason or expiration of the Contract, the Confidential Information shall be returned or destroyed in accordance with Section 10 of the Contract. If County has any outstanding payment obligations under this Contract, WatchGuard will issue a final invoice to County, which shall be due and payable upon thirty (30) days from County's receipt of the invoice. Notwithstanding the reason for termination or expiration, the County must pay WatchGuard for Products and Services already delivered and accepted. County has a duty to mitigate any damages under this Contract, including in the event of default by WatchGuard and County's termination of this Contract.

Notwithstanding the foregoing, Confidential Information shall not include information that is a public record pursuant to Ohio Revised Code Chapter 149.

(b) WatchGuard's Termination for Default by the County:

WatchGuard may terminate or suspend performance under this Contract in the event that the County is in default of any payment owed to WatchGuard, provided that WatchGuard first provides the County with thirty (30) days written notice of the default and opportunity to cure (the "Cure Period"). If County fails to cure the default within the thirty-day Cure Period, WatchGuard must provide the County with fifteen (15) days advance written notice of its intent to terminate or suspend performance under this Contract. For purposes of this Section 9.02(b), a default of any payment owed to WatchGuard does not include amounts listed on any invoice that has been rejected by the County in accordance with Section 7.02(c) or amounts currently in dispute.

Section 9.03 Delays due to Force Majeure

Neither party will be liable for delays in performing its obligations under this Contract to the extent that the delay is caused by Force Majeure; provided, however, that within ten business days of the Force Majeure event, the party whose performance is delayed provides the other party with written notice explaining the cause and extent thereof, as well as a request for a reasonable time extension equal to the estimated duration of the Force Majeure event.

Section 9.04 LIABILITY AND DISCLAIMER OF DAMAGES

(a) LIMITATION OF LIABILITY. EXCEPT FOR PERSONAL INJURY OR DEATH, THE TOTAL AGGREGATE LIABILITY OF WATCHGUARD FOR DIRECT DAMAGES ARISING OUT OF THIS CONTRACT, WHETHER BASED ON A THEORY OF CONTRACT OR IN TORT, LAW OR EQUITY, WILL BE LIMITED TO COUNTY'S ACTUAL DIRECT DAMAGES, NOT TO EXCEED TWO TIMES THE ONE-TIME FEES SET FORTH IN EXHIBIT 1. THE PRICES SET FORTH IN THIS CONTRACT ARE SET IN RELIANCE UPON THIS LIMITATION OF LIABILITY.

(b) EXCLUSION OF CERTAIN DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, IN NO EVENT WILL WATCHGUARD BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER OR DAMAGES FOR LOST PROFITS OR REVENUES, EVEN IF WATCHGUARD HAS BEEN ADVISED BY THE COUNTY OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES.

Section 10 Certifications and Affidavits

Section 10.01 Contractor's Warranty against an Unresolved Finding for Recovery

Ohio Revised Code (O.R.C.) §9.24 prohibits the County from awarding a contract to any contractor against whom the Auditor of the State has issued a finding for recovery if the finding for recovery is "unresolved" at the time of the award. By signing this Contract, WatchGuard warrants that it is not now, and will not become subject to an "unresolved" finding for recovery under O.R.C. §9.24, and agrees that it shall not take any action that would result in an unresolved finding for recovery under such Section.

Section 10.02 Suspension and Debarments

The County will not award a Contract for goods or services, funded in whole or in part with federal funds, to a person or vendor who has been suspended or debarred from doing business with the State of Ohio or who appears on the Excluded Parties List in the System for Award Management (SAM) database at https://www.sam.gov/SAM/, or as may be amended.

Section 10.03 Legal Compliance

WatchGuard must agree to comply with all applicable local, state, and federal laws in the performance of the work specified in this proposal including applicable state and federal laws regarding drug-free workplaces. WatchGuard will be required to accept full responsibility for payment of all taxes and insurance premiums including, but not limited to: unemployment compensation insurance premiums, Workers' Compensation, all income tax deductions, Social Security deductions, and any other taxes or payroll deductions required for all employees engaged by WatchGuard in the performance of the work specified in this Contract.

Section 10.04 Workers' Compensation Provision

WatchGuard shall be required to carry Workers' Compensation Liability Insurance as required by Ohio law for any work to be performed within the State of Ohio, as applicable by law. Unless otherwise listed in the proposal specifications, WatchGuard will be required to provide said certificate within seven calendar days after notification of award to: Franklin County Purchasing Department, 25th Floor, 373 S. High St., Columbus, OH 43215-6315.

Failure to provide certificate within the stated time period may deem WatchGuard as non-responsive and result in dismissal of award recommendation. Failure to maintain Workers' Compensation Liability Insurance coverage as required by law and any renewal thereto will be considered as a default.

Section 10.05 Reserved

Section 10.06 Nondiscrimination/Equal Opportunity Provisions

WatchGuard agrees that in the hiring of employees for the performance of work under the Contract, WatchGuard shall not, by reasons of race, color, religion, sex, age, disability, military status, veteran status, national origin, ancestry, sexual orientation, or gender identity, discriminate against any citizen of this state in the employment of a person qualified and available to perform the work to which the Contract relates. That WatchGuard or any person acting on behalf of WatchGuard, shall not, in any manner, discriminate against, intimidate, or retaliate against any employee hired for the performance of work under the Contract on account of race, color, religion, sex, age, disability, military status, veteran status, national origin, ancestry, sexual orientation, or gender identity.

By the signature affixed on Exhibit 3 *Nondiscrimination/Equal Opportunity Affidavit* of the Contract, WatchGuard certifies that it complies with the express language contained in O.R.C. §125.111 regarding Nondiscrimination/Equal Opportunity.

All contractors who contract with the state or any of its political subdivisions for materials, equipment, supplies, contracts of insurance, or services shall have a written affirmative action program for the employment and effective utilization of economically disadvantaged persons, as defined in O.R.C. §122.71. Annually, each such contractor shall file a description of the affirmative action program and a progress report on its implementation with the Equal Employment Opportunity Officer of the Ohio Department of Administrative Services.

Section 10.07 Delinquent Personal Property Taxes

By the signature affixed on Exhibit 4 *Delinquent Personal Property Taxes* of the Contract, WatchGuard certifies that they are not charged with delinquent personal property taxes on the general list of personal property in Franklin County, Ohio, or any other counties containing property in the taxing districts under the jurisdiction of the Auditor of Franklin County, Ohio.

Section 10.08 Confidentiality

Each party acknowledges that performance of this Contract may involve access to confidential information. "Confidential Information" includes any and all non-public information provided by one party ("Discloser") to the other ("Recipient") that is disclosed under the Contract in oral, written, graphic, machine recognizable, or sample form, being clearly designated, labeled or marked as confidential. With respect to the County, Confidential Information will also include but is not limited to personal identifying information, non-public case information, sealed or expunged records, juvenile records, records containing personal health information including information about drug dependency, developmental disability and mental health, adoption records, protective services records, certain records related to domestic abuse, education records, records related to cases involving peace officers, non-public court records and data, and sealed case files, all of which may not be considered to be public records as defined by the Ohio Revised Code, the Ohio Administrative Code, and the Ohio Rules of Superintendence. For purposes of this Contract, Confidential Information shall consist of the County "Confidential Information" and such other information as may be deemed confidential pursuant to Ohio Revised Code Chapter 149, including access to and disclosure of trade secrets, data, rates, procedures, materials, lists, systems and information belonging to the other. All of this information shall be referenced collectively as "Confidential Information." In order to be considered Confidential Information, information that is disclosed orally must be identified as confidential at the time of disclosure and confirmed by Discloser by submitting a written document to Recipient within thirty (30) days after such disclosure. The written document must contain a summary of the Confidential Information disclosed with enough specificity for identification purpose and must be labeled or marked as confidential or its equivalent.

Recipient shall ensure that the Discloser's Confidential Information remains confidential and shall take all reasonable steps to ensure that the Discloser's Confidential Information remain confidential and secure, including as against any WatchGuard employees who do not have a need to view or access the Discloser's Confidential Information. Access to any such Confidential Information shall not change its status as confidential. Except as set forth in the next paragraph, no Confidential Information shall be disclosed to any third party other than representatives of such party who have a need to know such Confidential Information, provided that such representatives are informed of the confidentiality provisions hereof and agree to abide by them. All such Information must be maintained in strict confidence.

Notwithstanding the provisions of the previous paragraph, WatchGuard understands and agrees that any Confidential Information may become subject to a Public Request for Information under Ohio Revised Code Chapter 149. In the event the County receives any such request for any Confidential Information, it will promptly notify WatchGuard in writing of the request to enable WatchGuard to take whatever action it deems appropriate to seek protection from disclosure. If WatchGuard fails to take any action within five business days of such written notice, the County may make such disclosure without any liability to the County.

These obligations of confidentiality will not apply to information that:

(a) Is in the public domain, either at the time of disclosure or afterwards, except by breach of this Contract by a party or its employees or agents;

(b) A party can establish by reasonable proof was in that party's possession at the time of initial disclosure;

(c) A party receives from a third party who has a right to disclose it to the receiving party; or

(d) Is the subject of a legitimate disclosure request under the open records laws or similar applicable public disclosure laws governing this Contract, or a subpoena, for materials applicable to this Contract; provided, however, that in the event the County receives such request above, the County will give WatchGuard prompt notice and otherwise perform the functions required by applicable law.

Recipient will not reverse engineer, de-compile or disassemble any Confidential Information.

Should the County Confidential Information be released in whole or in part to anyone, including a WatchGuard employee that has no need to view or access the records, then WatchGuard shall have the obligation to inform Franklin County within five (5) business days after WatchGuard determines the County Confidential Information has been improperly viewed or accessed. WatchGuard shall, at its sole cost and expense, take all commercially reasonable steps to eliminate any such unauthorized access to the County Confidential Information, and determine

which records were accessed and by whom. Failure to secure and securely maintain the County Confidential Information by WatchGuard shall constitute a material breach of this Contract.
County shall promptly notify WatchGuard upon discovery of any unauthorized use or disclosure of the Confidential Information and take reasonable steps to regain possession of the Confidential Information and prevent further unauthorized actions or other breach of this Agreement.

All Confidential Information is and will remain the property of the Discloser. Upon termination for any reason or expiration of the Contract, Recipient will return or destroy all Confidential Information to Discloser along with all copies and portions thereof or certify in writing that all such Confidential Information has been destroyed. However, Recipient may retain (a) one (1) archival copy of the Confidential Information for use only in case of a dispute concerning this Contract and (b) Confidential Information that has been automatically stored in accordance with Recipient's standard backup or recordkeeping procedures, provided, however that Recipient will remain subject to the obligations of this Contract with respect to any Confidential Information retained subject to clauses (a) or (b). No license, express or implied, in the Confidential Information is granted to the Recipient other than to use the Confidential Information in the manner and to the extent authorized by this Contract. Discloser represents and warrants that it is authorized to disclose any Confidential Information it discloses pursuant to this Contract.

Section 11 Special Considerations

Section 11.01 Governing Law/Venue

This Contract shall be governed by the laws of the State of Ohio (regardless of the laws that might be applicable under principles of conflicts of law) as to all matters, including but not limited to matters of validity, construction, effect, and performance. All actions regarding this Contract shall be forumed and venued in the United States District Court for the Southern District of Ohio or the Court of Common Pleas General Division located in Franklin County, Ohio and the parties hereby consent to the jurisdiction of such courts.

Section 11.02 Independent Status of the Contractor

(a) The parties will be acting as independent contractors. The partners, employees, officers, and agents of one party will act only in the capacity of representatives of that party and not as employees, officers, or agents of the other party and will not be deemed for any purpose to be such. Each party assumes full responsibility for the actions of its employees, officers, and agents, and agents while performing under this Contract and will be solely responsible for paying its people. Each party will also be solely responsible for withholding and paying income taxes and Social Security, Workers' Compensation, disability benefits, and the like for its people. Neither party will commit, nor be authorized to commit, the other party in any manner.

(b) WatchGuard shall have no claim against the County for vacation pay, sick leave, retirement benefits, Social Security, Workers' Compensation, health or disability benefits, unemployment insurance benefits, or other employee benefits of any kind.

Section 11.03 Entire Contract/Amendment/Waiver

This Contract and its exhibits and schedules and any documents referred to herein or annexed hereto constitute the complete understanding of the parties regarding the subject matter hereto and supersedes all previous agreements, proposal, and understandings, whether written or oral, relating to this subject matter. This Contract shall not be changed, modified, terminated, or amended except by a writing signed by a duly authorized officer of each party to this Contract. Any waiver must be in writing. Any waiver shall constitute a waiver of such right or remedy only and not of any other right or remedy of the waiving party. For purposes of any amendments or waivers, such amendment and waivers shall only be binding against the County if signed by the Franklin County Board of Commissioners. The preprinted terms and conditions found on any County purchase order, acknowledgment, or other form will not be considered an amendment or modification or part of this Contract, even if a representative of each Party signs such document.

Section 11.04 Notices

All notices and other communications which may or are required to be given hereunder shall be in writing and shall be deemed duly given if personally delivered, or sent by overnight express courier, or sent by United States mail, registered or certified, return receipt requested, postage prepaid, to the address set forth hereunder or to such other address as the other party hereto may designate in written notice transmitted in accordance with this provision. If either overnight express courier or United States mail delivery is not available or delivery is uncertain, then notices may be given by facsimile or by email. Notice shall be sent to the following addresses:

To WatchGuard:

WatchGuard Video, Inc.
Attention: Stuart Johnston
350 Worthington Road, Suite C
Westerville, OH 43082
Phone: (740) 953-0447
Email: Stuart.johnston@motorolasolutions.com

To the County:

Franklin County Sheriff's Office
Attention: David Masterson, Director of Administrative Services
410 S. High Street
Columbus, Ohio 43215
Phone: (614) 525-6746
Fax: (614) 525-3560
Email: dmmaster@franklincountyohio.gov

With a copy to:

Franklin County Purchasing Department
Attention: Purchasing Director
373 S. High Street, 25th Floor
Columbus, OH 43215
Phone: (614) 525-2402
Fax: (614) 525-3144
Email: mabaloni@franklincountyohio.gov

All notices or communications shall be deemed delivered upon the earlier of the following:

(i) Actual receipt by the receiving party;

(ii) Upon receipt by sender of certified mail, return receipt signed by an employee or agent of the receiving party; or

(iii) If not actually received, five days after deposit with the United States Postal Service authorized mail center with proper postage (certified mail, return receipt requested) affixed and addressed to the other party at the address set forth on the signature page hereto or such other address as the party may have designated by proper notice.

The consequences for the failure to receive a notice due to improper notification by the intended receiving party of a change in address will be borne by the intended receiving party.

Section 11.05 Green Initiatives

By adoption of Resolution 432-17, the Franklin County Board of Commissioners have reaffirmed the County's commitment to the mutually compatible goals of environmental protection and economic growth, and also expressed its intention to promote sustainable principles in policy decisions and programs. In that spirit, the County (a) promotes the purchase and use of products and services that enhance environmental, social and economic health; (b) develops waste management policies that reduce the amount of materials directed to landfills for disposal; and, (c) improves air quality through environmentally appropriate fleet management practices through deployment of alternate fuel and hybrid electric vehicles.

It is the Board of Commissioners intent to support the green energy economy through workforce partnerships and doing business with providers of goods and services who promote sustainable environmental policies within their own businesses and while doing business with Franklin County.

Section 11.06 Offshore Activities

No portion of this Contract may be performed offshore. All services under this Contract shall be performed within the borders of the United States or within the borders of any country with which the United States is engaged in an active free trade agreement. Any services that are described in the specifications or Statement of Work that directly pertain to servicing this Contract shall be performed within the borders of the United States or within the borders of any country with which the United States is engaged in an active free trade agreement. This shall include any back up services for Data, back-office services, and work performed by subcontractors at all tiers.

Section 11.07 Travel Expenses

All travel required by WatchGuard under this Contract is included in the costs listed in Exhibit 1. The County will pay for any additional travel that it requests only with prior written approval. The County will pay for all additional travel expenses that it requests in accordance with the Franklin County Board of Commissioner's travel policy attached as Exhibit 5.

Section 11.08 Headings

The headings used in this Contract are for convenience only and will not affect the interpretation of any of the Contract terms and conditions.

Section 11.09 Reserved

Section 11.10 Time of the Essence

The time limits and timelines set forth herein are of the essence of this Contract. WatchGuard has reviewed and approved all such time limits and timelines and confirms that all such limits are reasonable periods of time for its performance hereunder. Notwithstanding the foregoing, WatchGuard will not be responsible for delays or nonperformance caused by the County or that are outside the control of WatchGuard.

Section 11.11 Multiple Originals and Authorized Signatures

This Contract may be executed in multiple originals, any of which will be independently treated as an original document. The parties may sign in writing or by electronic signature. An electronic signature, or facsimile copy will be treated, and will have the same effect as an original signature, and will have the same effect, as an original signed copy of this document. Each party represents to the other that the signatory set forth below is duly authorized to bind that party to this Contract.

Section 11.12 Survival

Survival. The following provisions will survive the expiration or termination of this Contract for any reason: Section 5.01 Standard of Care; Section 5.03 Indemnification, Section 5.04 Intellectual Property Infringement, Section 7 – Payment and Invoicing; Section 9.02 – Effect of Termination or Expiration; Section 9.03_– Delays and Force Majeure; Section 9.04 – Limitation of Liability; Section 10.08 – Confidentiality and WatchGuard Materials.

Section 11.13 Cyber Breach

WatchGuard shall have a plan and adequate resources to address telecommunications and computer systems breach, and shall maintain intrusion detection services and procedures and/or data breaching systems to detect and address "hacking" and "phishing operations" into the WatchGuard's telecommunications system, that includes services and systems to detect any unauthorized access to or unauthorized activity on WatchGuard's telecommunications system, networks, computer systems, and network devices associated with the use of and access to the County's management systems, databases, and County information and data. WatchGuard will ensure that all intrusion detection measures and data breach systems are maintained and functional on a regular basis. Intrusion detection services and data breach systems shall include, at minimum, network-based intrusion detection and active monitoring of appropriate computer system access logs. WatchGuard shall notify the County, as soon as reasonably possible, of its detection of any potential or suspected intrusions that may affect the County with regard to disbursement of payments or access to County systems, networks, data, or information. Failure by WatchGuard to provide this notification shall be a breach under the contract. WatchGuard shall be liable for all costs and damages to the County related to or arising from the breach of WatchGuard's telecommunications systems, networks, or computer systems as a result of WatchGuard's negligent or willful misconduct, or failure to follow the requirements of this Section 11.13.

Section 11.14 Severability

If any term or provision of this Contract is held invalid or unenforceable, the remainder of this Contract will be considered valid and enforceable to the fullest extent permitted by law.

The parties hereto have set their hands and seal this ___________________________________.

Franklin County Board of Commissioners:

By:______________________________
Erica C. Crawley, President

By: ______________________________
John O'Grady, Commissioner

By: ______________________________
Kevin L. Boyce, Commissioner

WatchGuard Video, Inc.:

By: Giles Tipsword 2/3/2022 | 7:13 PM EST
Giles Tipsword, MSSSI Vice President

APPROVED AS TO FORM:
G. Gary Tyack
Prosecuting Attorney
Franklin County, Ohio

By: Jesse Armstrong
Assistant Prosecuting Attorney
Date: 2/3/2022 | 7:46 PM EST

APPROVED AS TO FORM:
Megan A. Perry-Balonier
Director, Purchasing Department
Franklin County, Ohio

By: Megan Perry-Balonier
Date: 2/3/2022 | 7:19 PM EST

Exhibit 1
Statement of Work and Investment Summary

Franklin County Ohio
January 2022

Video Evidence Statement of Work

1.1 INTRODUCTION

In accordance with the terms and conditions of the Agreement, this Statement of Work ("SOW") defines the principal activities and responsibilities of all parties for the delivery of the WatchGuard Video, Inc. ("WatchGuard") system as presented in this offer to Franklin County Ohio (hereinafter referred to as ("County"). When assigning responsibilities, the phrase "WatchGuard" includes our subcontractors and third-party partners.

Deviations and changes to this SOW are subject to mutual agreement between WatchGuard and the County and will be addressed in accordance with the change provisions of the Agreement.

Unless specifically stated, WatchGuard work will be performed remotely. County will provide WatchGuard resources with unrestricted direct network access to enable WatchGuard to fulfill its delivery obligations.

The number and type of software or subscription licenses, products, or services provided by WatchGuard or its subcontractors are specifically listed in the Agreement and any reference within this document, as well as subcontractors' SOWs (if applicable), does not imply or convey a software or subscription license or service that is not explicitly listed in the Agreement.

1.2 AWARD, ADMINISTRATION, AND PROJECT INITIATION

Project Initiation and Planning will begin following execution of the Agreement between WatchGuard and the County.

Following the conclusion of the Welcome/IT Call, the WatchGuard project personnel will communicate additional project information via email, phone call, or additional ad-hoc meetings.

Microsoft Teams will be utilized by the parties.

1.3 PROJECT MANAGEMENT TERMS

The following project management terms are used in this document. Since these terms may be used differently in other settings, these definitions are provided for clarity.

Deployment Date(s) refers to any date or range of dates when implementation, configuration, and training will occur. The deployment date(s) is subject to change based on equipment or resource availability and County readiness.

Exhibit 1

Statement of Work and Investment Summary

1.4 COMPLETION CRITERIA

WatchGuard Integration Services are considered complete upon WatchGuard performing the last task listed in a series of responsibilities or as specifically stated in the deployment checklist. Certain County tasks, such as hardware installation activities identified in Section 1.9 of this SOW, must be completed prior to WatchGuard commencing with its delivery obligations. County will provide WatchGuard written notification of County's acceptance of a deliverable.

The service completion will be acknowledged in accordance with the terms of the Agreement and the Service Completion Date will be memorialized by WatchGuard and County.

1.5 PROJECT ROLES AND RESPONSIBILITIES OVERVIEW

1.5.1 WatchGuard Project Roles and Responsibilities

A WatchGuard team, made up of specialized personnel, will be assigned to the project under the direction of the WatchGuard Project Manager. Team members will be multi-disciplinary and may fill more than one role. Team members will be engaged in different phases of the project as necessary.

In order to maximize efficiencies, WatchGuard's project team will provide services remotely via teleconference, web-conference, or other remote method in fulfilling its commitments as outlined in this SOW.

The personnel role descriptions noted below provide an overview of typical project team members. One or more resources of the same type may be engaged as needed throughout the project. There may be other personnel engaged in the project under the direction of the Project Manager.

WatchGuard's project management approach has been developed and refined based on lessons learned in the execution of hundreds of system implementations. Using experienced and dedicated people, industry-leading processes, and integrated software tools for effective project execution and control, we have developed and refined practices that support the design, production, and testing required to deliver a high-quality, feature-rich system.

Project Manager

A WatchGuard Project Manager will be assigned as the principal business representative and point of contact for the organization. The Project Manager's responsibilities include the following:

- Host the Welcome/IT Call.
- Manage the WatchGuard responsibilities related to the delivery of the project.
- Coordinate schedules of the assigned WatchGuard personnel and applicable subcontractors/supplier resources.
- Manage the Change Order process per the Agreement.
- Maintain project communications with the County.
- Identify and manage project risks.
- Collaborative coordination of County resources to minimize and avoid project delays.
- Conduct remote status meetings on mutually agreed dates to discuss project status.
- Provide timely responses to issues related to project progress.

System Technologists

The WatchGuard System Technologists (ST) will work with the County project team on system provisioning. ST responsibilities include the following:

- Provide consultation services to the County regarding the provisioning and operation of the WatchGuard system.
- Provide provisioning and training to the County to set up and maintain the system.
- Complete the provisioning ownership handoff to the County.
- Complete the project-defined tasks as defined in this SOW.
- Confirmation that the delivered technical elements meet contracted requirements.
- Engagement throughout the duration of the delivery.

Technical Trainer / Instructor

The WatchGuard Technical Trainer / Instructor provides training either on-site or remote (virtual) depending on the training topic and deployment type purchased. Responsibilities include:

- Review the role of the Learning eXperience Portal ("LXP") in the delivery and provide County Username and Access Information.

Sub-Contractors

The WatchGuard Project Manager may utilize WatchGuard certified subcontractors to complete specific project tasks. Here is a list of possible subcontractors:

- P&R Communications Service, Inc – 731 E. 1st Street, Dayton, Ohio 45402
  - Install and Training Services.

1.5.2 County Project Roles and Responsibilities Overview

The success of the project is dependent on early assignment of key County resources. In many cases, the County will provide project roles that correspond with WatchGuard's project roles. It is critical that these resources are empowered to make decisions based on the County's operational and administration needs. The County's project team should be engaged from project initiation through beneficial use of the system. The continued involvement in the project and use of the system will convey the required knowledge to maintain the system post-completion of the project. In some cases, one person may fill multiple project roles. The project team must be committed to participate in activities for a successful implementation. In the event the County is unable to provide the roles identified in this section, WatchGuard may be able to supplement County resources at an additional price.

Project Manager

The Project Manager will act as the primary County point of contact for the duration of the project. The Project Manager is responsible for management of any third-party vendors that are the County's subcontractors. In the event the project involves multiple locations, WatchGuard will work exclusively with a single County-assigned Project Manager (the primary Project Manager). The Project Manager's responsibilities include the following:

- Communicate and coordinate with other project participants.
- Manage the County project team, including timely facilitation of efforts, tasks, and activities.
- Maintain project communications with the WatchGuard Project Manager.
- Identify the efforts required of County staff to meet the task requirements in this SOW and identified in the Welcome/IT Call.
- Consolidate all project-related questions and queries from County staff to present to the WatchGuard Project Manager.
- Approve a deployment date offered by WatchGuard.

Exhibit 1
Statement of Work and Investment Summary

- Monitor the project to ensure resources are available as required.
- Attend status meetings.
- Provide timely responses to issues related to project progress.
- Liaise and coordinate with other agencies, County vendors, contractors, and common carriers.
- Review and administer change control procedures, hardware and software certification, and all related project tasks required to meet the deployment date.
- Ensure County vendors' readiness ahead of the deployment date.
- Assign one or more personnel who will work with WatchGuard staff as needed for the duration of the project, including at least one Application Administrator for the system and one or more representative(s) from the IT department.
- Identify the resource with authority to formally acknowledge and facilitate the approval of change orders, completion of work, and payments in a timely manner.
- Provide building access to WatchGuard personnel to all County facilities where system equipment is to be installed during the project. Temporary identification cards are to be issued to WatchGuard personnel, if required for access to facilities.
- Ensure remote network connectivity and access to WatchGuard resources.
- Provide reasonable care to prevent equipment exposure to contaminants that cause damage to the equipment or interruption of service.
- Ensure a safe work environment for WatchGuard personnel.
- Identify and manage project risks.
- Point of contact to work with the WatchGuard System Technologists to facilitate the training plan.

IT Support Team

The IT Support Team (or County designee) manages the technical efforts and ongoing tasks and activities of their system. Manage the County-owned provisioning maintenance and provide required information related to LAN, WAN, wireless networks, server, and client infrastructure. They must also be familiar with connectivity to internal, external, and third-party systems to which the WatchGuard system will interface.

The IT Support Team responsibilities include the following:

- Participate in overall delivery and training activities to understand the software, interfaces, and functionality of the system.
- Participate with the County subject matter experts during the provisioning process and training.
- Authorize global provisioning choices and decisions, and be the point(s) of contact for reporting and verifying problems and maintaining provisioning.
- Obtain inputs from other user agency stakeholders related to business processes and provisioning.
- Implement changes to County owned and maintained infrastructure in support of the Evidence Management System installation.

Subject Matter Experts

The Subject Matter Experts (SME or Super Users) are the core group of users involved with delivery analysis, training, and the provisioning process, including making global provisioning choices and decisions. These members should be experienced users in the working area(s) they represent (dispatch, patrol, etc.), and should be empowered to make decisions related to provisioning elements, workflows, and department policies related to the Evidence Management System.

General County Responsibilities

In addition to the County Responsibilities stated elsewhere in this SOW, the County is responsible for the following:

Exhibit 1

- All County-provided equipment, including hardware and third-party software, necessary for delivery of the System not specifically listed as a WatchGuard deliverable. This will include end user workstations, network equipment, camera equipment and the like.
- Configuration, maintenance, testing, and supporting the third-party systems the County operates which will be interfaced to as part of this project.
- Communication between WatchGuard and County's third-party vendors, as required, to enable WatchGuard to perform its duties.
- Active participation of County Subject Matter Experts (SMEs) in project delivery meetings and working sessions during the course of the project. County SMEs will possess requisite knowledge of County operations and legacy system(s) and possess skills and abilities to operate and manage the system.
- Electronic versions of any documentation associated with the business processes identified.
- Providing a facility with the required computer and audio-visual equipment for training and work sessions.
- Ability to participate in remote project meeting sessions using Google Meet or a mutually agreeable, County-provided, alternate remote conferencing solution.

1.6 PROJECT PLANNING

A clear understanding of the needs and expectations of both WatchGuard and the County are critical to fostering a collaborative environment of trust and mutual respect. Project Planning requires the gathering of project-specific information in order to set clear project expectations and guidelines, and set the foundation for a successful implementation.

1.6.1 Welcome/IT Call - Teleconference/Web Meeting

A Project Planning Session teleconference will be scheduled after the Agreement has been executed. The agenda will include the following:

- Review the Agreement documents.
- Review project delivery requirements as described in this SOW.
- Provide shipping information for all purchased equipment.
- Discuss deployment date activities.
- Provide assigned technician information.
- Review IT questionnaire and County infrastructure.
- Discuss which tasks will be conducted by WatchGuard resources.
- Discuss County involvement in provisioning and data gathering to confirm understanding of the scope and required time commitments.
- Review the initial project tasks and incorporate County feedback.
- Confirm CJIS background investigations and fingerprint requirements for WatchGuard employees and/or contractors. Required fingerprints will be submitted on WatchGuard provided FBI FD-258 Fingerprint cards.
- Review the On-line Training system role in project delivery and provide County User Name and Access Information.
- Discuss WatchGuard remote access requirements (24-hour access to a secured two-way Internet connection to the WatchGuard system firewalls for the purposes of deployment, maintenance, and monitoring).
- Discuss County obligation to manage change among the stakeholder and user communities.
- Review deployment completion criteria and the process for transitioning to support.

Exhibit 1

Statement of Work and Investment Summary

WatchGuard Responsibilities

- Host Welcome/IT Call**.**
- Request the attendance of any additional County resources that are instrumental in the project's success, as needed.
- Review WatchGuard's delivery approach and its reliance on County-provided remote access.
- Provide County with steps to follow to register for Online Training.
- Request user information required to establish the County in the Learning eXperience Portal ("LXP").

County Responsibilities

- Complete the Online Training registration form and provide it to WatchGuard within ten business days of the Project Planning Session.
- Review the received (as part of order) and completed IT questionnaire.
- Provide a County point of contact for the project.
- Provide data for completing the policy validation form.
- Provide LXP user information as requested by WatchGuard.
- Verify County Administrator(s) have access to the LXP.

WatchGuard Deliverables

- Welcome Call presentation and key meeting notes
- Send an email confirming deployment date and ST assigned email
- Communicate with the County via email confirming shipment and tracking information.
- Instruct the County on How to Register for Training email.
- Provide and review the Training Plan.

1.7 SOLUTION PROVISIONING

Solution provisioning includes the configuration of user configurable parameters (unit names, personnel, and status codes). The system will be provisioned using WatchGuard standard provisioning parameters and will incorporate County-specific provisioning.

1.7.1 In-Car Video Provisioning

If in-car video is a part of the system, the WatchGuard Application Specialist will complete the following provisioning tasks.

WatchGuard Responsibilities

- Conduct a remote review of the standard provisioning database with the County prior to the start of provisioning.
- Provide and review the Provisioning Export Worksheets with the County.
- Conduct a conference call with the County to review the completeness of the Provisioning Export Worksheets prior to the start of provisioning.

1.7.2 Body Worn Camera Provisioning

If body worn cameras are a part of the system, the provisioning of the in-car system will generally follow the completion of the base in-car video provisioning.

WatchGuard Responsibilities

- Configure transfer stations for connectivity to the evidence management server.

- Configure devices within the evidence management system.
- Check out devices and create a test recording.
- Verify successful upload from devices after docking back into the transfer station or USB dock.

1.7.3 Command Central Evidence Provisioning

1.7.4 AGENCY AND USER SETUP

The County's agency(s) and CommandCentral users must be provisioned within the CommandCentral cloud platform using the CommandCentral Admin tool. The provisioning process allows the agency(s) to define the specific capabilities and permissions of each user.

WatchGuard Responsibilities

- Use the CommandCentral Admin tool to establish the County and the County's agency(s) within the CommandCentral cloud platform. This activity is completed during the order process.
- Provision agency's CommandCentral initial users and permissions.

County Responsibilities

- Identify a System Administrator(s).
- Ensure all System Administrators complete the CommandCentral Admin training.
- Use the CommandCentral Admin tool to setup CommandCentral administration and user passwords, and provision agency's CommandCentral users and permissions.

Completion Criteria

Initial agencies and users have been configured.

1.7.5 COMMUNITY INTERACTION TOOL

WatchGuard enables the Community Interaction Tool during the order process.

WatchGuard Responsibilities

- Refer to Agency and User Setup section of SOW.
- Connect County incident data ingest.

County Responsibilities

- Provision policies and procedures, tags, retention periods, and user permissions.
- Configure Community Interaction Tool settings (location of agency pin, shape of agency, keywords, agency page, URL, which forms to deploy).
- Provide access to WatchGuard' team to connect incident data ingest.

Completion Criteria

Community Interaction Tool subscription enabled.

1.7.6 RECORDS MANAGEMENT

This document describes the activities required to ensure access to the subscription software and the County's provisioning activities.

Exhibit 1

Records Management features preconfigured Incident Forms and standard Workflows. As a result, minimal configuration work is required prior to operation.

WatchGuard Responsibilities

- Refer to the Agency and User Setup section of SOW.

County Responsibilities

- Provision all required custom Offence Codes using the CommandCentral user interface.

Completion Criteria

Records Management enabled and offence codes provisioned.

1.7.7 DIGITAL EVIDENCE MANAGEMENT

WatchGuard will discuss industry best practices, current operations environment, and subsystem integration in order to determine the optimal configuration for Digital Evidence Management. WatchGuard enables the subscription during the order process.

Note that while Digital Evidence Management is capable of interfacing with a variety of data sources, any additional interfaces are not included in this implementation.

WatchGuard Responsibilities

- Refer to the Agency and User Setup section of SOW.
- Connect County incident data ingest.
- If a hybrid on-premise and cloud solution is included, configure Evidence Library to Digital Evidence Management interface(s) to support the functionality described in the Solution Description.
- Integrate Records Management with Digital Evidence Management.

County Responsibilities

- Provision policies, procedures, and user permissions.
- Configure Digital Evidence Management settings.
- Provide access to WatchGuard' team to connect incident data ingest.

Completion Criteria

Digital Evidence Management subscription enabled. Configured to provide the end-to-end solution for the County.

1.7.8 FIELD RESPONSE APPLICATION

The Field Response Application provides Android / iOS multimedia capture allowing a smartphone to send data to Digital Evidence Management.

WatchGuard Responsibilities

- None.

County Responsibilities

- Download “CommandCentral Capture” Application from App Store.
- Determine if video can be uploaded to Digital Evidence Management via WiFi and cellular network or WiFi only.

Exhibit 1

- Set confirmation parameters in Digital Evidence Management Admin.
- Determine specific video resolution or a range of resolutions.

Completion Criteria

Work is considered complete upon County successfully installing application. The Field Response Application is configured and data is being received in Digital Evidence Management.

1.7.9 THIRD-PARTY INTERFACES

The delivery, installation, and integrations of interfaces may be an iterative series of activities depending upon access to third-party systems. If proposed, interfaces will be installed and configured in accordance with the schedule.

Connectivity will be established between CommandCentral systems and the external and/or third-parties to which they will interface. WatchGuard will configure CommandCentral systems to support each contracted interface. The County is responsible for engaging third-party vendors if and as required to facilitate connectivity and testing of the interface(s).

WatchGuard Responsibilities

- Develop interface(s) in accordance with the Solution Description.
- Establish connectivity to external and third-party systems.
- Configure interface(s) to support the functionality described in the Solution Description.
- Perform functional validation to confirm each interface can transmit and or receive data in accordance with the Interface Feature Description (IFD).

County Responsibilities

- Act as liaison between WatchGuard and third-party vendors or systems as required to establish connectivity with Digital Evidence Management.
- Provide personnel proficient with and authorized to make changes to the network and third-party systems to support WatchGuard' interface installation efforts.
- Provide network connectivity between Digital Evidence Management and the third-party systems.
- Provide requested information on API, SDKs, data schema, and any internal and third-party documents necessary to establish interfaces with all local and remote systems and facilities within 10 days of the Interface Engagement Meeting.
- Adhere to the requirements presented in the IFD.

WatchGuard Deliverables

Contracted Interface(s).

Completion Criteria

Connectivity is established between CommandCentral systems and the external and/or third-parties using said interface.

Unknown circumstances, requirements, and anomalies at the time of initial design can present difficulties in interfacing CommandCentral Vault to some third-party applications. These difficulties could result in a poorly performing or even a non-functional interface. At such time that WatchGuard is provided with information and access to systems, we will be able to mitigate these difficulties. If WatchGuard mitigation requires additional third-party integration, application upgrades, API upgrades, and/or additional software licenses those costs will need to be addressed through the change provision of the contract.

1.8 SOFTWARE INSTALLATION

1.8.1 On-site Software Installation

Client software will be installed on workstations and up to 5 mobile devices to facilitate provisioning training to County personnel. County will complete software installation on the remaining workstations and cameras.

WatchGuard Responsibilities

- Verify system readiness.
- Request client software.
- Deliver the pre-installation preparation checklist.
- Provide instruction on client software installation and install client software on one workstation and up to five mobile devices.
- Total of training overview sessions shall not exceed 4 hours.
- Provide instruction on client software deployment utility.

County Responsibilities

- Provide and install workstation/mobile device hardware in accordance with specifications.
- Assign personnel to observe software installation training.
- Complete installation of client software on remaining workstations and mobile devices.
- Attend onsite deployment training sufficient to enable user proficiency.
- Complete online training.

WatchGuard Deliverables

- Provide a pre-installation preparation checklist.
- Provide installation guide.
- Provide training overviews on hardware/software and system administration for County during deployment dates.

1.9 Infrastructure Validation

Hardware will be installed on the network to facilitate provisioning, testing, and will be used to provide instruction to County personnel after the complete software installation.

WatchGuard Responsibilities

- Verify that the server is properly racked and connected to the network.
- Verify that access points are properly installed and connected to the network.
- Verify that transfer stations are connected to the network and configured.

County Responsibilities

- Verify that the server network has access to the internet for software installation and updates.
- Verify that the network routing is correct for the transfer stations and access points to communicate with the server.
- Verify that the client computers can access the server on the required ports.

1.9.1 Hardware Installation

Physical installation of hardware (i.e. servers, cameras, Access Points, WiFi docs, etc.) are not included in the standard scope of the solution. If a custom quote for installations is included in this purchase, WatchGuard will manage the subcontractor and their deliverables as part of this SOW.

Customers who perform or procure their own installations assume all installation responsibilities including cost, oversight and risk.

1.10 SYSTEM TRAINING

Training and knowledge sharing are important aspects of our overall solution. WatchGuard ' goal is to help all stakeholders (officers, supervisors, system administrators, installers, etc.) obtain a level of training required for their specific role. To achieve this goal, we will conduct formal training classes and provide useful reference documentation for the operation of the system. WatchGuard support staff will also be available to assist 24 hours a day, seven days a week

The training and handoff phase of implementation will last approximately five days, the five days include the following:

- 3 days of End-User Training – 3 Classes per day
- 1 day of Admin Training
- 1 day of Train the Trainer

WatchGuard training consists of both computer-based (online) and instructor-led (on-site or remote). Training delivery methods vary depending on course content. Self-paced online training courses, additional live training, documentation and resources can be accessed and registered for on the WatchGuard Learning eXperience Portal (LXP).

Class Name	Description	Participants	Class Size
End User Training	Training of Franklin County staff will take place onsite as needed for the in-car user experience and will take approximately 1 to 2 hours per class.	End-User / Officer	Up to 15
Admin Training	This classroom based comprehensive training includes camera user, administrative functions, troubleshooting, and CommandCentral Evidence configuration and management. The training will consume an entire day and can be sectioned off, if needed by Franklin County Ohio, to isolate certain areas for certain users.	Supervisors and Administrative staff responsible for CommandCentral Evidence	Up to 20
CommandCentral Evidence User Training	This video or classroom based training is intended to train users to search for and produce evidence.	Admin staff / Prosecutors, as appropriate	N/A
CommandCentral Evidence Admin Training	This training is intended to train Information Technology support personnel on the operations aspects of the CommandCentral Evidence system and servers (if applicable). This training can be provided onsite or via web session and is included with CommandCentral Evidence installation (if applicable).	IT staff	N/A

Class Name	Description	Participants	Class Size
Online Training	Available with two courses: Basic Operation and using CommandCentral Evidence software. These classes are self-paced and include an assessment at the end of each course. The results can be provided to Supervisors if needed. A list of names and email addresses is necessary for sign up.	Determined by Franklin County Ohio	N/A

1.10.1 Online Training

Online training is made available to the County via WatchGuard's LXP. This subscription service provides the County with continual access to our library of online learning content and allows users the benefit of learning at times convenient to them. Content is added and updated on a regular basis to keep information current. This training modality allows the County to engage in training when convenient.

- Access to WatchGuard's LXP is included in the SaaS subscription, no additional charges to the County during the contract term
- County will have unlimited number of user access to the WatchGuard's LXP during the contract term

A list of available online training courses can be found in the Training Plan.

WatchGuard Responsibilities

- Designate a LXP Administrator to work with the County.
- Establish an accessible instance of the LXP for the County.
- Organize content to align with the County's selected technologies.
- Create initial County user accounts and a single Primary Administrator account.
- During on-boarding, assist the County with LXP usage by providing training and job aids as needed.
- Create and maintain user role Learning Paths defined by the County.
- Install security patches when available.
- Provide technical support for user account and access issues, base system functionality, and WatchGuard -managed content.
- Monitor the Learning Subscription server. Provide support for server incidents.

County Responsibilities

- Provide user information for the initial creation of accounts.
- Provide network and internet connectivity for the County's users to access the LXP.
- The County's primary LXP administrator should complete the following self-paced training: LXP Introduction online course (LXP0001), LXP Primary Site Administrator Overview online course (LXP0002), and LXP Group Administrator Overview (LXP0003)
- Advise agency learners of the availability of training via the LXP.
- Ensure users complete LXP training in accordance with the Project Schedule.
- Order and maintain subscriptions to access WatchGuard's LXP.
- Contact WatchGuard to engage Technical Support when needed.

Exhibit 1

WatchGuard Deliverables

- Learning Experience Portal (LXP) Enablement.

1.10.2 Instructor-Led Training (Onsite and Remote)

A list of Instructor-Led and Virtual Instructor-Led courses can be found in the Training Plan.

WatchGuard Responsibilities

- Deliver User Guides and training materials in electronic .PDF format.
- Perform training in accordance with the Training Plan.
- Provide County with training Attendance Rosters and summarize any pertinent observations that may impact end user training.

County Responsibilities

- Supply classrooms with a workstation for the instructor (if Onsite) and at least one workstation for every student based on the requirements listed in the Training Plan.
- Designate training representatives who will work with the WatchGuard trainers in the delivery of training.
- Conduct end user training in accordance with the Project Schedule.

WatchGuard Deliverables

- Electronic versions of User Guides and training materials.
- Attendance Rosters.
- Technical Training Catalog.

1.11 Functional Validation and Project Closure

The objective of Functional Validation is to demonstrate the features and functions of the system in the County’s provisioned environment. The functional demonstration may not exercise all functions of the system, if identified as not being applicable to the County’s operations or for which the system has not been provisioned. The functional demonstration is a critical activity that must occur following the completion of provisioning.

WatchGuard Responsibilities

- Conduct a power on functional demonstration of the installed system per the deployment checklist
- Manage to resolution any documented punch list items noted on the deployment checklist.
- Provide trip report outlining all activities completed during the installation as well as outstanding follow up items
- Provide an overview of the support process and how to request support.
- Walk through support resources, web ticket entry and escalation procedures.
- Provide a County survey upon closure of the project.

County Responsibilities

- Witness the functional demonstration and acknowledge its completion via signature on the deployment checklist.
- Participate in prioritizing the punch list.
- Coordinate and manage County action as noted in the punch list.

- Provide signatory approval on the deployment checklist providing WatchGuard with final acceptance.
- Complete County Survey

1.12 Transition to Support and Customer Success

Following the completion of the activation of CommandCentral components, implementation activities are complete. The transition to the WatchGuard' support organization completes the implementation activities.

Customer Success is the main point of contact as you integrate this solution into your agency's business processes. Our team will work with you to ensure CommandCentral Evidence has met your expectations and that the solution satisfies your goals and objectives. Contact Customer Success at CommandCentralCS@motorolasolutions.com.

Our Customer Support team will be the point of contact for technical support concerns you might have and can be reached either by phone at 1-800-MSI-HELP (option x4, x4, x3) or by emailing support-commandcentral@motorolasolutions.com.

WatchGuard Responsibilities

- Provide the County with WatchGuard's support engagement process and contact information.
- Gather contact information for the County users authorized to engage WatchGuard support.

County Responsibilities

- Provide WatchGuard with specific contact information for those users authorized to engage WatchGuard's support.
- Engage the WatchGuard support organization as needed.

Completion Criteria

Conclusion of the handover to support and the implementation is complete.

Exhibit 1

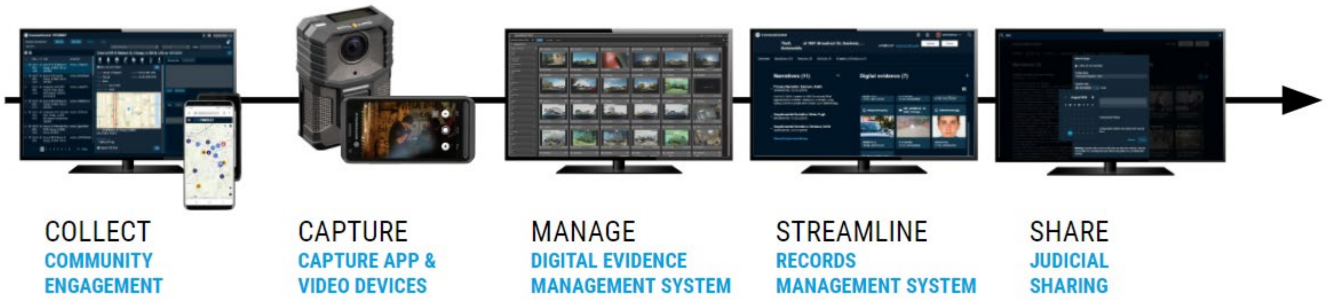
Statement of Work and Investment Summary

Section 2

Video-as-a-Service Solution Description

2.1 Overview

Video-as-a-Service is a subscription-based solution that enhances video policing programs with a robust camera system and digital evidence management tools. This end-to-end service streamlines the collection, capture, management, and sharing of data to and from multiple sources.


COLLECT
COMMUNITY ENGAGEMENT
CAPTURE
CAPTURE APP & VIDEO DEVICES
MANAGE
DIGITAL EVIDENCE MANAGEMENT SYSTEM
STREAMLINE
RECORDS MANAGEMENT SYSTEM
SHARE
JUDICIAL SHARING

Video-as-a-Service combines features from the CommandCentral platform to remove data silos and streamline access to digital evidence:

- CommandCentral Community allows users to gather evidence via a secure, case-specific agency link.
- CommandCentral Evidence allows users to view, redact, tag, and audit evidence from different sources.
- CommandCentral Records allows users to view and share case-related data from a single user interface.

Video-as-a-Service is available at a monthly service cost, without any upfront investment. The monthly service costs cover the camera system, software, video storage, and maintenance. This price structure enables agencies to quickly deploy a new camera system.

This service offers three camera system hardware options: the WatchGuard V300 body-worn camera, the 4RE in-car video system, and a combined solution that integrates these devices. These options are described more fully below.

Exhibit 1

2.1.1 WatchGuard V300 Body-Worn Camera

The WatchGuard V300 HD body-worn camera provides extended operation during long shifts. To support this continuous operation, officers can easily detach and swap the battery. Charged spares can remain in a docking station for a quick shift change. This enables agencies to pool camera usage by reassigning inbound cameras to outbound officers. This keeps cameras in the field, where they are most needed.

The V300 camera is easy to activate, with four control buttons and single-press recording. If an officer does not trigger a recording, the device still captures important video evidence with the Record-After-the-Fact® technology. This feature ensures important details are captured for post-incident review.

The V300 supports automatic wireless upload of video evidence, allowing officers to stay in contact from the field without distraction. The WatchGuard V300 uploads to CommandCentral Evidence via a WiFi or broadband network, such as LTE or FirstNet.

WatchGuard V300 specifications include the following:

- 4k sensor, 1080p max resolution capture, and high dynamic range.
- 128GB of memory ensures space for a full day of recorded events.
- IP67 rating for all-weather operation.
- Top backlit LCD display to view status updates on the go.
- Dual-microphone noise reduction.
- Lens distortion correction for clear video footage.
- Built-in GPS, WiFi, and Bluetooth.

2.1.2 WatchGuard 4RE In-Car Video System

The WatchGuard 4RE In-Car Video System is a robust system that provides panoramic HD video coverage from a vehicle. This system integrates two cameras in a ruggedized housing. A primary camera provides normal coverage area that can be aimed as needed via a turret-mounted lense. A panoramic camera captures a wider single-camera view that is fixed in place.Together, these cameras use multi-resolution recording to capture critical event detail while on patrol.

The 4RE system features an icon-driven interface and intuitive controls to streamline field operations. Users can program various sensors to activate a new record event. These sensors include emergency lights, siren, auxiliary input, wireless microphone, vehicle speed, and crash detection. If a recording was not triggered by the user or one of these sensors, the device still captures important video evidence with the Record-After-the-Fact® technology. The system supports wireless video footage upload to CommandCentral Evidence via a WiFi or broadband network, such as LTE or FirstNet.

Exhibit 1

WatchGuard 4RE specifications include the following:

- Up to 80 hours of HD video recording.
- 256 GB storage capacity.
- Certified to MIL STD 810-G standard.
- Integrated GPS and crash detection.
- Automatic Camera triggers from vehicle equipment.

2.1.3 Fully Integrated Solution

The 4RE In-Car System links with V300 body-worn cameras to create a unified video-policing system. Any camera (in-car or body-worn) can initiate a recording. Upon initiation, the other cameras will also begin recording. This feature captures an incident from multiple vantage points and synchronizes footage for playback and sharing. No one camera acts as a central controller, removing a single point of failure from the system.

The integrated system includes the body camera system, in-car system, and V300 WiFi dock. When a body-worn camera is docked in a vehicle, the device can upload data to CommandCentral Evidence via broadband networks such as LTE or FirstNet. This ensures command center staff receive up-to-date information to inform better decisions.

Video-as-a-Service provides unlimited storage for events captured by the WatchGuard 4RE and V300 systems where the applied data retention period does not exceed one year for non-evidentiary recordings or 10 years for evidentiary recordings (recordings associated with a case). Additionally, the video recording policy must be event-based (policies that require officers to record their entire shift will not qualify for this plan). For non-camera data storage (data not captured by the body camera and/or in-car system), agencies receive 50GB of storage per device, per month, averaged across all devices in the program.

The following sections detail the CommandCentral Community Standard, Records Starter, and Evidence software features that enhance the body-worn cameras and in-car video systems.

Hybrid Option: See Section 2.02 of the Software as a Service Agreement.

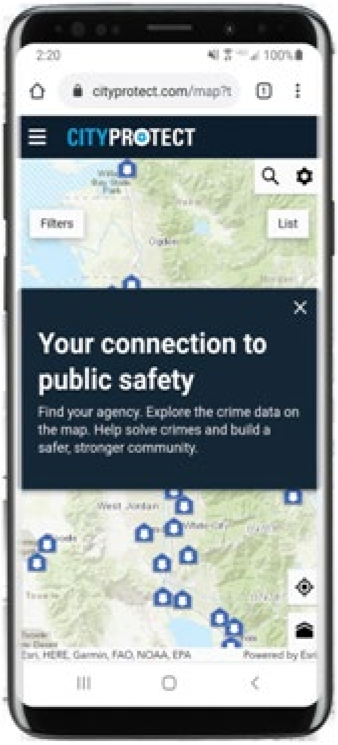
2.2 THE COMMANDCENTRAL PLATFORM

Video-as-a-Service provides capabilities from Motorola Solutions' CommandCentral platform. This platform provides interconnected solutions that unify data and streamline public safety workflows from a tip or call to case closure. Through single sign-on capabilities, your personnel can access all CommandCentral applications with one agency username and password for a more streamlined workflow. The CommandCentral platform puts your agency's information to better use, improves safety for critical personnel, and helps keep your focus on the communities you serve.

CommandCentral is built to evolve over time, maximizing the value of existing investments while adopting new capabilities that better meet your personnel's growing needs. With cloud-based services and an agile development methodology through constant user feedback, Motorola Solutions can rapidly deliver new features and functionality in a more manageable, non-intrusive way.

2.3 COMMANDCENTRAL COMMUNITY

As part of Video-as-a-Service, Motorola Solutions' CommandCentral Community enhances the partnership between your agency and the community. As the foundation for transparent community engagement, this solution streamlines the flow of information between your agency and the people you serve. CommandCentral Community's toolkit helps build public trust and push your investment further. CommandCentral Community functionality can be integrated with the solutions your agency already uses to reduce the need for headcount and increase the value of community intelligence.



Your connection to public safety

Find your agency. Explore the crime data on the map. Help solve crimes and build a safer, stronger community.

The CommandCentral Community experience centers around CityProtect.com. This mobile-friendly webpage offers citizens a centralized set of tools to contribute to public safety. The tools and forms within CityProtect create a dialogue with your community and promote the value of citizen intelligence. Sharing and receiving important information is streamlined to make engagement easier.

2.3.1 Agency Page

This community solution provides a dedicated, public-facing webpage for your agency. This customizable page offers a unique URL to serve as the hub for community interaction with access to the tools for the public to connect with your agency.

The agency page shows quick, rotating messages—bulletins (up to five 244-character messages)—to keep the public informed. Your agency will control the order, schedule, and expiration date of these bulletins. The page also integrates an agency's social media feeds to further unify communications.

2.3.2 Digital Evidence Collection

CommandCentral Community's Digital Evidence Collection allows your agency to collect case-specific digital material without needing a personal device or physical storage, such as CDs, USBs, or other devices generally checked into physical evidence stores. This can be managed using the CommandCentral digital evidence management tools.

2.3.3 Public Submissions

The public can submit information online with an easy-to-use interface. There are multiple self-service form options for online submissions, including anonymous tipping, non-emergency online submissions, and digital evidence collection. Your agency can decide which of these forms to deploy and how to personalize these forms with built-in form management tools. The public can use these forms on CityProtect to submit tips, or they can use anonymous SMS communication. Together, these submissions help agencies build a more accurate operating picture using information from the community.

Exhibit 1
Statement of Work and Investment Summary

These public submissions are managed in one location and can be linked to your records to create a more efficient workflow. Submissions from the community are collected in the Community Inbox, where your agency can review submissions before they are entered into the master tables to avoid duplication. This leads to cleaner incident record data, while preserving the original record for future reference. The consolidated record view shows all linked submissions in one, complete location.

2.3.4 Crime Map

CommandCentral Community's Crime Map is built into the CityProtect home page. Crime Map automatically publishes crime data and incident information from your RMS or CAD system to an interactive, online map. This map keeps the public informed of local crime activity and offers visibility into your operations. CommandCentral Community's Crime Map provides the following:

- Incident data display with up to hourly update.
- Primary Agency shapefile.
- Sex offender options.
- Crime data download option and action link.

Users can customize and manage data published on Crime Map so that only appropriate public information is shared.

2.3.5 Camera Registration

Camera Registration allows citizens to register their residential or commercial security cameras in CityProtect. Each community member can create a free CityProtect user account to manage their camera information. Your agency can then access the location of these cameras and contact the owner for potential video evidence. The data from these accounts is visualized in a variety of CommandCentral applications, such as CommandCentral Aware and CommandCentral Investigate.

2.4 COMMANDCENTRAL RECORDS STARTER

As part of Video-as-a-Service, Motorola Solutions' CommandCentral Records Starter is an easy-to-use solution that enables users to quickly and easily search video, audio, images, and other digital content from incidents. This content is centralized in the Cloud, streamlining access and management of this data across your organization. This approach reduces the complexity of records management. As a result, CommandCentral Records Starter saves your personnel valuable time and allows them to focus on their communities.

CommandCentral Records Starter offers users the following features to benefit records management workflows:

- Consolidated Record View – Enter and view incident information, officer narrative, and digital evidence with one user interface, allowing officers to spend more time in the field.
- Task Creation and Assignment – View, create, and assign tasks or projects for the day as part of the Insights Dashboard. This helps build and close cases faster by tracking progress and assigning ownership to activities.

Exhibit 1

- Case Package Sharing – Enter a recipient's email address and email them a link to share the Consolidated Record View.
- Dictated Narrative Transcription – The system enables narratives to be dictated into the CommandCentral Capture app. The audio is transcribed, tagged, associated with the incident, and uploaded to CommandCentral Evidence and CommandCentral Records. This becomes the primary narrative in the Consolidated Record View, providing context for digital evidence. The narrative audio is searchable via Unified Search.
- Assisted Narrative – CommandCentral Records is able to identify the names of individuals already associated with a case when they are mentioned in the primary narrative of the incident record. The names in the primary narrative are linked directly to the named record, helping to identify persons of interest faster and expedite investigations by increasing productivity.
- Data Insights Reporting – Access critical insight with pre-built reports and dashboards to make data-driven decisions. Reports include law incident summary by offenses, by officer, and by officer with full incident detail. These reports are done through Microsoft Power BI.
- Master Indexes – Validate data on persons, vehicles, and organizations against the master indexes, which have been verified. For example, agencies can verify that an arrested person, person of interest, or suspect's information is accurate.

2.5 COMMANDCENTRAL EVIDENCE

CommandCentral Evidence is part of Video-as-a-Service, providing a cloud-based digital evidence management application that streamlines collecting, securing, and managing multimedia evidence content. CommandCentral Evidence helps users build a secure digital evidence library with data from multiple sources. Users create this unified evidence storage framework by uploading digital evidence from a variety of sources to CommandCentral Evidence to quickly build cases. Evidence stored within CommandCentral Evidence is easy to search, correlate, and review alongside other case-related information from your CAD or RMS database. Relevant content can be marked and intelligently sorted to quickly locate critical information from a centralized touchpoint. This unified storage framework allows personnel to make informed decisions from a more organized and complete case evidence view, while offering an access control system to allow only authorized personnel to view sensitive information.

2.5.1 Store and Manage

CommandCentral Evidence simplifies building a secure digital evidence library by incorporating data from multiple sources into a unified evidence storage framework. Products from Motorola Solutions, such as body-worn cameras, in-car cameras, the CommandCentral Capture application, and other

CommandCentral software automatically transmit data to CommandCentral Evidence. This saves the time and effort needed to manually upload files. Once the content is securely stored in CommandCentral Evidence, content management is more efficient.

CommandCentral Evidence streamlines content management workflows, with tags and metadata that make it easier to correlate, search, and manage evidence. The application automatically links evidence based on the tags and metadata attached to those files, helping users find additional contextual information on an incident and build cases quickly. Users can search and filter content to locate additional relevant data to link to a case or incident. To quickly access evidence items that they frequently need to reference, users can group or bookmark files within the CommandCentral Evidence interface.

Video-as-a-Service provides unlimited storage for events captured by the WatchGuard 4RE and V300 systems where the applied data retention period does not exceed one year for non-evidentiary recordings or 10 years for evidentiary recordings (recordings associated with a case). Additionally, the video recording policy must be event-based (policies that require officers to record their entire shift will not qualify for this plan). For non-camera data storage (data not captured by the body camera and/or in-car system), agencies receive 50GB of storage per device, per month, averaged across all devices in the program.

2.5.2 Judicial Sharing and Redaction

With Judicial Sharing, personnel can share validated evidence items with judicial partners for use in court. This allows judicial partners to access digital evidence files as part of the CommandCentral Evidence application's verifiable chain of custody, maintaining the admissibility of shared items.

The application's efficient redaction and sharing capabilities enable personnel to release appropriate items to the community, providing a transparent incident record in urgent and day-to-day circumstances. With these redaction tools, users can obscure personally identifiable information across video frames. This protects the privacy of individuals in the video, while still providing the public with clear incident records.

2.6 COMMANDCENTRAL CAPTURE APPLICATION

The CommandCentral Capture Application is an integrated smartphone application with direct, secure upload to CommandCentral Evidence. This allows users to capture multimedia evidence with advanced camera controls. Integrated metadata population and tagging provides immediate access to content in CommandCentral Evidence. Application isolation ensures evidence is not accessible by other apps and ensures an uncompromised chain of custody from the moment of capture.

The CommandCentral Capture App is a capture source for officers, detectives, command staff, supervisors, and other law enforcement personnel. The user interface for the CommandCentral Capture App is in a single ecosystem with CommandCentral Evidence. Users can easily and securely capture and upload digital evidence through CommandCentral Capture to CommandCentral Evidence. The application is available on iOS and Android.

2.7 CAD/RMS Correlation Interface

Video-as-a-Service includes a Motorola CAD/RMS correlation interface that uses different mechanisms (DB polling, REST, file polling) to extract required data fields. The data fields are then mapped to a corresponding format accepted by CommandCentral Evidence, and sent to the respective applications correlation service. Those fields are accepted by the correlation service, based on the logic applied for your agency.

Data fields include the following:

- AgencyName.
- IncidentID.
- IncidentData.
- Latitude.
- Longitude.
- OfficerID (officer's email address or badge ID).
- CreatedTimestamp.
- UpdatedTimestamp.

This interface supports the following use cases:

- Retrieve data containing required fields from third-party and Motorola Solutions CAD/RMS systems.
- Map fields and send data in payload to the correlation service.
- Correlation based on time + geographic location.
- Correlation based on time + officer ID.

2.7.1 Server Requirements

A customer-provided virtual machine is required to support the CAD/RMS interface. The virtual machine must meet the following minimum specifications:

- 2 vCPU.
- 8GB RAM.
- 40GB Hard Drive.
- VMWare 5.5U2 1 CPU License or Hyper-V License.
- Access to Customer-Provided Internet.

The Customer provided Virtual Machine will allow CloudConnect to be installed to enable CommandCentral cloud applications to connect to on-premises applications, like CAD/RMS systems.

Exhibit 1
Statement of Work and Investment Summary

WATCHGUARD V300
CONTINUOUS-OPERATION BODY CAMERA

The WatchGuard V300 continuous-operation body camera with detachable battery, wireless uploading and expansive storage addresses law enforcement's need for cameras to operate beyond a 12-hour shift.

Exhibit 1
Statement of Work and Investment Summary

KEY FEATURES

DETACHABLE BATTERY – Easily change the WatchGuard V300's rechargeable battery while on the go. Keep an extra battery at the ready for unexpectedly long shifts, extra shifts or part-time jobs where a body camera is required.

AUTOMATIC WIRELESS UPLOADING – Send critical video back to headquarters while still in the field. When docked in the vehicle, the V300 uploads to evidence management systems via wireless networks like LTE and FirstNet, anytime, anywhere.

INTEGRATED WITH IN-CAR SYSTEM – One or more V300 cameras and a WatchGuard 4RE® in-car system can work seamlessly as a single system, capturing synchronized video of an incident from multiple vantage points.

NATURAL FIELD OF VIEW – Eliminate the fisheye effect from wide-angle lenses that warps video footage. Our distortion correction technology provides a clear and complete evidence review process.

ABSOLUTE ENCRYPTION – Elevate your data security with encryption at rest and in transit technology. V300 guards your data and your reputation.

RECORD-AFTER-THE-FACT – Go back in time and capture video from events days after they happened, even when a recording wasn't automatically triggered or initiated by the officer. Don't rely on mere seconds of pre-event buffering to prove your case.

SPECIFICATIONS

Dimensions	2.6 x 1.1 x 3.6 in (65 x 29 x 91 mm) W x D x H
Weight	6.8 oz (193 g)
Storage	128 GB
IP Rating	IP 67
Resolution	1080p, 720p and 480p
Microphones	Dual
Vertical Field of View	Electronic Turret +15° /- 20°
Field of View	130°
Encryption	At rest and in transit

For more information, visit www.motorolasolutions.com/v300

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**

Exhibit 1
Statement of Work and Investment Summary

WatchGuard Video
□1□ E. Exchange
Allen, TX 7□002
□P□□00-□0□-□7□□ □F□212-□□□-□□□1

MOTOROLA SOLUTIONS

Prepared For:
Fran□lin County Sheriff□s Office - Attention: Julie Whiting
□□0 Body Camera - V□00

Sourcewell Contract #: 010720-WCH

QUOTATION - _DF-0074-06

DATE: 01-27-22

Deliverables / Materials / Services	Qty	Sell Price	Amount
Body-worn camera and evidence management software - 5 Year Video-as-a-Service Package @ $49 per Month AAS-BWC-□YR-001 ***(PaaS)*** Video-as-a-Service includes CommandCentral Evidence, the cloud-based evidence management system with unlimited device storage and unlimited cloud sharing. 1 □ser License per Body Worn Camera. □0 GB of non-device storage included per device, averaged across all devices in the program CommandCentral Evidence, Records, Redaction, Sharing, Community Engagement capabilities and capture application included. Body-worn camera □battery □ choice of mount included□ Third year technology □Hardware□refresh. □-year agreement □billed Quarterly or Annually□ Advanced hardware replacement service □ 2□7 support □o-Fault hardware warranty	**650**	**$2,940.00**	**$1,911,000.00**
CC Evidence Unlimited Data Storage for ICV SSV00S027□□A ***(PaaS)*** □nlimited for In Car Video Priced Annually: □□2 per car per month	**375**	**$624.00**	**$234,000.00**

Exhibit 1
Statement of Work and Investment Summary

CommandCentral Evidence PLUS - Five (5) Year Subscription SSV00S02□01A-0□ Digital Evidence Management Field Response Application Records Management PL□S these additional features: Advanced Tools: Redaction, Transcription, and Reporting Community Interaction Tools Case Sharing Capabilities Five □□□Year Subscription Duration Priced Per □amed □ser □Qty □# of □sers□	**20**	**$585.00**	**$11,700.00**
V300, Battery, Removable and Rechargable, 3.8V, 4180mAh WGP02□1□	**650**	**$99.00**	**$64,350.00**
V300 WiFi In-car Radio Base Bundle, includes Radio Base and Smart PoE Switch. IV-AC□-BD-V□--- V□00 WiFi In-car Radio Base Bundle WiFi Charging Radio Base Smart PoE Switch Cables and Brac□ets	**75**	**$545.00**	**$40,875.00**
Transfer Station (8 Bay) Video-as-a-Service Package @ $30 per Month AAS-BWC-XFS-DOC ***(PaaS)*** □-Bay Ethernet Transfer Station Ethernet Cable, Rac□mount □optional□□ Power Cord	**40**	**$1,800.00**	**$72,000.00**
V300 CAMERA MOUNT, M330 MOLLE LOOP W/ QUICK RELEASE LEVERS WGP02□□□	**650**	**$50.00**	**$32,500.00**
Upload Server On-Premise - Video-as-a-Service Package @ $100 per Month AAS-□PL-SVR-001 ***(PaaS)*** Store and Forward Server for Fast Video Offload □se with in-car upload via Access Point or Body Worn Camera Transfer Stations On-premise deployment, 1□ rac□mount, □TB of storage, 1□GB RAM, 2x10G networ□cards, Intel Xeon processor □HDW-□PL-SRV-□01□ □Year Warranty	**2**	**$6,000.00**	**$12,000.00**

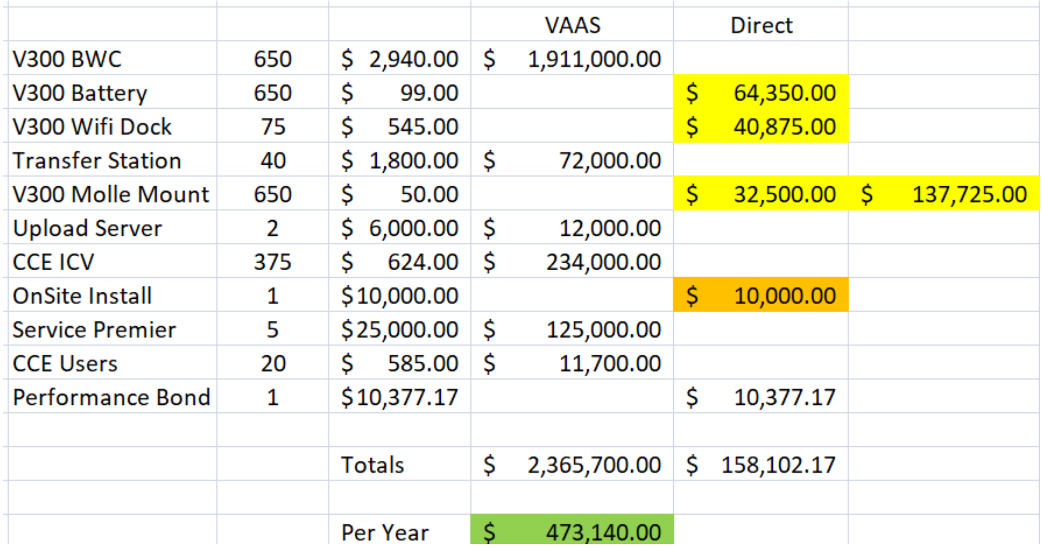
Exhibit 1

Statement of Work and Investment Summary

Managed Software Installation Service; Complete On-Site Install, Training, Configuration, Project Management, Consultation WGW00122-□02 ***(PaaS)***	**1**	**$10,000.00**	**$10,000.00**
Premier Support Service (Annual Subscription) WGW001□□ ***(PaaS)*** Premier Support Service provides a dedicated Technical Account Manager □TAM□, who acts as a customer advocate for support activities, to proactively monitor the system, communicate with the customer and ta□e recovery actions to remedy incidents. Premier Support highlights: Incident Management to restore normal service operation as quic□ly as possible and minimi□e impact on normal operations, if and when incidents occur. Release Management of licensed, tested, and version-certified software, which functions as intended when introduced into existing customer infrastructure. Change Management to develop and interloc□with the customer’s change management processes. Quarterly Business Reviews to ensure continued alignment around the customer’s operational goals and video solutions performance. Annual System Health Chec□to evaluate the operating status, configuration, alarms and performance of major system components. See Premier Support SOW for a complete list of services.	**5**	**$25,000.00**	**$125,000.00**
Performance Bond Performance Bond ***(PaaS)***	**1**	**$10,377.17**	**$10,377.17**

Exhibit 1
Statement of Work and Investment Summary

INVESTMENT SUMMARY



			VAAS	Direct	
V300 BWC	650	$ 2,940.00	$ 1,911,000.00		
V300 Battery	650	$ 99.00		$ 64,350.00	
V300 Wifi Dock	75	$ 545.00		$ 40,875.00	
Transfer Station	40	$ 1,800.00	$ 72,000.00		
V300 Molle Mount	650	$ 50.00		$ 32,500.00	$ 137,725.00
Upload Server	2	$ 6,000.00	$ 12,000.00		
CCE ICV	375	$ 624.00	$ 234,000.00		
OnSite Install	1	$10,000.00		$ 10,000.00	
Service Premier	5	$25,000.00	$ 125,000.00		
CCE Users	20	$ 585.00	$ 11,700.00		
Performance Bond	1	$10,377.17		$ 10,377.17	
		Totals	$ 2,365,700.00	$ 158,102.17	
		Per Year	$ 473,140.00		

Fee Payment Schedule:

Implementation Costs billable upon delivery, completion and acceptance by the County of each deliverable:

V300 Battery	$64,350
V300 WiFi Dock	$40,875
V300 Molle Mount	$32,500
OnSite Install	$10,000*
*incl. Training Costs (5 Days)	
Performance Bond	$10,377.17
Total Implementation =	$158,102.17

SaaS Fees:	$473,140.00/annually (Yrs 1-5)
Total SaaS Fees =	$2,365,700.00

Total Cost =	**$2,523,802.17**

Go-Live Phases (est. 5-month period; see timeline below):

1. Patrol
2. Support Services (SWAT, etc.)
3. Corrections
4. Security Operations (Courthouses, etc.)
5. Investigations
6. Administration (Civil, Real Estate, etc.)

Year 1 SaaS Fee Payment

$236,570 (50% of Yr 1 SaaS Fee) upon Go-Live of Phase 1

$236,570 (50% of Yr 1 SaaS Fee) upon Final Acceptance

SaaS Fees for Years 2 through 5 will be billable annually in advance, with Year 2 SaaS Fees billable 12-months after successful Go-Live of the Patrol Phase.

Exhibit 1
Statement of Work and Investment Summary

Proposed Milestone Timeline

Task Name	Duration
Training Management Plan	**125 days**
Super User Patrol Training	5 days
Patrol Test Group	26 days
Patrol Operations	**31 days**
Training Plan Development	2 days
Supervisor Training	8 days
Officer Training	20 days
Go Live	1 day
Support Services	**33 days**
Training Plan Development	2 days
Supervisor Training	10 days
Officer Training	20 days
Go Live	1 day
Corrections	**35 days**
Training Plan Development	2 days
Supervisor Training	10 days
Officer Training	30 days
Go Live	1 day
Security Operations	**33 days**
Training Plan Development	2 days
Supervisor Training	10 days
Officer Training	20 days
Go Live	1 day
Investigations	**35 days**
Training Plan Development	2 days
Supervisor Training	10 days
Officer Training	20 days
Go Live	1 day
Administration	**37 days**
Training Plan Development	2 days
Supervisor Training	10 days
Officer Training	20 days
Go Live	5 days

Exhibit 1
Statement of Work and Investment Summary

Franklin County, OH - Preliminary Project Schedule

ID	Task Name	Duration	Start	Finish
1	**Franklin County WatchGuard Implementation**	**271 d**	**Tue 2/8/22**	**Thu 3/2/23**
2	**Contract**	**16 d**	**Tue 2/8/22**	**Wed 3/2/22**
3	Contract Award	1 d	Tue 2/8/22	Wed 2/9/22
4	Peformance Bond (within 10 days of Contract)	10 d	Wed 2/9/22	Wed 2/23/22
5	Contract Administration	12 d	Wed 2/9/22	Fri 2/25/22
6	Project Kick-Off	1 d	Fri 2/25/22	Mon 2/28/22
7	IT Welcome Call / Review	2 d	Mon 2/28/22	Wed 3/2/22
8	**Order Processing**	**5 d**	**Mon 2/28/22**	**Mon 3/7/22**
9	Process Orders	4 d	Mon 2/28/22	Fri 3/4/22
10	Trial Validation	1 d	Fri 3/4/22	Mon 3/7/22
11	Order Bridged	0 d	Mon 3/7/22	Mon 3/7/22
12	**Manufacturing**	**90 d**	**Mon 3/7/22**	**Wed 7/13/22**
13	Manufacture WatchGuard/Motorola Equipment	80 d	Mon 3/7/22	Tue 6/28/22
14	Ship Equipment to Field	5 d	Tue 6/28/22	Wed 7/6/22
15	Perform Equipment Inventory	5 d	Wed 7/6/22	Wed 7/13/22
16	**Command Central Evidence Installation**	**103 d**	**Wed 3/2/22**	**Wed 7/27/22**
17	Connectivity - Internet (CUSTOMER RESPONSIBILITY)	45 d	Wed 3/2/22	Wed 5/4/22
18	Command Central Evidence Installation	10 d	Wed 7/13/22	Wed 7/27/22
19	Command Central Evidence Install Complete	0 d	Wed 7/27/22	Wed 7/27/22
20	**Installation in Vehicles & Deploy Patrol BWC's**	**25 d**	**Wed 7/13/22**	**Wed 8/17/22**
21	Install WI-FI dock in Vehicles (CUSTOMER RESPONSIBILITY)	25 d	Wed 7/13/22	Wed 8/17/22
22	Transfer and Upload Station Installation	20 d	Wed 7/13/22	Wed 8/10/22
23	Initial Deploy: Program/Configure/Deploy BWC - Patrol	10 d	Wed 8/3/22	Wed 8/17/22
24	Installation Docks, Patrol BWC Deploy Complete	0 d	Wed 8/17/22	Wed 8/17/22
25	**System Validation**	**28 d**	**Wed 8/17/22**	**Tue 9/27/22**
26	Perform Functional Validation	3 d	Wed 8/17/22	Mon 8/22/22
27	Perform Field System Validation	25 d	Mon 8/22/22	Tue 9/27/22
28	Functional and System Validation Complete	0 d	Tue 9/27/22	Tue 9/27/22
29	**Training**	**70 d**	**Tue 9/27/22**	**Thu 1/5/23**
30	Perform Training - Administrator/CCE/Patrol End User/Train the Trainer	10 d	Tue 9/27/22	Tue 10/11/22
31	Perform Training - End User (CUSTOMER REPONSIBILITY)	60 d	Tue 10/11/22	Thu 1/5/23
32	**Go Live - Patrol**	**1 d**	**Tue 10/11/22**	**Wed 10/12/22**
33	Go Live Acceptance - Patrol	1 d	Tue 10/11/22	Wed 10/12/22
34	Go Live Complete - Patrol	0 d	Wed 10/12/22	Wed 10/12/22
35	**Deploy V300 BWC's (CUSTOMER RESPONSIBILITY)**	**100 d**	**Tue 9/27/22**	**Fri 2/17/23**
36	Deploy Support Services	20 d	Tue 9/27/22	Tue 10/25/22
37	Deploy Corrections	20 d	Tue 10/25/22	Tue 11/22/22
38	Deploy Security Operations	20 d	Tue 11/22/22	Thu 12/22/22
39	Deploy Investigations	20 d	Thu 12/22/22	Fri 1/20/23
40	Deploy Administration	20 d	Fri 1/20/23	Fri 2/17/23
41	BWC Installation and Deployment Complete	0 d	Fri 2/17/23	Fri 2/17/23
42	**Finalize**	**9 d**	**Fri 2/17/23**	**Thu 3/2/23**
43	Resolve Punchlist	4 d	Fri 2/17/23	Thu 2/23/23
44	Finalize Documentation	5 d	Thu 2/23/23	Thu 3/2/23
45	Final Acceptance	0 d	Thu 3/2/23	Thu 3/2/23

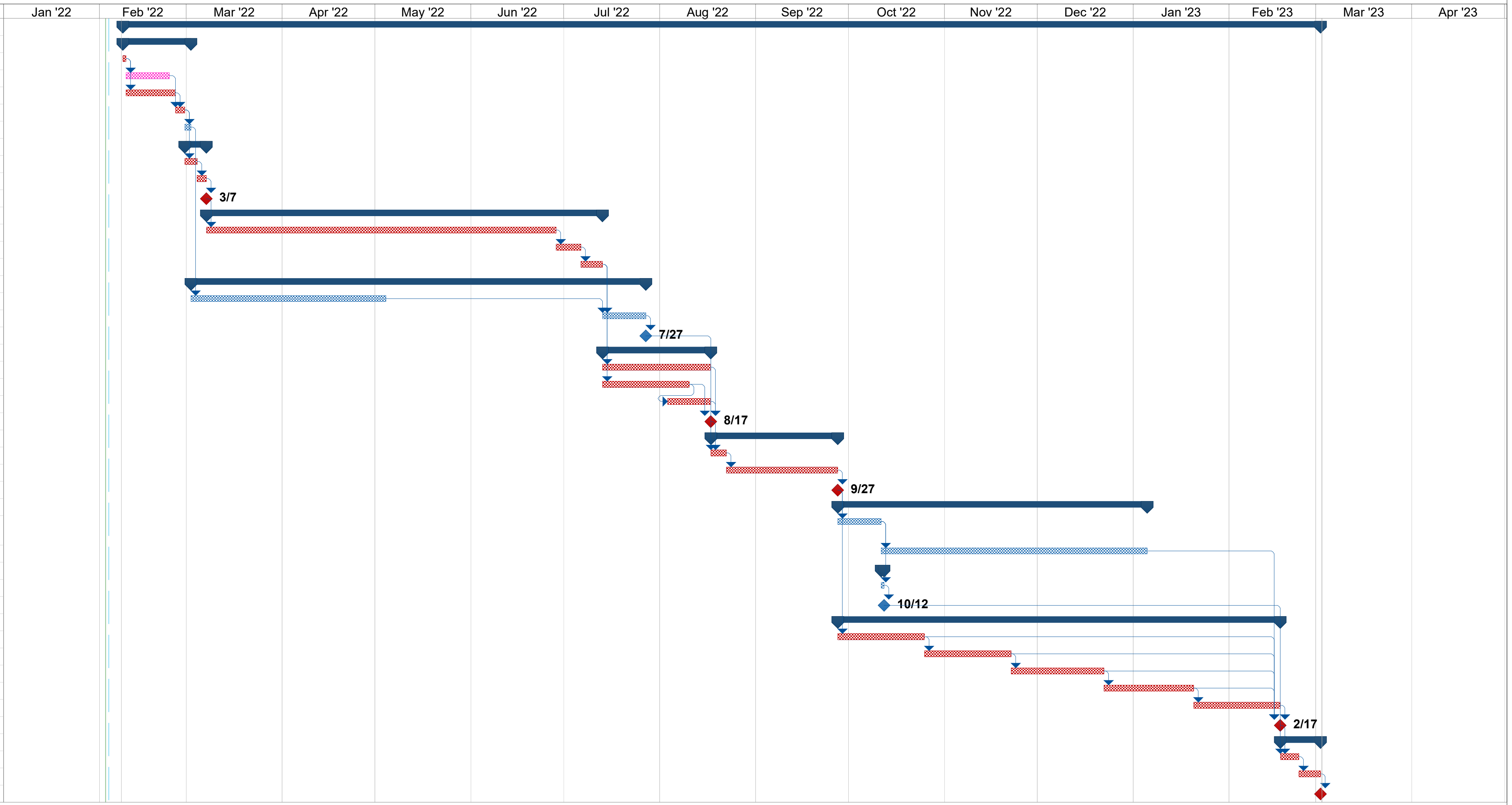


EXHIBIT 2

SOFTWARE AS A SERVICE AGREEMENT

This Software as a Service Agreement is made between WatchGuard and the County.

WHEREAS, the County selected WatchGuard to provide certain products and services set forth in the Statement of Work and Investment Summary, including providing the County with access to WatchGuard's proprietary software products, and WatchGuard desires to provide such products and services under the terms of this Agreement and the Services Contract to which this Agreement is attached;

NOW THEREFORE, in consideration of the foregoing and of the mutual covenants and promises set forth in this Agreement, WatchGuard and the County agree as follows:

Section 1 Definitions

- **"Agreement"** means this Software as a Service Agreement.
- **"Authorized Users"** means County's employees and full-time contractors that are engaged for the purpose of using and supporting Products and Services at the discretion of the County.
- **"County,"** **"means** Franklin County Board of Commissioners and the Franklin County Sheriff's Office.
- **"Configuration"** means processes by which WatchGuard will install and configure the WatchGuard Solution to the County's requirements.
- **"Data"** means those terms as defined in Section 2.03.1 of this Agreement.
- **"Data Storage Capacity"** means the contracted amount of storage capacity for County Data identified in this Agreement Section 2.02.
- **"Defect"** means a failure of the Watchguard hardware or Watchguard Solution to conform to the Functional Descriptions, or their functional equivalent. Future functionality may be updated, modified, or otherwise enhanced through Watchguard's future releases as available or identified in Product Newsletters.
- **"Disaster"** means an event that causes an unrecoverable failure of an operations center, such as fire, flood, etc. A system outage does not constitute a Disaster.
- **"Documentation"** means any online or written documentation related to the use or functionality of the WatchGuard Solution that is provided or otherwise made available to the County, including instructions, user guides, manuals, and other training or self-help documentation.
- **"Effective Date"** means the last signature date set forth in the signature block below.
- **"Equipment"** means the hardware provided by WatchGuard.
- **"Enhancement" or "Update"** means any change to the WatchGuard Software developed by WatchGuard to support or maintain the WatchGuard Software.
- **"Final Acceptance"** means the timeline set forth in Section 8.04 of the Services Contract.
- **"Force Majeure"** means an event beyond the reasonable control of County or WatchGuard, including, without limitation, governmental action, war, riot or civil commotion, fire, natural disaster, pandemic, epidemic, or any other cause that could not with reasonable diligence be foreseen or prevented by County or WatchGuard.
- **"Functional Description"** means the technical and functional specifications as set forth in Exhibit 1 to the Services Contract, and technical and functional specifications as may be updated, modified, and enhanced through WatchGuard's future releases as available or identified in Product Newsletters.
- **"Hosting Solution"** means a WatchGuard Solution provided to and used by the County as a service that includes at least one mobile video product(s) and WatchGuard Software hosted in a data center.
- **"Integrations"** means the connection of new and existing systems to the WatchGuard Software to facilitate the exchange of Data, developed by WatchGuard and identified in the Statement of Work and Investment Summary.

- **“Initial Term”** means five years from the first day following Go-Live acceptance of the first phase.
- **"Investment Summary"** means the agreed upon cost proposal for the products and services attached to the Services Contract as Exhibit 1.
- **“Judicial Partner”** means any entity or individual to which or to whom the County discloses County Data, including, but not limited to, any local, state, or federal agency or regulatory and enforcement agencies, law enforcement agencies, prosecutorial departments, and Courts or other adjudicatory bodies, both within and outside Franklin County, that may need access to County Data from time to time.
- **“Licensed Software”** means the software which is either pre-installed on Equipment or installed on County-provided equipment and licensed to County by WatchGuard for a perpetual or other defined licensed term.
- **“Product”** means, collectively, the Equipment, Licensed Software and Subscription Software.
- **“Product Newsletters”** means technical information relating to the Product, including product releases, cancellations, training and other information as more specifically set forth at the following website: https://www.motorolasolutions.com/en_us/support/technical-product-newsletter.html.
- **"Proper Invoice"** is defined as an itemized invoice that states which WatchGuard deliverable(s) in the milestone payment schedule in Exhibit 1 are being billed, and is otherwise free of defects, discrepancies, errors, or other improprieties. A Proper Invoice should include the invoice remittance address, as designated in the Contract, as well as the name and address of WatchGuard, the billing period, and the cost of the deliverables completed.
- **“Renewal Term”** means one additional five-year term after the Initial Term.
- **"RPO" or "Recovery Point Objective"** means the maximum tolerable period during which County Data may be lost, measured in relation to a Disaster WatchGuard declares, said declaration will not be unreasonably withheld.
- **"RTO" or "Recovery Time Objective"** means the amount of time, after WatchGuard declare a Disaster, within which County access to the WatchGuard Software must be restored.
- **"SaaS Fees"** means the fees for the SaaS Services identified in Exhibit 1 to the Services Contract.
- **"SaaS Service(s)"** means software as a service consisting of system administration, system management, and system monitoring activities that WatchGuard performs for the WatchGuard Software, and includes the right to access and use the WatchGuard Software, receive maintenance and support on the WatchGuard Software, including downtime resolution under the terms of the SLA, and Data storage and archiving pursuant to the terms set forth in this Agreement. SaaS Services do not include support of an operating system or hardware, support outside of WatchGuard normal business hours, or training, consulting, or other professional services.
- **“Services”** means one-time services (implementation and configuration services) as more specifically set forth in Exhibit 1 to the Services Contract. Services does not include SaaS Services.
- "**Security Breach"** means unauthorized access to and acquisition of computerized Data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of the State of Ohio, as defined by Ohio law.
- **"SLA"** means the service level agreement, which details certain responsibilities of the parties related to the WatchGuard Solution and the Hosting Solution. The SLA is attached hereto as Exhibit A.
- **"Solution Host"** means the data center where WatchGuard Software is hosted.
- **"Statement of Work"** means the Services and SaaS Services as governed by the Services Contract and SaaS Agreement, respectively, and outlined in Exhibit 1 to the Services Contract.

- **“Subscription Software”** means licenses of cloud-based software as a service products and other software which is either preinstalled on Equipment or installed on County-provided equipment, but licensed to County by WatchGuard on a subscription basis for the County’s own use in accordance with the SaaS Agreement.
- **"Support Call Process"** means the support call processes available to the County and all Authorized Users who access and use the WatchGuard Solution. WatchGuard’s current Support Call Process is attached as Exhibit B to the SaaS Agreement.
- **"Third Party Terms"** means, if any, the end user license agreement(s) or similar terms, as applicable and attached as Exhibit C.
- **"Third Party Software"** means any software not developed by WatchGuard, as identified in the Investment Summary, and not embedded in the WatchGuard Software.
- **"WatchGuard Software"** means WatchGuard’s Subscription Software, including any Integrations, or other related interfaces identified in the Investment Summary that is hosted in a data center and provided to the County as a Service. The WatchGuard Software may also include embedded third party software that WatchGuard is licensed to embed in WatchGuard proprietary software and sublicense to the County.
- **"WatchGuard Solution"** means the WatchGuard Software and the Hosting Solution on which the software is installed, as designed and implemented by WatchGuard.
- **"WatchGuard"** means WatchGuard Video, Inc

Section 2 SaaS Services, Delivery and License to WatchGuard Software

Section 2.01 Delivery

(a) SaaS Services. During the applicable Term (as defined below), WatchGuard will provide to County the SaaS Service in accordance with the terms of the Agreement. WatchGuard will provide County advance notice (which may be provided electronically) of any planned downtime. Delivery will occur upon County’s receipt of credentials required for access to, and County’s ability to successfully access, the SaaS Service in accordance with the terms of the Agreement.

(b) Modifications. WatchGuard may modify the SaaS Service, any associated recurring Services and any related systems so long as the functionality is not degraded, as determined upon mutual agreement of the parties. Documentation for the SaaS Service may be updated to reflect such modifications. New features or enhancements that are added to any SaaS Service may be subject to additional fees as mutually agreed upon. Any new features or enhancement purchased by the County will be effective upon the execution of a written contract modification, signed by both parties and approved via resolution by the Franklin County Board of Commissioners.

(c) User Credentials. If applicable, WatchGuard will provide County with administrative user credentials for the SaaS Service, and County will ensure such administrative user credentials are accessed and used only by County’s employees with training on their proper use. County will protect, and will cause its users to protect, the confidentiality and security of all user credentials, including any administrative user credentials, and maintain user credential validity, including by updating passwords. WatchGuard shall not be liable for cost and expenses resulting from the County’s or County employees’ misuse of credentials, including any changes to the SaaS Service through such misuse of credentials or user impact arising therefrom. To the extent WatchGuard must provide one-time services to help resolve such changes to the SaaS Service, the parties shall mutually agree on cost and expenses associated with the inoperable SaaS Service.

(d) Documentation. Products and Services may be delivered with documentation for the Equipment, software Products, or data that specifies technical and performance features, capabilities, users, or operation, including training manuals, and other deliverables, such as reports, specifications, designs, plans, drawings, analytics, or other information (collectively, “**Documentation**”). Documentation is and will be owned by WatchGuard, unless otherwise expressly agreed in an Addendum or Ordering Document that certain Documentation will be owned by County. WatchGuard hereby grants County a limited, royalty-free, worldwide, non-exclusive license to use the Documentation solely for its internal business purposes in connection with the Products and Services. Notwithstanding the foregoing, the parties hereto agree that the County will at all times be subject to the release of Documentation in accordance with the Ohio Public Records Act, Ohio Revised Code Section 149.43.

Section 2.02 SaaS Fees

The County agrees to pay WatchGuard an amount not-to-exceed $2,365,700 for SaaS Fees during the Initial Term of this Agreement.

(a) Reserved.

(b) Reserved.

(c) SaaS Fees and Payment.

The County agrees to pay WatchGuard SaaS Fees for recurring SaaS Services after Final Acceptance of the WatchGuard Solution. Those amounts are payable annually, in advance, in accordance with Section 6 Invoicing and Payment below.

(d) Data Storage Capacity shall be as indicated in the Quote included in Exhibit 1 during the term of this Agreement and any Renewal Term hereto.

The parties agree that within twelve months of the Effective Date of the Services Contract, Watchguard shall provide the County with an option to transition from a cloud-based hosted environment to a hybrid environment (the “Hybrid Option”). At the time the Hybrid Option is offered, Watchguard shall have completed all development necessary to commence the transition to the hybrid environment immediately. County shall have no obligation to select the Hybrid Option, but the Hybrid Option shall remain open for at least the Initial Term of the Agreement. As part of the Hybrid Option, Watchguard shall include a proposal to provide to the County all hardware necessary to operate the hybrid environment; however, County may purchase or use hardware from other sources and shall have no obligation to purchase the hardware from Watchguard in the event that the County selects the Hybrid Option. In the event that Watchguard fails to provide the Hybrid Option within the timeframe specified in this paragraph, then the County shall be entitled to a 50% reduction in Year 2 SaaS Fees.

In the event that County decides, in its own discretion, to move forward with the Hybrid Option, Watchguard shall provide all services and support necessary to transition all County Data to the hybrid environment at no cost to the County. If the transition occurs, the parties agree to enter into additional agreement(s) or an Amendment to this Agreement to provide the terms and conditions for the transition and hybrid environment.

Section 2.03 Proprietary Rights; Data and Feedback

2.03.1 Data Definitions. The following terms will have the stated meanings: “**County Contact Data**” means data WatchGuard collects from County, its Authorized Users, and their end users for business contact purposes, including marketing, advertising, licensing and sales purposes; “**Service Use Data**” means data generated by County’s use of the Products and Services or by WatchGuard’s support of the Products and Services, including product performance and error information, activity logs and date and time of use; “**County Data**” means data, information, and content, including images, text, videos, documents, audio, telemetry, location and structured data base records, provided by, through, or on behalf of County, its Authorized Users, and their end users through the use of the Products and Services. County Data does not include County Contact Data, Service Use Data, or information from publicly available sources or other Third-Party Data or WatchGuard Data; **“Third-Party Data”** means information obtained by WatchGuard from publicly available sources or its third party content providers and made available to County through the Products or Services; “**WatchGuard Data**” means data owned or licensed by WatchGuard; “**Feedback**” means comments or information, in oral or written form, given to WatchGuard by County or Authorized Users, including their end users, in connection with or relating to the Products or Services; and **“Process”** or **“Processing”** means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, copying, analyzing, caching, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.03.2 WatchGuard Materials. County acknowledges that WatchGuard may use or provide County with access to software, tools, data, and other materials, including designs, utilities, models, methodologies, systems, and specifications, which WatchGuard has developed or licensed from third parties (including any corrections, bug fixes, enhancements, updates, modifications, adaptations, translations, de-compilations, disassemblies, or derivative works of the foregoing, whether made by WatchGuard or another party) (collectively, "**WatchGuard Materials**"). The Products and Services, WatchGuard Data, Third-Party Data, and Documentation, are considered WatchGuard Materials. Except when WatchGuard has expressly transferred title or other interest to County by way of an Addendum or Ordering Document, the WatchGuard Materials are the property of WatchGuard or its licensors, and WatchGuard or its licensors retain all right, title and interest in and to the WatchGuard Materials (including, all rights in patents, copyrights, trademarks, trade names, trade secrets, know-how, other intellectual property and proprietary rights, and all associated goodwill and moral rights). For clarity, this Agreement does not grant to County any shared development rights in or to any WatchGuard Materials or other intellectual property. WatchGuard and its licensors reserve all rights not expressly granted to County, and no rights, other than those expressly granted herein, are granted to County by implication, estoppel or otherwise. County will not modify, disassemble, reverse engineer, derive source code or create derivative works from, merge with other software, distribute, sublicense, sell, or export the Products and Services or other WatchGuard Materials, or permit any third party to do so.

2.03.3 Ownership of County Data. County retains all right, title and interest, including intellectual property rights, if any, in and to County Data. WatchGuard acquires no rights to County Data except those rights granted under this Agreement including the right to Process and use the County Data as set forth in **Section 2.03.4 – Processing County Data** below and in other applicable Addenda. The Parties agree that with regard to the Processing of personal information which may be part of County Data, County is the controller and WatchGuard is the processor, and may engage sub-processors pursuant to **Section 2.03.4(c) – Sub-processors**.

2.03.4 Processing County Data.

(a) WatchGuard Use of County Data. To the extent permitted by law, County grants WatchGuard and its subcontractors a right to use County Data. For any use, the County Data must be anonymized. WatchGuard acknowledges and agrees that County Data may contain confidential information that may not be viewed or disclosed by WatchGuard without written authorization from the County.

(c) Sub-processors. Subject to WatchGuard's request and County's prior written approval, WatchGuard may engage sub-processors to process County Data in accordance with this Agreement. When engaging sub-processors, WatchGuard will enter into agreements with the sub-processors to bind them to data processing obligations to the extent required by law or by this Agreement, whichever is more restrictive.

2.03.5 Data Retention and Deletion. Except for anonymized County Data, as described above, or as otherwise provided under the Agreement, WatchGuard will delete all County Data following termination or expiration of this Agreement or the applicable Addendum or Ordering Document, with such deletion to occur within a mutually agreed upon timeframe following the applicable date of termination or expiration, unless otherwise required to comply with applicable law. Any requests for the exportation or download of County Data must be made by County to WatchGuard in writing before expiration or termination, subject to **Section 9.15 – Notices**. WatchGuard will work with the County to transfer any County Data prior to expiration or termination of the mutually agreed upon timeframe. No County Data shall be deleted without the written authorization of the County.

2.03.6 Anonymized Service Use Data. County understands and agrees that WatchGuard may collect and use anonymized Service Use Data for its own purposes, including the uses described below. WatchGuard may use anonymized Service Use Data to (a) operate, maintain, manage, and improve existing and create new products and services, (b) test products and services, and (c) to aggregate Service Use Data and combine it with that of other users.

2.03.7 Third-Party Data and WatchGuard Data. WatchGuard Data and Third-Party Data may be available to County through the Products and Services. County and its Authorized Users may use WatchGuard Data and Third-Party Data as permitted by WatchGuard and the applicable Third-Party Data provider, as described in the Agreement. Unless expressly permitted in the Agreement, County will not, and will ensure its Authorized Users will not: (a) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (b) use such data in violation of applicable laws; or (c) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data. Any rights granted to County or Authorized Users with respect to WatchGuard Data or Third-Party Data will terminate within a mutually agreed upon timeframe following the applicable date of termination or expiration of the Agreement. Further, WatchGuard shall notify the County in writing in the event that WatchGuard or the applicable Third-Party Data provider believes County's or the Authorized User's use of the data violates the Agreement, applicable law or WatchGuard's agreement with the applicable Third-Party Data provider and such parties may suspend, change, or terminate County's or any Authorized User's access to WatchGuard Data or Third-Party Data if County fails to provide a plan to cure any alleged violation within fifteen business (15) days from County's receipt of notice from WatchGuard. Upon termination of County's rights to use any WatchGuard Data or Third-Party Data, County and all Authorized Users will discontinue use of such data and delete all copies of such data and confirm such deletion in writing to WatchGuard. Notwithstanding any provision of the Agreement to the contrary, WatchGuard will have no liability for Third-Party Data or WatchGuard Data available through the Products and Services, except to the extent of any indemnification provision in this Agreement. WatchGuard and its Third-Party Data providers reserve all rights in and to WatchGuard Data and Third-Party Data not expressly granted herein.

2.03.8 Feedback. Any systematic enhancement made by WatchGuard based on Feedback provided by County will not create any confidentiality obligation for WatchGuard, even if designated as confidential by County. WatchGuard may use County Feedback to develop, design, and create systematic enhancements to WatchGuard Products and Services; however, WatchGuard may not use any County Feedback for the purposes of promotion of WatchGuard Products and Services, unless otherwise agreed to by the parties in writing.

2.03.9 Improvements; Products and Services. The Parties agree that, notwithstanding any provision of this Agreement to the contrary, all fixes, modifications and improvements to the Services or Products conceived of or made by or on behalf of WatchGuard that are based either in whole or in part on the Feedback, anonymized County Data or anonymized Service Use Data are the exclusive property of WatchGuard and all right, title and interest in and to such fixes, modifications or improvements will vest solely in WatchGuard.

2.03.10 WatchGuard as a Controller. In all instances where WatchGuard acts as a controller of data, it will comply with the applicable provisions of the WatchGuard Privacy Statement at https://www.motorolasolutions.com/en_us/about/privacy-policy.html#privacystatement, as may be updated from time to time. WatchGuard holds all County Contact Data as a controller and shall process such County Contact Data in accordance with the WatchGuard Privacy Statement and the terms of this Agreement.

Section 2.04 Reserved

Section 2.05 Restrictions

The County will not, and will not allow others including the Authorized Users, to:

(a) make the WatchGuard Software or Documentation resulting from the SaaS Services available in any manner to any third party, not including the County's Judicial Partners, for use in the third party's business operations;

(b) modify, make derivative works of, disassemble, reverse compile, reverse engineer or reprogram software used to provide the Subscription Software or any portion thereof to a human readable form; merge the Subscription Software with other software, copy, reproduce, distribute, lend, or lease the Subscription Software or Documentation for or to any third party;

(c) take any action that would cause the Subscription Software, software used to provide the Subscription Software, or Documentation to be placed in the public domain, except for the release of any Subscription Software, software used to provide the Subscription Software, or Documentation which may be required pursuant to Ohio Public Records laws;

(d) remove, alter, or obscure, any copyright or other notice; share user credentials with individuals who are not Authorized Users use the Subscription Software to store or transmit malicious code; or attempt to gain unauthorized access to the Subscription Software or its related systems or networks;

(e) access or use the SaaS Services in order to build or support, and/or assist a third party in building or supporting, products or services competitive to WatchGuard; or

(f) license, sell, rent, lease, transfer, assign, distribute, display, host, outsource, disclose, permit timesharing or service bureau use, or otherwise commercially exploit or make the SaaS Services, WatchGuard Software, or Documentation available to any third party other than as expressly permitted by this Agreement.

Nothing in this Section shall be deemed to prohibit the County from integrating Third Party Software or solutions through any WatchGuard-created APIs or third-party APIs.

Section 2.06 Compliance

WatchGuard's SaaS Services are audited at least yearly in accordance with the AICPA's Statement on Standards for Attestation Engagements ("SSAE") No. 18and SOC 2 Type 2. WatchGuard has attained, and will maintain, Type II SSAE compliance, or its equivalent. Additionally, services provided by us shall comply with the requirements of the Criminal Justice Information Services ("CJIS") Security Policy (current version 5.7, dated August 16, 2018), as it may be amended. WatchGuard incorporates by reference the terms of the CJIS Security Addendum located at: https://www.fbi.gov/file-repository/cjis-security-policy_v5-7_20180816.pdf/view. Upon execution of a mutually agreeable Non-Disclosure Agreement ("NDA"), WatchGuard will provide County with our AICPA SOC 2 Type 2 compliance report or its equivalent. Every year thereafter, for so long as the NDA is in effect and in which County makes a written request, WatchGuard will provide that same information.

Section 2.07 Architecture

The Solution Host will have fully redundant telecommunications access, electrical power, and the required hardware to provide access to the WatchGuard Software. County will be hosted on shared hardware by the designated Solution Host but in a database dedicated to the County, which is inaccessible to WatchGuard's other customers. WatchGuard shall provide secure data transmission paths from each of County workstations to WatchGuard servers.

Section 2.08 Backup

Throughout the term of the Agreement, WatchGuard will perform full nightly backups and transaction log backups of the County's Data.

Section 2.09 Disaster Recovery Plan

In the event of a declared Disaster, WatchGuard is responsible for restoring any lost or corrupted Data as set forth in this subsection. In no case shall the RPO exceed a maximum of four hours from declaration of Disaster. For purposes of this subsection, RPO represents the maximum tolerable period during which County Data may be lost, measured in relation to a Disaster WatchGuard declares, said declaration will not be unreasonably withheld. In the event WatchGuard declares a Disaster, WatchGuard's RTO is six hours. For purposes of this subsection, RTO represents the amount of time, after WatchGuard declares a Disaster, within which County access to the WatchGuard Software must be restored.

WatchGuard will schedule and test the disaster recovery plan at least once per year and will provide any certifications or information related to the annual disaster recovery testing to the County upon completion.

Section 2.10 Security

(a) Employees

All WatchGuard employees have undergone criminal background checks. All WatchGuard employees sign a confidentiality agreement when hired and agree to follow WatchGuard security policies. Background checks will be completed for all WatchGuard employees providing onsite services or who will have access to the County's Data.

(b) Security Testing and Compliance

WatchGuard conducts annual vulnerability testing of both the production network and web application. This vulnerability test will include testing on both the production and nonproduction environments. WatchGuard will maintain industry standard intrusion detection and prevention systems to monitor malicious activity in the network and to log and block any such activity.

WatchGuard will provide County with a written or electronic record of the actions taken by us in the event that any unauthorized access to County database(s) is detected as a result of WatchGuard security protocols. WatchGuard will undertake an additional security audit, on terms and timing to be mutually agreed to by the parties, at County written request.

You may not attempt to bypass or subvert security restrictions in the SaaS Services or environments related to the WatchGuard Software. Unauthorized attempts to access files, passwords or other confidential information, and unauthorized vulnerability and penetration test scanning of WatchGuard network and systems (hosted or otherwise) is prohibited without the prior written approval of WatchGuard IT Security Officer.

(c) Security Breach Response Plan

WatchGuard shall notify the County within 72 hours of any Security Breach of which WatchGuard becomes aware. WatchGuard will collaborate with the County throughout the incident and will provide updates on remediation every 24 hours until the incident is resolved. Upon incident remediation, WatchGuard will provide the County with a full incident report which includes incident timeline from awareness to remediation, method and timing of entry, at risk Data, any Data manipulation or exfiltration that occurred, and remediation actions taken.

WatchGuard will provide to the County security policies and protocols for the Solution Host, including any updates to such policies and protocols, as such policies and protocols are publicly available.

Section 2.11 Cyber Breach

WatchGuard shall have a plan and adequate resources to address telecommunications and computer systems breach, and shall maintain intrusion detection services and procedures and/or data breaching systems to detect and address "hacking" and "phishing operations" into the WatchGuard's telecommunications system, that includes services and systems to detect any unauthorized access to or unauthorized activity on WatchGuard's telecommunications system, networks, computer systems, and network devices associated with the use of and access to the County's management systems, databases, and County information and data. WatchGuard will ensure that all intrusion detection measures and data breach systems are maintained and functional on a regular basis. Intrusion detection services and data breach systems shall include, at minimum, network-based intrusion detection and active monitoring of appropriate computer system access logs. WatchGuard shall notify the County, as soon as reasonably possible, of its detection of any potential or suspected intrusions that may affect the County with regard to disbursement of payments or access to County systems, networks, data, or information. Failure by WatchGuard to provide this notification shall be a breach under the contract. WatchGuard shall be liable for all costs and damages to the County related to or arising from the breach of WatchGuard's telecommunications systems, networks, or computer systems, or failure to follow the requirements of this Section 2.11.

Section 2.12 SaaS License Grant and Restrictions

(a) WatchGuard grants to the County and its Authorized Users a limited, non-transferrable, non-sublicenseable and nonexclusive license to use the Subscription Software and associated Documentation solely for the County's internal business purposes. The County may permit access to the SaaS Services to Authorized Users solely to meet the County's internal business purposes; provided, however, the County ensures that all Authorized Users comply with the terms of this Agreement. The foregoing license grant will be limited to the number of licenses set forth in Exhibit 1 (if applicable), and will continue for the Term of this Agreement. County may access, and use the Subscription Software only in County's owned or County authorized remote sites; provided, however, that Authorized Users using authorized mobile or handheld devices may log into and access the Subscription Software remotely from any location. WatchGuard's Solution will be made available to the County and its Authorized Users in accordance with the terms of the SLA.

(b) End User Licenses. Notwithstanding any provision to the contrary in the Agreement, certain Subscription Software is governed by a separate license, EULA, or other agreement, including terms governing third-party software, such as open source software, included in the Subscription Software. WatchGuard shall provide County with a copy of all additional third-party terms and conditions no later than thirty days from their effective date and all such terms and conditions shall be included in Exhibit C.

(c) The Documentation is licensed to the County and may be used and copied by County and its Authorized Users and Judicial Partners for internal, noncommercial reference purposes only. County and Authorized Users will comply with the applicable Documentation and the copyright laws of the United States (including the copyright laws where County uses the Subscription Software) in connection with their use of the Subscription Software.

(d) County-Provided Equipment. Certain components, including equipment and software, not provided by WatchGuard may be required for use of the Products and Services ("County-Provided Equipment"). County will be responsible, at its sole cost and expense, for providing and maintaining the County-Provided Equipment in good working order. County represents and warrants that it has all rights in County-Provided Equipment to permit WatchGuard to access and use the applicable County-Provided Equipment to the extent necessary to provide the Products and Services under this Agreement, and such access and use will not violate any laws or infringe any third-party rights (including intellectual property rights). County (and not WatchGuard) will be fully liable for County-Provided Equipment, and County will promptly notify WatchGuard of any County-Provided Equipment damage, loss, change, or theft that will substantially impact WatchGuard's ability to provide the Products and Services under this Agreement, and County acknowledges that any such events may cause a change in the Fees or performance schedule under the applicable Ordering Document. Any modification in fees will require the execution of a written modification by the parties.

Section 3 Maintenance and Support

Section 3.01 Maintenance and Support Terms

For so long as the County timely pays their SaaS Fees according to Section 6 Invoicing and Payment, then in addition to the terms set forth in the SLA and the Support Call Process, WatchGuard will:

(a) perform its maintenance and support obligations in a professional, good, and workmanlike manner, at a minimum consistent with industry standards, to reasonably resolve Defects in the WatchGuard Software consistent with the terms of this Agreement, SLA, and the Support Call Process;

(b) perform telephone support during WatchGuard established support hours;

(c) correct or otherwise cure documented Defects to the then-current WatchGuard Software made available to the County;

(d) maintain personnel that are sufficiently trained to be familiar with the WatchGuard Software, Third Party Software (if any), and WatchGuard-developed Integrations in order to provide maintenance and support services; and

(e) provide all other support services in accord with the terms of this Agreement.

Section 3.02 Remote and Onsite Support

WatchGuard will use all reasonable efforts to perform support services as outlined in this Agreement. The County agrees to provide WatchGuard with a login account and local administrative privileges as WatchGuard may reasonably require to perform remote services. WatchGuard will, at WatchGuard's option, use the secure connection to assist with proper diagnosis and resolution, subject to any reasonably applicable security protocols. If WatchGuard cannot resolve a support issue remotely, WatchGuard may be required to provide onsite services. In such event, WatchGuard will be responsible for WatchGuard's travel expenses, unless it is determined that the reason onsite support was required was a reason outside WatchGuard's control. Any such travel shall be in accordance with the Franklin County Board of Commissioners' Travel Policy. Either way, the County agrees to provide WatchGuard with full and free access to the WatchGuard Software, working space, adequate facilities within a reasonable distance from the equipment, and use of machines, attachments, features, or other equipment reasonably necessary for WatchGuard to provide the maintenance and support services, all at no charge to WatchGuard.

Section 3.03 Restrictions

(a) For the avoidance of doubt, maintenance and support services do not include the following: (1) onsite support (unless WatchGuard cannot remotely correct a Defect in the WatchGuard Software, as set forth above); (2) application design; (3) other consulting services; (4) support outside WatchGuard normal business hours as listed in WatchGuard's then-current Support Call Process; or (5) support of the County operating systems or hardware.

(b) Requested services such as those outlined in this Section will be billed: (1) during the 12-month period after Final Acceptance, at the rates set forth in the Investment Summary; or (2) following the 12-month period after Final Acceptance, on a time and materials basis, at WatchGuard then-current rates. The County must provide one-week notice for these services.

Section 3.04 Legislative Change Support

(a) WatchGuard will provide the County with Enhancements or other modifications to the WatchGuard Software as necessary to comply with enacted statewide legislation or statewide administrative regulation.

(b) WatchGuard will use commercially reasonable efforts to implement such changes within the time frames set in the applicable legislation, regulation, or rule, or any extension granted thereto.

(c) Prior to performing any services under this Section that would result in fees to the County, WatchGuard will provide the County with a change order or addendum.

(d) WatchGuard's legislative change support obligations do not apply to services required to support new duties or responsibilities that expand upon the scope of the County's internal business purposes disclosed to us as of the Effective Date.

Section 3.05 Product Enhancements and Updates

Information surrounding Product releases, cancellation and other technical information relating to the WatchGuard Software is available to the County via Product Newsletters at the following website: https://www.motorolasolutions.com/en_us/support/technical-product-newsletter.html. To remain informed on the recent news, the County is able to complete and submit the form as indicated on the website.

If WatchGuard and the County mutually determine that training for any enhancements or updates to the WatchGuard Software is necessary, WatchGuard shall provide such training to all users at no additional cost to the County.

Section 4 Other Professional Services

Section 4.01 Reserved

Section 4.02 Other Services

After Final Acceptance of the WatchGuard Solution, the County may request consulting, design, analysis, project management, programming, or other services, all related to additional Integrations, Configurations, Solution Hosting, or training for the WatchGuard Software. Fees for these services shall be at the current rate established by WatchGuard, any such services shall require execution of a written Amendment to this Agreement signed by the parties.

Section 4.03 Fees for Additional Products and Services

County may purchase additional WatchGuard products and services, including training at WatchGuard's then-current list price. The terms of this Agreement will control any such additional purchase(s), unless otherwise mutually agreed to by the parties, any such additional purchases shall require execution of a written modification of the parties.

Section 4.04 Site Access and Requirements

At no cost to WatchGuard, the County agrees to provide WatchGuard with full and free access to County personnel, facilities, and equipment as may be reasonably necessary for WatchGuard to provide implementation services, subject to any reasonable security protocols or other written policies provided to WatchGuard as of the Effective Date, and thereafter subject to mutual agreement. The County agrees that it is the County's responsibility to ensure that the County satisfies the then-current system requirements minimally required to run the WatchGuard Software.

Section 4.05 Video as a Service Program Terms. All hardware provided by WatchGuard to County under the VaaS Program will be considered Equipment. Additionally, the following terms and conditions apply to any Equipment provided under the VaaS Program:

4.05.1 Technology Refresh. All body cameras and associated batteries provided under the VaaS Program ("**Body Cameras**") are eligible for a one-time replacement at no additional cost to the County beginning on the date three (3) years following the date of delivery of the initial Body Cameras and associated batteries provided under the VaaS Program during the Initial Term. In the event the parties enter into a Renewal Term, County shall receive a technology refresh at the start of the Renewal Term, and shall be eligible for an additional technology refresh beginning on the date three (3) years following the date of delivery of the Body Cameras and associated batteries provided under the VaaS Program during the Renewal Term. In order to receive any replacement Body Camera applicable under this Section 4.05.1, County must return the existing Body Camera to WatchGuard in working condition, reasonable wear and tear excepted. The corresponding replacement Body Camera will be the then-current model of the Body Camera at the same tier as the Body Camera that is returned to WatchGuard. For clarity, any other Equipment received by County as part of the VaaS Program, other than Body Cameras, will not be eligible for a technology refresh hereunder.

4.05.2 No-Fault Warranty. Subject to the disclaimers set forth in the Agreement, upon delivery of any Equipment provided as part of the VaaS Program, WatchGuard will provide a No-fault Warranty to County for such Equipment; except that the No-fault Warranty will not apply to: (i) any Equipment with intentionally altered or removed serial numbers, or (ii) any Equipment that WatchGuard determination was changed, modified, or repaired by County or any third party. The "**No-fault Warranty**" means that WatchGuard will repair or replace any Equipment components or parts that render the applicable Equipment unable to perform its intended purpose. With respect to any batteries in Body Cameras, a battery will be considered faulty and covered under this No-fault Warranty if it falls below sixty percent (60%) of rated capacity.

4.05.3 Reserved.

4.05.4 Additional Devices. Any additional Equipment, including any accessory items, ordered by County after County's initial receipt of Equipment hereunder may be subject to an incremental increase in Fees at a price agreeable to the parties and upon the execution of a written modification to the Agreement, signed by the parties and approved via resolution by the Franklin County Board of Commissioners. In the event County orders additional Equipment under the VaaS Program, such Equipment will be included in and subject to the terms of the Agreement at the prices established herein, pro-rated for the remainder of the term of this Agreement, except that any additional devices purchased with less than eighteen (18) months remaining under the Agreement shall be subject to pricing as agreed to by the parties. Any additional devices purchased by the County shall not be eligible for a technology refresh until three (3) years after delivery of the additional devices.

4.05.5 Included Subscription Software.

(a) EvidenceLibrary.com. Subject to the Vaas Term and Termination provisions below, the VaaS Program provides the County with a subscription to the Cloud Hosted Evidence Management System, subject to the terms and condition of the Agreement. The County's subscription will include unlimited users, Unlimited Storage and unlimited sharing, as outlined in Exhibit 1. Following expiration of the Initial Term, if County desires to continue use of expired Equipment with the Cloud Hosted Evidence Management System, County must purchase additional access to Cloud Hosted Evidence Management System based on WatchGuard's prevailing rates, or WatchGuard may disconnect connectivity of any expired Equipment to the Cloud Hosted Evidence Management System.

(b) CommandCentral. For each Body Camera, in-car system or integrated system purchased, County will receive one user license for WatchGuard CommandCentral, which provides access to CC Community, CC Capture, CC Vault and CC Records. If the County requires additional licenses to CommandCentral they must be purchased for an additional fee which shall be subject to the execution of a written modification of the Agreement.

4.05.6 Reserved.

4.05.7 Reserved.

4.05.8 Reserved.

4.05.9 Additional Cloud Terms. The terms set forth in this Section 4.05.9 **– Additional Cloud Terms** apply in the event County purchases any cloud hosted software Products under this Agreement, including a Cloud Hosted Evidence Management System.

(a) Data Storage. WatchGuard will determine, in its sole discretion, the location of the stored content for cloud hosted software Products. All data, replications, and backups will be stored at a location in the United States within Microsoft Azure's GovCloud to ensure CJIS compliance.

(b) Data Retrieval. Cloud hosted software Products will leverage different types of storage to optimize software, as determined in WatchGuard's sole discretion. For multimedia data, such as videos, pictures, audio files, WatchGuard will, in its sole discretion, determine the type of storage medium used to store the content. The type of storage and medium selected by WatchGuard will determine the data retrieval speed. Access to content in archival storage may take up to twenty-four (24) hours to be viewable.

(c) Availability. Availability shall be governed by the terms of the Service Level Agreement attached hereto as Exhibit A.

(d) Maintenance. Maintenance shall be governed by the terms of the Service Level Agreement attached hereto as Exhibit A.

Section 5 Third Party Software and Non-WatchGuard Content

To the extent there are any Third Party Software identified in the Investment Summary, the Third Party Terms will apply.

The County acknowledges that WatchGuard may have embedded third party functionality in the WatchGuard Software that is not separately identified in the Investment Summary. If that third party functionality is not separately identified in the Investment Summary, the limited warranty applicable to the WatchGuard Software applies.

Non-WatchGuard Content. In certain instances, County may be permitted to access, use, or integrate County or third-party software, services, content, and data that is not provided by WatchGuard (collectively, "**Non-WatchGuard Content**") with or through the Products and Services. If County accesses, uses, or integrates any Non-WatchGuard Content with the Products or Services, County will first obtain all necessary rights and licenses to permit County's and its Authorized Users' use of the Non-WatchGuard Content in connection with the Products and Services. County will also obtain the necessary rights for WatchGuard to use such Non-WatchGuard Content in connection with providing the Products and Services, including the right for WatchGuard to access, store, and process such Non-WatchGuard Content (e.g., in connection with Subscription Software), and to otherwise enable interoperation with the Products and Services. County represents and warrants that it will obtain the foregoing rights and licenses prior to accessing, using, or integrating the applicable Non-WatchGuard Content with the Products and Services, and that County and its Authorized Users will comply with any terms and conditions applicable to such Non-WatchGuard Content. If any Non-WatchGuard Content requires access to County Data (as defined below), County hereby authorizes WatchGuard to allow the provider of such Non-WatchGuard Content to access County Data, in connection with the interoperation of such Non-WatchGuard Content with the Products and Services. County acknowledges and agrees that WatchGuard is not responsible for, and makes no representations or warranties with respect to, the Non-WatchGuard Content (including any disclosure, modification, or deletion of County Data resulting from use of Non-WatchGuard Content or failure to properly interoperate with the Products and Services). If County receives notice from an authorized WatchGuard representative that any Non-WatchGuard Content must be removed, modified, or disabled within the Products or Services, County will promptly do so in a timeframe mutually agreeable to both parties. Upon failure by the County to remove, modify or disable the Non-WatchGuard Content within the established timeframe after receipt of notice from WatchGuard, WatchGuard will have the right to disable or remove Non-WatchGuard Content if WatchGuard believes a violation of law or third-party rights is likely to occur, or if such Non-WatchGuard Content poses or may pose a security or other risk or adverse impact to the Products or Services, WatchGuard, WatchGuard's systems, or any third party (including other WatchGuard Counties).

Section 6 Invoicing and Payment; Invoice Disputes

Section 6.01 Invoicing and Payment

WatchGuard will invoice the County as set forth below:

(a) SaaS Fees

Year 1 SaaS Fees shall be invoiced and paid as described in Exhibit 1. SaaS Fees for Years 2 through 5 shall be invoiced and paid annually in advance in accordance with Section 6.04 of this Agreement.

Upon expiration of the Initial Term (as defined in Section 7.01 below), the parties will mutually agree upon SaaS Fees for any Renewal Term. The County's annual SaaS Fees will be as set forth in the Investment Summary.

(b) Other WatchGuard Products and Services

Additional WatchGuard products, and other professional services purchased under Section 4.03 shall be invoiced at the rates agreed to by the parties in a separate contract or amendment hereto.

Section 6.02 Reserved

Section 6.03 Invoicing Method

The County agrees to set up an ACH payment account to ensure timely electronic payment to WatchGuard.

WatchGuard will provide the County with electronic payment information within five (5) business days following the Effective Date.

WatchGuard will submit a Proper Invoice itemizing which deliverables are being billed. Failure to provide a Proper Invoice will be cause for rejection of the invoice with a written notice stating the deficiencies. Payment will be delayed until the deficiencies are corrected and a Proper Invoice is submitted. WatchGuard will be required to submit invoices electronically, by mail, sent by courier, or sent as an attachment to an email to the bill to address identified in the purchase orders used to issue orders against this Agreement. WatchGuard's Federal Tax Identification Number should appear on all statements and invoices.

Section 6.04 Payment

WatchGuard shall invoice the County for SaaS Fees under this Agreement annually in advance and payment for undisputed invoices is due within 30 days from the date the invoice is received. The County will not pay late fees, interest, or other penalties for later payment. Any entity authorized to utilize this Agreement, outside the responsibility of the County, is responsible for all orders, invoices, payment, and/or tracking.

License True-Up. WatchGuard will have the right to conduct an audit of total user licenses credentialed by County for any Subscription Software during the term of the Agreement, and County will cooperate with such audit. If WatchGuard determines that County's usage of the Subscription Software during the term of the Agreement exceeded the total number of licenses purchased by County, WatchGuard may invoice County for the additional licenses used by County, pro-rated for each additional license from the date such license was activated, and County will pay such invoice in accordance with this Agreement. Notwithstanding the foregoing, any change in pricing shall be subject to the execution of a written modification of the Agreement.

Section 6.05 Invoice Disputes

If the County disputes the performance or delivery of any software, service, or product under this Agreement, the County will provide WatchGuard with written notice within 30 days of the County's receipt of a Proper Invoice. The written notice must contain reasonable detail of the disputed issues so that WatchGuard can confirm the issues and respond to the County's notice with either a justification of the invoice, an adjustment to the invoice, or a proposal addressing the issues presented in the County's notice. Should WatchGuard's justification, adjustment, or proposal addressing the issue be insufficient to resolve the dispute, WatchGuard will work with the County to develop an action plan that outlines reasonable steps to be taken by each of the parties to resolve any issues presented in the County's notice.

The County may withhold payment of the amount(s) actually in dispute, and only those amounts, until WatchGuard completes the action items outlined in the plan. If WatchGuard is unable to complete the action items outlined in the action plan because of the County's failure to complete the items agreed to be done by the County, and the County does not rectify that failure within a commercially reasonable timeframe after WatchGuard has notified the County of it, then WatchGuard may demand immediate full payment of the invoice.

Section 6.06 Failure to Pay

If the County fails to timely pay undisputed invoices, WatchGuard shall provide written notice of such alleged failure. The County shall cure any late payments within 30 days of receiving said written notice.

Section 6.07 Taxes

The fees in the Investment Summary do not include any taxes, including, without limitation, sales, use, or excise tax. The County is tax exempt and will provide a tax-exempt certificate to WatchGuard upon WatchGuard's request. WatchGuard is responsible for reporting and paying its income taxes, both federal and state, as applicable, arising from WatchGuard's performance of this Agreement.

Section 7 Term and Termination

Section 7.01 Term

The Initial Term of this Agreement is five years from the first day following Go-Live acceptance of the first phase (the "Initial Term"), unless earlier terminated as set forth below. Upon the expiration of the Initial Term of this Agreement, this Agreement may be renewed for one additional five-year term, such term to constitute a "Renewal Term".

Section 7.02 Termination

This Agreement may be terminated as set forth below. In the event of termination, the County will pay WatchGuard for all undisputed fees and expenses related to the software, products, and/or services the County has received, or WatchGuard has incurred or delivered, prior to the effective date of termination. Disputed fees and expenses in all terminations must have been submitted as invoice disputes in accordance with Section 6.05 of this Agreement.

(a) Failure to Pay SaaS Fees

WatchGuard shall provide written notice of its intent to terminate this Agreement for failure to pay undisputed SaaS Fees following the County's receipt of a "Failure to Pay" notice pursuant to Section 6.06 of this Agreement. If the County fails to cure the nonpayment within 45 days of receiving WatchGuard's notice of its intent to terminate, WatchGuard may terminate this Agreement.

(b) For Cause

The County may terminate this Agreement for cause, which shall include, but not be limited to, the following material breaches: (1) WatchGuard no longer offers SaaS Services for the WatchGuard Solution; (2) WatchGuard fails to maintain compliance and certifications as set forth in Section 2.06 of this Agreement (or their equivalent); (3) WatchGuard is subject to voluntary or involuntary bankruptcy; (4) WatchGuard merges or consolidates substantially all of its assets to an assignee who fails to maintain or offer the SaaS Services for the WatchGuard Solution; (5) the County terminates the Services Agreement for a material breach.

Prior to any Notice of Default being issued, the County will provide WatchGuard with written notice of a perceived failure ("Perceived Failure Notice"). WatchGuard may, within seven business days following the Perceived Failure Notice, propose a written action plan acceptable to the County to remedy the perceived failures, infractions, or defaults ("Perceived Failure Plan"), or request a meeting by the parties to discuss the perceived failures, infraction, or defaults ("Perceived Failure Notice Meeting"). The Perceived Failure Notice Meeting shall occur not later than 45 days following the issuance of the Perceived Failure Notice. Following the Perceived Failure Notice Meeting, WatchGuard shall have 15 days to provide a Perceived Failure Plan. Should WatchGuard fail to provide a Perceived Failure Plan within the required timeframe or should Franklin County reasonably determine the Perceived Failure Plan is not acceptable, then Franklin County shall have the right to issue a Notice of Default, in whole or in part, and may within ten business days following issuance of the Notice of Default terminate this Agreement, in whole or in part, for default.

(c) Lack of Appropriations

This Agreement is contingent upon the County budgeting and appropriating the funds on an annual basis necessary for the continuation of this Agreement in any contract year. In the event that the funds necessary for the continuation of this Agreement are not approved for expenditure in any year, this Agreement shall terminate on the last day of the fiscal year in which funding was approved, without penalty to the County. The County will provide WatchGuard with written notification within 30 days after being notified that the funding of the Agreement is no longer approved. The County will pay WatchGuard for all products and services delivered through the date of termination and will not be entitled to a refund or offset of previously paid, but unused SaaS Fees.

(d) Termination. Notwithstanding the termination provisions of the Agreement, WatchGuard may terminate this Agreement, or suspend delivery of Subscription Software or Services, upon written notice to County, which remains uncured for a period of 30 days, or such other timeframe as mutually agreed to by the parties, following County's receipt of notice, if (a) County breaches Section 2.12 of this Agreement, or any other provision related to Subscription Software license, or (b) it determines that County's use of the Subscription Software poses, or may pose, a security or other risk or adverse impact to any Subscription Software, WatchGuard, WatchGuard's systems, or any third party (including other WatchGuard customers).

Section 8 Indemnification, Limitation of Liability, and Insurance

Section 8.01 Intellectual Property Infringement Indemnification

WatchGuard will defend County against any third-party claim alleging that a WatchGuard-developed or manufactured Product or Service (the "**Infringing Product**") infringes a United States patent, copyright, or trade secret of any third party ("**Infringement Claim**"), and WatchGuard will pay all damages finally awarded against County by a court of competent jurisdiction for an Infringement Claim, or agreed to in writing by WatchGuard in settlement of an Infringement Claim. WatchGuard's duties under this **Section 8.01 – Intellectual Property Infringement** are conditioned upon: (a) County promptly notifying WatchGuard in writing of the Infringement Claim; (b) WatchGuard having sole control of the defense of the suit and all negotiations for its settlement or compromise; and (c) County cooperating with WatchGuard and, if requested by WatchGuard, providing reasonable assistance in the defense of the Infringement Claim at WatchGuard's expense.

8.01.1 If an Infringement Claim occurs, or in WatchGuard's opinion is likely to occur, WatchGuard may at its option and expense: (a) procure for County the right to continue using the Infringing Product; (b) replace or modify the Infringing Product so that it becomes non-infringing; or (c) grant County (i) a pro-rated refund of any amounts pre-paid for the Infringing Product (if the Infringing Product is a software Product, i.e., Licensed Software or Subscription Software) or (ii) a credit for the Infringing Product, less a reasonable charge for depreciation (if the Infringing Product is Equipment, including Equipment with embedded software).

8.01.2 In addition to the other damages disclaimed under this Contract, WatchGuard will have no duty to defend or indemnify County for any Infringement Claim that arises from or is based upon: (a) County Data, County-Provided Equipment, Non-WatchGuard Content, or third-party equipment, hardware, software, data, or other third-party materials; (b) the combination of the Product or Service with any products or materials not provided by WatchGuard; (c) a Product or Service designed, modified, or manufactured in accordance with County's designs, specifications, guidelines or instructions and not otherwise approved by WatchGuard; (d) a modification of the Product or Service by a party other than WatchGuard; (e) use of the Product or Service in a manner for which the Product or Service was not designed or that is inconsistent with the terms of this Contract; or (f) the failure by County to use or install an update to the Product or Service that is intended to correct the claimed infringement, except to the extent that WatchGuard is responsible for making or publishing such update to the Product or Service. In no event will WatchGuard's liability resulting from an Infringement Claim extend in any way to any payments due on a royalty basis, other than a reasonable royalty based upon revenue derived by WatchGuard from County from sales or license of the Infringing Product.

8.01.3 This **Section 8.01 – Intellectual Property Infringement** provides County's sole and exclusive remedies and WatchGuard's entire liability in the event of an Infringement Claim. For clarity, the rights and remedies provided in this Section are subject to, and limited by, the restrictions set forth in **Section 8.03 – Limitation of Liability** below.

Section 8.02 General Indemnification

WatchGuard will defend, indemnify, and hold harmless the County's and the County's agents, officials, and employees from and against any and all third party claims, losses, liabilities, damages, costs, and expenses (including reasonable attorney's fees and costs) for (1) personal injury, death or direct damage to tangible property to the extent caused by WatchGuard's negligence, gross negligence or willful misconduct, or (2) WatchGuard's violation of a law applicable to WatchGuard's performance under this SaaS Agreement. The County must notify WatchGuard promptly in writing of the claim and give WatchGuard sole control over the defense of the suit and all negotiations for its settlement or compromise. The County agrees to provide WatchGuard with reasonable assistance, cooperation, and information in defending the claim at WatchGuard's expense.

Section 8.03 LIABILITY AND DISCLAIMER OF DAMAGES

(a) <u>LIMITATION OF LIABILITY</u>. EXCEPT FOR PERSONAL INJURY OR DEATH, THE TOTAL AGGREGATE LIABILITY OF WATCHGUARD FOR ANY SUBSCRIPTION SOFTWARE OR FOR ANY RECURRING SERVICES, WILL NOT EXCEED AN AMOUNT EQUAL TO TWO TIMES THE ANNUAL SAAS FEES. THE PRICES SET FORTH IN THIS AGREEMENT ARE SET IN RELIANCE UPON THIS LIMITATION OF LIABILITY.

(b) <u>EXCLUSION OF CERTAIN DAMAGES</u>. EXCEPT FOR PERSONAL INJURY OR DEATH, IN NO EVENT SHALL WATCHGUARD BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, OR DAMAGES FOR LOST PROFITS OR REVENUES, EVEN IF WATCHGUARD HAS BEEN ADVISED BY THE COUNTY OF THE POSSIBILITY OF

SUCH DAMAGES OR LOSSES.

(c) ADDITIONAL EXCLUSIONS. WATCHGUARD WILL HAVE NO LIABILITY FOR DAMAGES ARISING OUT OF (A) COUNTY DATA, INCLUDING ITS TRANSMISSION TO WATCHGUARD; (B) COUNTY-PROVIDED EQUIPMENT, NON-WATCHGUARD CONTENT, THE SITES, OR THIRD-PARTY EQUIPMENT, HARDWARE, SOFTWARE, DATA, OR OTHER THIRD-PARTY MATERIALS, OR THE COMBINATION OF PRODUCTS AND SERVICES WITH ANY OF THE FOREGOING; (C) MODIFICATION OF PRODUCTS OR SERVICES BY ANY PERSON OTHER THAN WATCHGUARD OR OTHERWISE APPROVED BY WATCHGUARD; OR (D) COUNTY'S OR ANY AUTHORIZED USERS' BREACH OF THIS AGREEMENT OR MISUSE OF THE PRODUCTS AND SERVICES.

Section 8.04 Insurance

(a) During the course of performing services under this Contract, WatchGuard agrees to maintain the following levels of insurance:

(i) Commercial General Liability of $5,000,000 per occurrence with $5,000,000 general aggregate;

(ii) Automobile Liability of $1,000,000 combined single limit;

(iii) Professional Liability including Cyber Insurance of $5,000,000 per claim and aggregate. Throughout the contract period, WatchGuard must maintain cyber breach insurance that shall include; third party liability coverage for loss or disclosure of data, including electronic data, network security failure, unauthorized access and/or use or other intrusions, infringement of any intellectual property rights (except patent infringement and trade secret misappropriation) unintentional breach of contract, negligence or breach of duty to use reasonable care, breach of any duty of confidentiality, invasion of privacy, or violation of any other legal protections for personal information, defamation, libel, slander, commercial disparagement, negligent transmission of computer virus, ransomware, worm, logic bomb, or Trojan horse or negligence in connection with denial of service attacks, or negligent misrepresentation. WatchGuard will notify the County immediately if WatchGuard's insurance coverage is reduced or terminated;

(iv) Workers' Compensation complying with applicable statutory requirements; and

(b) WatchGuard shall provide the County with a certificate of insurance identifying the County as a certificate holder within a commercially reasonable timeframe after the Effective Date. Additionally, WatchGuard shall include the County as an additional insured to its Commercial General Liability and Automobile Liability policies. That additional insured status will be reflected on the certificate of insurance WatchGuard provides the County after the Effective Date. WatchGuard agrees that the insurance will be primary on claims for which WatchGuard is responsible. Copies of WatchGuard's insurance policies are only available in the event of a disputed or litigated claim during discovery period.

(c) Watchguard's required insurance shall (i) apply as primary and non-contributory to any insurance or program of self-insurance that may be maintained by the County and (ii) contain waivers of subrogation on all coverage except Professional Liability/Cyber Liability insurance.

(d) During the term of this Contract and any renewal thereto, WatchGuard, and any agent of WatchGuard, at its sole cost and expense, shall maintain the required insurance coverage as described in the Contract. County may require WatchGuard to provide respective certificate(s) of insurance in order to verify coverage. Failure to provide a requested certificate within a seven (7) calendar day period may be considered as default.

Section 9 General Terms and Conditions

Section 9.01 Representations and Warranties

(a) Mutual Representations and Warranties. Each party represents and warrants to the other party that (a) it has the right to enter into the Agreement and perform its obligations hereunder, and (b) the Agreement will be binding on such party.

(b) Limited Software Warranty

WatchGuard warrants that the WatchGuard Software will perform without Defects during the term of this Agreement. If the WatchGuard Software does not perform as warranted, WatchGuard will use all reasonable efforts, consistent with industry standards, to cure any Defect in accordance with the maintenance and support process set forth in Section 3 of this Agreement, the SLA and WatchGuard's then-current Support Call Process, or to provide the County with a functional equivalent. For the avoidance of doubt, to the extent any Third Party Software is embedded in the WatchGuard Software, the County's limited warranty rights are limited to WatchGuard's Defect resolution obligations set forth above; the County does not have separate rights against the Developer of the embedded Third Party Software.

(c) No-Fault Warranty. WatchGuard provides a no-fault warranty for Equipment as provided in Section 4.05.2 of this Agreement.

(d) Subject to the disclaimers and exclusions below, WatchGuard represents and warrants that (a) Services will be provided in a good and workmanlike manner and will conform in all material respects to the Functional Descriptions in Exhibit 1; and (b) the Services will be free of material defects in materials and workmanship. Other than as set forth in subsection (a) above, recurring Services are not warranted but rather will be subject to the requirements of Section 3 of the SaaS Agreement and the Service Level Agreement attached hereto as Exhibit A. WatchGuard provides other express warranties for WatchGuard-manufactured equipment, WatchGuard-owned software products, and certain Services as provided in the Services Contract. Such express warranties for the VaaS Program are included in Section 4.05.2 of this Agreement.

(e) Warranty Claims; Remedies. To assert a warranty claim, County must notify WatchGuard in writing of the claim. Upon receipt of such claim, WatchGuard will investigate the claim and use commercially reasonable efforts to repair or replace any confirmed materially non-conforming Product or re-perform any non-conforming Service, as agreed to by the parties. Such remedies are County's sole and exclusive remedies for WatchGuard's breach of a warranty. WatchGuard's warranties are extended by WatchGuard to County only, and are not assignable or transferrable.

(f) Pass-Through Warranties. Notwithstanding any provision of this Agreement to the contrary, WatchGuard will have no liability for third-party software or hardware provided by WatchGuard; provided, however, that to the extent offered by third-party providers of software or hardware and to the extent permitted by law, WatchGuard will pass through express warranties provided by such third parties. To the extent that pass-through warranties exist under this Agreement, Watchguard shall assist the County in making any pass-through warranty claim or will make the claim on behalf of the County, as needed.

(g) WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS AND PASS THROUGH WARRANTIES IN THIS AGREEMENT, PRODUCTS AND SERVICES PURCHASED HEREUNDER ARE PROVIDED "AS IS". WARRANTIES SET FORTH IN THE CONTRACT ARE THE COMPLETE WARRANTIES FOR THE PRODUCTS AND SERVICES AND WATCHGUARD DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND QUALITY. WATCHGUARD DOES NOT

REPRESENT OR WARRANT THAT USE OF THE PRODUCTS AND SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR FREE OF SECURITY VULNERABILITIES.

Section 9.02 Reserved

Section 9.03 Dispute Resolution

Each party agrees to provide the other party with written notice within 45 days of becoming aware of a dispute. The parties agree to cooperate with each other in trying to reasonably resolve all disputes, including, if requested by either party, appointing a senior representative to meet and engage in good-faith negotiations with the other party's appointed senior representative. Senior representatives will convene within 45 days of the written dispute notice, unless otherwise agreed.

Section 9.04 Reserved

Section 9.05 Reserved

Section 9.06 Travel

All travel required by WatchGuard under this Contract is included in the costs listed in Exhibit 1. The County will pay for any additional travel that it requests only with prior written approval. The County will pay for all additional travel expenses that it requests in accordance with the Franklin County Board of Commissioner's travel policy attached as Exhibit 5.

Section 9.07 Subcontracting

WatchGuard confirms that it will be the primary contractor who will be performing the work under the Agreement. WatchGuard may use subcontractors for portions of the work under the Agreement, but WatchGuard will remain the primary contractor and will remain liable for all work performed hereunder regardless of whether performed directly by it or by a subcontracted entity. Prior to the Effective Date, WatchGuard provided the County with a list of subcontractors it currently uses.

WatchGuard shall not use any subcontractor who has been subject to action that limits the subcontractor's right to do business with the local, state, or federal government. The County reserves the right to deny use of a subcontractor(s) if the County determines that WatchGuard will not be the primary contractor who will be performing the work under the Agreement.

Section 9.08 Binding Effect; No Assignment

This Agreement shall be binding on, and shall be for the benefit of, either County or WatchGuard successor(s) or permitted assign(s). Neither party will assign any of its rights under this Agreement without the other party's prior written consent. Except WatchGuard may, without the prior written consent of the County, assign the Agreement in its entirety to the surviving entity of any merger or consolidation or to any purchaser of substantially all of WatchGuard's assets. Following any such assignment, the County may enter into a novation agreement with assignee acceptable to the County. The parties hereto understand that the County is legally prohibited from making payment to any entity other than WatchGuard unless the aforementioned novation agreement is executed by the County and assignee. The County may assert against an assignee any claim or defense the County had against WatchGuard under this Agreement.

WatchGuard shall notify the County as soon as possible, but no later than 60 days, after converting into, merging or consolidating with, or selling or transferring substantially all of its assets or business to another corporation, person, or entity.

Section 9.09 Delays due to Force Majeure

Neither party will be liable for delays in performing its obligations under this Agreement to the extent that the delay is caused by Force Majeure; provided, however, that within ten business days of the Force Majeure event, the party whose performance is delayed provides the other party with written notice explaining the cause and extent thereof, as well as a request for a reasonable time extension equal to the estimated duration of the Force Majeure event.

Section 9.10 No Intended Third Party Beneficiaries

This Agreement is entered into solely for the benefit of the County and WatchGuard. No third party will be deemed a beneficiary of this Agreement, and no third party will have the right to make any claim or assert any right under this Agreement. This provision does not affect the rights of third parties under any Third Party Terms.

Section 9.11 Entire Agreement; Amendment; No Waiver

This Agreement and its exhibits and schedules and any documents referred to herein or annexed hereto constitute the complete understanding of the parties regarding the subject matter hereto and supersedes all previous agreements, proposal, and understandings, whether written or oral, relating to this subject matter. This Agreement shall not be changed, modified, terminated, or amended except by a writing signed by a duly authorized officer of each party to this Agreement. Any waiver must be in writing. Any waiver shall constitute a waiver of such right or remedy only and not of any other right or remedy of the waiving party. For purposes of any amendments or waivers, such amendment and waivers shall only be binding against the County if signed by the Franklin County Board of Commissioners. The preprinted terms and conditions found on any County purchase order, acknowledgment, or other form will not be considered an amendment or modification or part of this Agreement, even if a representative of each Party signs such document.

Section 9.12 Severability

If any term or provision of this Agreement is held invalid or unenforceable, the remainder of this Agreement will be considered valid and enforceable to the fullest extent permitted by law.

Section 9.13 Reserved

Section 9.14 Independent Contractor

(a) The parties will be acting as independent contractors. The partners, employees, officers, and agents of one party will act only in the capacity of representatives of that party and not as employees, officers, or agents of the other party and will not be deemed for any purpose to be such. Each party assumes full responsibility for the actions of its employees, officers, and agents, and agents while performing under this Agreement and will be solely responsible for paying its people. Each party will also be solely responsible for withholding and paying income taxes and Social Security, Workers' Compensation, disability benefits, and the like for its people. Neither party will commit, nor be authorized to commit, the other party in any manner.

(b) WatchGuard shall have no claim against the County for vacation pay, sick leave, retirement benefits, Social Security, Workers' Compensation, health or disability benefits, unemployment insurance benefits, or other employee benefits of any kind.

Section 9.15 Notices

(a) All notices or communications required or permitted as a part of this Agreement, such as notice of an alleged material breach for a termination for cause or an invoice dispute, must be in writing and will be deemed delivered if personally delivered, sent by overnight express courier, or sent by United States mail, registered or certified, return receipt requested, postage prepaid, to the address set forth hereunder or to such other address as the other party hereto may designate in written notice transmitted in accordance with this provision. If either overnight express courier or United States mail delivery is not available or delivery is uncertain, then notices may be given by email. Notices shall be sent to the following addresses:

To WatchGuard:

WatchGuard Video, Inc.
Attention: Stuart Johnston
350 Worthington Road, Suite C
Westerville, OH 43082
Phone: (740) 953-0447
Email: Stuart.johnston@motorolasolutions.com

To the County:

Franklin County Sheriff's Office
Attention: David Masterson, Director of Administrative Services
410 S. High Street
Columbus, Ohio 43215
Phone: (614) 525-6746
Fax: (614) 525-3560
Email: dmmaster@franklincountyohio.gov

With a copy to:

Franklin County Purchasing Department
Attention: Purchasing Director
373 S. High Street, 25th Floor
Columbus, OH 43215
Phone: (614) 525-2402
Fax: (614) 525-3144
Email: mabaloni@franklincountyohio.gov

(b) All notices or communications shall be deemed delivered upon the earlier of the following:

(i) Actual receipt by the receiving party;

(ii) Upon receipt by sender of certified mail, return receipt signed by an employee or agent of the receiving party;

(iii) If not actually received, five days after deposit with the United States Postal Service authorized mail center with proper postage (certified mail, return receipt requested) affixed and addressed to the other party at the address set forth on the signature page hereto or such other address as the party may have designated by proper notice.

(c) The consequences for the failure to receive a notice due to improper notification by the intended receiving party of a change in address will be borne by the intended receiving party.

Section 9.16 County Lists

The County agrees that WatchGuard may identify the County by name in County lists, marketing presentations, and promotional materials.

Section 9.17 Confidentiality

Each party acknowledges that performance of this Contract may involve access to confidential information. "Confidential Information" includes any and all non-public information provided by one party ("Discloser") to the other ("Recipient") that is disclosed under the Contract in oral, written, graphic, machine recognizable, or sample form, being clearly designated, labeled or marked as confidential. With respect to the County, Confidential Information will also include but is not limited to personal identifying information, non-public case information, sealed or expunged records, juvenile records, records containing personal health information including information about drug dependency, developmental disability and mental health, adoption records, protective services records, certain records related to domestic abuse, education records, records related to cases involving peace officers, non-public court records and data, and sealed case files, all of which may not be considered to be public records as defined by the Ohio Revised Code, the Ohio Administrative Code, and the Ohio Rules of Superintendence. For purposes of this Contract, Confidential Information shall consist of the County "Confidential Information" and such other information as may be deemed confidential pursuant to Ohio Revised Code Chapter 149, including access to and disclosure of trade secrets, data, rates, procedures, materials, lists, systems and information belonging to the other. All of this information shall be referenced collectively as "Confidential Information." In order to be considered Confidential Information, information that is disclosed orally must be identified as confidential at the time of disclosure and confirmed by Discloser by submitting a written document to Recipient within thirty (30) days after such disclosure. The written document must contain a summary of the Confidential Information disclosed with enough specificity for identification purpose and must be labeled or marked as confidential or its equivalent.

Recipient shall ensure that the Discloser's Confidential Information remains confidential and shall take all reasonable steps to ensure that the Discloser's Confidential Information remain confidential and secure, including as against any WatchGuard employees who do not have a need to view or access the Discloser's Confidential Information. Access to any such Confidential Information shall not change its status as confidential. Except as set forth in the next paragraph, no Confidential Information shall be disclosed to any third party other than representatives of such party who have a need to know such Confidential Information, provided that such representatives are informed of the confidentiality provisions hereof and agree to abide by them. All such Information must be maintained in strict confidence.

Notwithstanding the provisions of the previous paragraph, WatchGuard understands and agrees that any Confidential Information may become subject to a Public Request for Information under Ohio Revised Code Chapter 149. In the event the County receives any such request for any Confidential Information, it will promptly notify WatchGuard in writing of the request to enable WatchGuard to take whatever action it deems appropriate to seek protection from disclosure. If WatchGuard fails to take any action within five business days of such written notice, the County may make such disclosure without any liability to the County.

These obligations of confidentiality will not apply to information that:

(a) Is in the public domain, either at the time of disclosure or afterwards, except by breach of this Contract by a party or its employees or agents;

(b) A party can establish by reasonable proof was in that party's possession at the time of initial disclosure;

(c) A party receives from a third party who has a right to disclose it to the receiving party; or

(d) Is the subject of a legitimate disclosure request under the open records laws or similar applicable public disclosure laws governing this Contract, or a subpoena, for materials applicable to this Contract; provided, however, that in the event the County receives such request above, the County will give WatchGuard prompt notice and otherwise perform the functions required by applicable law.

Recipient will not reverse engineer, de-compile or disassemble any Confidential Information.

Should the County Confidential Information be released in whole or in part to anyone, including a WatchGuard employee that has no need to view or access the records, then WatchGuard shall have the obligation to inform Franklin County within five (5) business days after WatchGuard determines the County Confidential Information has been improperly viewed or accessed. WatchGuard shall, at its sole cost and expense, take all commercially reasonable steps to eliminate any such unauthorized access to the County Confidential Information, and determine which records were accessed and by whom. Failure to secure and securely maintain the County Confidential Information by WatchGuard shall constitute a material breach of this Contract.

County shall promptly notify WatchGuard upon discovery of any unauthorized use or disclosure of the

Confidential Information and take reasonable steps to regain possession of the Confidential Information and prevent further unauthorized actions or other breach of this Agreement.

All Confidential Information is and will remain the property of the Discloser. Upon termination for any reason or expiration of the Contract, Recipient will return or destroy all Confidential Information to Discloser along with all copies and portions thereof or certify in writing that all such Confidential Information has been destroyed. However, Recipient may retain (a) one (1) archival copy of the Confidential Information for use only in case of a dispute concerning this Contract and (b) Confidential Information that has been automatically stored in accordance with Recipient's standard backup or recordkeeping procedures, provided, however that Recipient will remain subject to the obligations of this Contract with respect to any Confidential Information retained subject to clauses (a) or (b). No license, express or implied, in the Confidential Information is granted to the Recipient other than to use the Confidential Information in the manner and to the extent authorized by this Contract. Discloser represents and warrants that it is authorized to disclose any Confidential Information it discloses pursuant to this Contract.

Section 9.18 Business License

In the event a local business license is required for WatchGuard to perform services hereunder, the County will promptly notify WatchGuard and provide WatchGuard with the necessary paperwork and/or contact information so that WatchGuard may timely obtain such license.

Section 9.19 Governing Law; Jurisdiction

This Agreement shall be governed by the laws of the State of Ohio (regardless of the laws that might be applicable under principles of conflicts of law) as to all matters, including but not limited to matters of validity, construction, effect, and performance. All actions regarding this Agreement shall be forumed and venued in the United States District Court for the Southern District of Ohio or the Court of Common Pleas General Division located in Franklin County, Ohio and the parties hereby consent to the jurisdiction of such courts.

Section 9.20 Multiple Originals and Authorized Signatures

This Agreement may be executed in multiple originals, any of which will be independently treated as an original document. The parties may sign in writing or by electronic signature. An electronic signature, facsimile copy will be treated, and will have the same effect as an original signature, and will have the same effect, as an original signed copy of this document. Each party represents to the other that the signatory set forth below is duly authorized to bind that party to this Agreement.

Section 9.21 Offshore Activities

No portion of this Agreement may be performed offshore. All services under this Agreement shall be performed within the borders of the United States or within the borders of any country with which the United States is engaged in an active free trade agreement. Any services that are described in the specifications or Statement of Work that directly pertain to servicing this Agreement shall be performed within the borders of the United States or within the borders of any country with which the United States is engaged in an active free trade agreement. This shall include any back up services for Data, back-office services, and work performed by subcontractors at all tiers.

Section 9.22 Contract Documents

This Agreement includes by reference Exhibits 1 through 5 of the Services Contract. The following exhibits are also included herein:

Exhibit A	Service Level Agreement
Exhibit B	Support Call Process
Exhibit C	Third Party Terms

{Remainder of page left blank. Signature page to follow.}

The parties hereto have set their hands and seal this ___________________________________.

Franklin County Board of Commissioners:	**WatchGuard Video, Inc.:**
By:________________________ Erica C. Crawley, President	By: Giles Tipsword 2/3/2022 | 7:13 PM EST Giles Tipsword, MSSSI Vice President
By: ______________________________ John O'Grady, Commissioner	
By: ______________________________ Kevin L. Boyce, Commissioner	

APPROVED AS TO FORM: G. Gary Tyack Prosecuting Attorney Franklin County, Ohio	APPROVED AS TO FORM: Megan A. Perry-Balonier Director, Purchasing Department Franklin County, Ohio
By: Jesse Armstrong Assistant Prosecuting Attorney Date: 2/3/2022 | 7:46 PM EST	By: Megan Perry-Balonier Date: 2/3/2022 | 7:19 PM EST

EXHIBIT A

SERVICE LEVEL AGREEMENT

I. Agreement Overview

This SLA operates in conjunction with, and does not supersede or replace any part of, the Agreement. It outlines the information technology service levels that WatchGuard will provide to the County to ensure the availability of the application services that the County has requested WatchGuard to provide. All other support services are documented in the Support Call Process.

II. Definitions. Except as defined below, all defined terms have the meaning set forth in the Agreement.

- *Attainment:* The percentage of time the WatchGuard Software is available during a calendar quarter, with percentages rounded to the nearest whole number.
- *County Error Incident*: Any service unavailability resulting from the County's applications, content, equipment, or the acts or omissions of any of County service users or third party providers over whom WatchGuard exercises no control.
- *Downtime*: Those minutes in any quarter of Service during which the WatchGuard Software is not available for County's use, whether due to the WatchGuard Software or the Hosting Solution. Downtime does not include those instances in which only a Defect is present or as a result of one or more of the exclusions.
- *Emergency Maintenance*: The (1) maintenance that is required to patch a critical security vulnerability, (2) maintenance that is required to prevent an imminent outage of Service Availability, or (3) maintenance that is mutually agreed upon in writing by WatchGuard and the County.
- *Scheduled Downtime*: WatchGuard performs regularly scheduled maintenance on Saturdays from 10 p.m. to 6 a.m. EST and may extend into Sunday depending on conditions. For such other Scheduled Downtime to allow the performance of maintenance on the WatchGuard Solution, WatchGuard shall provide to the County notice of such activities. WatchGuard shall, to the maximum extent practicable, provide 3 days notice, but notice shall not be less than 48 hours prior to such activity. Scheduled Downtime will consist of no more than twelve (12) hours per month.
- *Service Availability*: The total number of minutes in a calendar quarter that the WatchGuard Software is capable of receiving, processing, and responding to requests, excluding Scheduled Downtime, Emergency Maintenance, County Error Incidents, and Force Majeure.

III. Service Availability

The Service Availability of the WatchGuard Software is intended to be 24/7/365. WatchGuard sets Service Availability goals and measures whether WatchGuard has met those goals by tracking Attainment.

a. County Responsibilities

Whenever County experiences Downtime, County must make a support call according to the procedures outlined in the Support Call Process. County will receive a Trouble Ticket incident number.

All Downtime that the County has experienced during a calendar quarter should be emailed to WatchGuard quarterly as outlined in the notices section. The County must deliver such documentation to WatchGuard within 30 days of a quarter's end if County is requesting a credit.

b. WatchGuard Responsibilities

When WatchGuard's support team receives notification from the County that Downtime has occurred or is occurring, WatchGuard will work with the County to identify the cause of the Downtime (including whether it may be the result of a County Error Incident or Force Majeure). WatchGuard will also work with the County to resume normal operations.

Upon timely receipt of the County's Downtime report, WatchGuard will compare that report to WatchGuard's own outage logs and support tickets to confirm that Downtime for which WatchGuard was responsible indeed occurred.

WatchGuard will respond to the County's Downtime report within 7 days of receipt. To the extent WatchGuard has confirmed Downtime for which WatchGuard is responsible, WatchGuard will provide the County with the relief set forth below.

c. County Relief

When a Service Availability goal is not met due to confirmed Downtime, WatchGuard will provide the County with relief that corresponds to the percentage amount by which that goal was not achieved, as set forth in the County Relief Schedule below.

Notwithstanding the above, the total amount of all relief that would be due under this SLA per quarter will not exceed 15% of one quarter of the then-current SaaS Fees. The total credits confirmed by WatchGuard in one or more quarters of a billing cycle will be applied to the SaaS Fees for the next billing cycle. Issuing of such credit does not relieve WatchGuard of WatchGuard's obligations under the Agreement to correct the problem which created the service interruption.

Every quarter, WatchGuard will compare confirmed Downtime to Service Availability. In the event actual Attainment does not meet the targeted Attainment, the following County relief will apply, on a quarterly basis:

Targeted Attainment	Actual Attainment	County Relief
100%	99-100%	No credit will be issued
100%	95-98.9%	5% credit of fee for affected calendar quarter will be posted to next billing cycle
100%	91-94.9%	10% credit of fee for affected calendar quarter will be posted to next billing cycle
100%	<91%	15% credit of fee for affected calendar quarter will be posted to next billing cycle

The County may request a report from WatchGuard that documents Service Availability, Downtime, any remedial actions that have been/will be taken for any time period specified by the County through WatchGuard's Support Call Process. WatchGuard will provide such report no later than seven (7) days from the date of County's request.

IV. Applicability and Exclusions

The commitments for service availability set forth in this SLA do not apply during Scheduled Downtimes, Emergency Maintenance, County Error Incidents, and Force Majeure.

WatchGuard performs maintenance during Scheduled Downtime. Scheduled Downtime shall occur during times known to be reliably low-traffic times. If and when maintenance is predicted to occur during periods of higher traffic, WatchGuard will work with the County to define a mutually agreeable window for that maintenance.

(a) Causes beyond WatchGuard's reasonable control, for example natural disaster, war, acts of terrorism, riots, government action, or the performance of any third-party hosting provider or communications or internet service provider;
(b) Any unauthorized action or lack of action when required by County, or County's employees, agents, contractors or vendors, or anyone gaining access to the Service by means of County's passwords or equipment, or otherwise resulting from County's failure to following commercially reasonably security practices;
(c) County's failure to adhere to any required configurations, follow any policies for acceptable use or use the Service in a manner consistent with the features and functionality of the Service described in the proposal;
(d) Caused by County's use of a Service after WatchGuard advised County to modify County's use of the Service, if County did not modify County's use as advised;
(e) Failure, interruption, outage, inadequate bandwidth, or other problem with any software, hardware, system, network, or facility that WatchGuard has not provided or authorized pursuant to the Agreement (other than third-party software or equipment within WatchGuard's direct control);
(f) During or with respect to preview, pre-release, beta or trial versions of a service, feature or software;
(g) Scheduled Downtime or backups to the Services; or
(h) Disabling, suspension, or termination of the Services by Watchguard in accordance with the respective rights granted by the Agreement

V. Reserved

VI. Force Majeure

The County will not hold WatchGuard responsible for not meeting service levels outlined in this SLA to the extent any failure to do so is caused by Force Majeure. In the event of Force Majeure, WatchGuard will file with the County a signed request that said failure be excused. That writing will at least include the essential details and circumstances supporting WatchGuard's request for relief pursuant to this Section. The County will not unreasonably withhold its acceptance of such a request.

EXHIBIT B

SUPPORT CALL PROCESS

I. Definitions

Except as defined below, all defined terms have the meaning set forth in the Agreement.

- **"Circumvention Procedures"** means a temporary resolution for a reported Defect.
- **"Incident"** or **"Support Incident"** means a Defect reported using the Support Channels listed below or any items listed under the characteristics of Support Call Process Table below.

II. Support Channels and Resources

WatchGuard provides the following channels of software support for authorized users:

Premier Support Service
Premier Support Service provides a dedicated resource assigned to the County's account. This Technical Account Manager (TAM), proactively monitors the system, communicates with the County and takes recovery actions to remedy the incident. Premier Support includes the following enhanced services.

Dedicated Premier Support Technical Account Manager
The dedicated TAM acts as the County's primary support contact and is responsible for staying current on the County's system configuration, documenting changes, performing proactive monitoring and ensuring the health of the system. The TAM acts as a customer advocate for support activities within WatchGuard. TAM performs problem resolution activities ranging from end-user assistance to remote diagnostics and system configuration, all the while updating status, notes and results.

(1) Telephone – A service representative can be reached at any time by dialing WatchGuard's toll-free phone support number - (800) 605-6734.
(2) Website - Service requests can also be made on WatchGuard's website at https://www.motorolasolutions.com/en_us/support/watchguard.html

III. Support Availability

WatchGuard views quality customer service and support as the foundational function of the organization. A service representative can be reached 24/7/365.

IV. Incident Handling

Incident Tracking and Management

Incident Management
The goal of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. The Technical Support team will perform the following tasks to deliver Incident Management upon notification from the County:

- Trouble Ticket Generation
- Trouble Isolation

- Track/Manage Incident to Closure

Not all of the above functions are included in all levels of service. The following sections describe these features and functions in more detail.

Trouble Isolation
Trouble Isolation activities are initiated when an Incident is generated and include:

- Fault Isolation
- Service Issue Resolution
- Hardware Issue Resolution
- Hardware Logical Configuration Resolution

Track/Manage Events to Closure
A web-based trouble ticketing system will be used by WatchGuard and County to monitor the history of Incidents. A trouble ticket tracks all of the activity associated with the outage including the following:

- Status changes
- Related tickets are associated with the Incident.
- Comments are added to the ticket as developments and testing is completed
- Fix Agency feedback is added to the ticket
- Resolution is captured, and the ticket is solve
- Tickets are created whenever the County informs the Service Desk of an Incident.

Problem Management
Problem Management includes the monitoring, identification and resolution of chronic incidents. A chronic incident is any repeated problem or pattern of problems with a device, location or service. A chronic condition may be the result of an intermittent hardware, circuit, software, power issue or periodic congestion on the network. When reported, these conditions initiate the problem management process to determine if there is a problem which otherwise would go unnoticed until actual failure. Once the chronic condition has been identified, root cause analysis of the problem will be performed, and appropriate actions will be taken by the team to prevent Incidents from reoccurring.

Release Management
Release Management is used for the distribution of software. Purchase of the Software Warranty ensures the availability of licensed, tested, and version-certified software, which functions as intended when introduced into existing infrastructure. Quality control during the implementation of new software is also the responsibility of Release Management. This guarantees that all software meets the demands of the business processes. The goals of release management are:

- Plan and schedule the software upgrade
- Effectively communicate and manage expectations of the County during the planning and rollout of new releases
- Control the distribution and installation of changes to IT systems
- The focus of release management is the protection of the live environment and its services through the use of formal procedures and checks.

Change Management
Change Management involves development and interlock with the County's change management process. Upon interlock, change management will be responsible for:

- Definition of the changes required
- Measuring the impact of the proposed change
- Developing a back out plan
- Obtaining any relevant approvals for change

- Scheduling the implementation of the changes
- Testing the change as applicable
- Implementing the change

For each reported Defect, WatchGuard shall assign appropriate personnel to diagnose and correct the reported Defect as set forth in the chart below. WatchGuard's initial response shall include an acknowledgement of notice of the reported Defect and confirmation that WatchGuard has received sufficient information concerning the reported Defect. Remediation of reported Defects shall include either notification of WatchGuard's resolution or an action plan for resolution of the reported Defect. All Defects reported to WatchGuard by the County shall be resolved by restoring the WatchGuard Solution to the same functionality that existed just prior to the reported Defect, unless otherwise agreed by the County.

Defect resolution can be deployed in a Patch, which includes Defect remediation only, or a release which includes Defect remediation and new functionality.

Once an issue is resolved, the County is notified by phone or email, and they are also able to see status updates on the website. If a software update is needed, the County is notified of which software version the remedy will be placed in. Updates are available for download via the internet.

Response Times

The County may connect with County's Dedicated Premier Support TAM during Business Hours (7:00 AM – 6:00 PM CST) or After Hours (6:00 PM – 7:00 AM CST), for reporting, recording and resolution of Incidents. The County's TAM will adhere to the following response times to ensure a better alignment to County's priorities.

Incident Priority	**Definition**	**Premier Response Time – Business Hours**	**Premier Response Time – After Hours**
Low	Incident impacting a single camera's ability to record/upload or a single user's ability to review video/login.	< 20 Minutes	< 60 Minutes
Medium	Incident involving more than one camera's ability to record/ upload or more than one user's ability to review video/login.	< 20 Minutes	< 20 Minutes
High	Incident affecting all cameras ability to record/upload or all users ability to review video/login. All *Server Down* issues are High Priority.	< 20 Minutes	< 20 Minutes

Incident Priority

Each Incident is assigned a priority level, which corresponds to the County's needs and deadlines. WatchGuard and the County will reasonably set the priority of the Incident per the chart below. This chart is not intended to address every type of support Incident. The goal is to help guide the County towards clearly understanding and communicating the importance of the issue and to describe generally expected response and resolution targets in the production environment only.

References to a "confirmed Support Incident" mean that WatchGuard and the County have successfully validated the reported Defect/Support Incident.

As to Defects caused by any third party vendor utilized by WatchGuard Software for core functionality, WatchGuard shall not be subject to the timeframes set forth under Resolution Targets in the below table to resolve the Support Incident. Notwithstanding the foregoing, WatchGuard shall be required to provide an initial response as required by the Resolution Targets. WatchGuard will use commercially reasonable efforts to work with the third party vendor to resolve the Defect, which may include a circumvention procedure.

Support Call Process Table		
Priority Level	Characteristics of Support Incident	Resolution Targets
1 High	Support Incident that causes (a) complete WatchGuard Software failure or WatchGuard Software unavailability; (b) WatchGuard Software failure or unavailability in one or more of the County's remote location; (c) systemic loss of multiple essential system functions; or (d) loss or corruption of Data affecting multiple essential system functions. Including, but not limited to: • Export Service ○ Only at High Priority Request for Evidence Export for a Court Case-Eminent requirement (Including any shooting event or District Attorney request, etc) ○ **Workaround -** Manually provide Raw Video • Login Issues ○ No Officers can log in • Reinstallation due to hardware failure / ransomware • SERVER DOWN • If recording devices are full and loss of evidence is imminent Change Priority to P1.	WatchGuard shall provide an initial response to Priority Level 1 Incidents within one business hour of receipt of the Incident. Once the Incident has been confirmed, WatchGuard shall use commercially reasonable efforts to resolve such Support Incidents or provide a Circumvention Procedure within one business day. For lost or corrupted Data not due to a declared Disaster, WatchGuard is responsible for the restoration of Data to the most recent backup.

Support Call Process Table		
Priority Level	Characteristics of Support Incident	Resolution Targets
2 Major/Medium	Support Incident that causes (a) repeated, consistent failure of essential functionality affecting more than one user, or (b) loss or corruption of Data. Including, but not limited to: • Out of Storage Space • Wireless Service Down ○ All cars are not uploading ○ VTS or VTS2 not importing • Import Service Down • Export Service Down	WatchGuard shall provide an initial response to Priority Level 2 Incidents within four business hours of receipt of the Incident. Once the Incident has been confirmed, WatchGuard shall use commercially reasonable efforts to resolve such Support Incidents or provide a Circumvention Procedure within ten business days. For lost or corrupted Data not due to a declared Disaster, WatchGuard is responsible for the restoration of Data to the most recent backup.
3 Minor/Low	Priority Level 1 Incident with an existing Circumvention Procedure that is accepted by the County, or a Priority Level 2 Incident that affects only one user or for which there is an existing Circumvention Procedure. Including, but not limited to: • One or a few events Stuck Importing, Partial, Faulted ○ Exceptions would be if needed for a Court Case. • DVD Robot • Rimage • CloudShare • Export to Removable Media • Manually copy to Removable Media • Wireless Access Point • Time Sensitive RATF (Record-After-the-Fact) to create for body worn or in car • Time Sensitive Video Pull • In car or body worn device that will not record new evidence	WatchGuard shall provide an initial response to Priority Level 3 Incidents within one business day of receipt of the incident. Once the Incident has been confirmed, WatchGuard shall use commercially reasonable efforts to resolve such Support Incidents without the need for a Circumvention Procedure with the next published maintenance update or service pack, which shall occur at least quarterly.

Support Call Process Table		
Priority Level	Characteristics of Support Incident	Resolution Targets
4 Service Requests	Support Incident that causes failure of non-essential functionality or a cosmetic or other issue that does not qualify as any other Priority Level. Including, but not limited to: • RMA • Flip • Password change • Not Product related • SQL Queries, audits • How to… • Upgrade Request • Wireless Microphone / Cabin Microphone not recording audio • Etc.	WatchGuard shall provide an initial response to Priority Level 4 Incidents within two business days of receipt of the Incident. Once the Incident has been confirmed, WatchGuard shall use commercially reasonable efforts to resolve such Support Incidents, as well as cosmetic issues, with a future version release.

Incident Escalation

WatchGuard's support consists of four types of personnel:

(1) Technical Account Manager ("TAM");
(2) Support Desk Representative - (800) 605-6734;
(3) Premier Support Manager (Phil Rhoades: Phil.Rhoades@motorolasolutions.com); and
(4) Local Account Team (Stuart Johnson: stuart.johnston@motorolasolutions.com; Matt Marino: matthew.marino@motorolasolutions.com).

Remote Support Tool

Some support calls may require further analysis of the County's database, processes, or setup to diagnose a problem or to assist with a question. WatchGuard will, at its discretion and with notice to the County, use an industry-standard remote support tool. WatchGuard's support team must have the ability to quickly connect to the County's system and view the site's setup, diagnose problems, or assist with screen navigation. WatchGuard shall, upon request, provide information about WatchGuard's remote support tool.

Quarterly Business Reviews

WatchGuard will conduct quarterly business reviews via video conference or on-site. Quarterly reviews ensure continued alignment around County's operational goals and WatchGuard's performance. Detailed reports provide insightful and actionable data.

Annual System Health Check

WatchGuard will conduct annual system health checks which proactively prevent potential issues and improve on-going performance. The service is performed on-site or remotely using tools to evaluate the operating status, configuration, alarms and performance of major system components.

EXHIBIT C
THIRD PARTY TERMS

Microsoft As-a-Service Terms

END USER LICENSE TERMS

TERMS AND CONDITIONS REGARDING USE OF MICROSOFT SOFTWARE

This document governs the use of Microsoft software, which may include associated software, media, printed materials, and "online" or electronic documentation (individually and collectively, "Products") provided by Motorola Solutions, Inc. (hereinafter referred to as "Customer"). Customer does not own the Products and the use thereof is subject to certain rights and limitations of which Customer must inform you. Your right to use the Products is subject to the terms of your agreement with Customer, and to your understanding of, compliance with, and consent to the following terms and conditions, which Customer does not have authority to vary, alter, or amend.

1. DEFINITIONS. "Client Software" means software that is installed on a Device that allows the Device to access or utilize the Products. "Device" means each of a computer, workstation, terminal, handheld PC, pager, telephone, personal digital assistant, "smart phone," server or any other hardware where software can be installed that would allow End User to interact with the Product. "End User" means an individual or legal entity that obtains Software Services directly from Customer, or indirectly through a Software Services Reseller. "Redistribution Software" means the software described in Paragraph 4 ("Use of Redistribution Software") below. "Software Services" means services that Customer provides to you that make available, display, run, access, or otherwise interact, directly or indirectly, with the Products. Customer must provide these services from data center(s) through the Internet, a telephone network or a private network, on a rental, subscription or services basis, whether or not Customer receives a fee. Software Services exclude any services involving installation of a Product directly on any End User device to permit an End User to interact with the Product.

2. OWNERSHIP OF PRODUCTS. The Products are licensed to Customer from an affiliate of the Microsoft Corporation (collectively "Microsoft"). Microsoft Products are protected by copyright and other intellectual property rights. Products and other Product elements including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Products are owned by Microsoft or its suppliers. You may not remove, modify or obscure any copyright trademark or other proprietary rights notices that are contained in or on the Products. The Products are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Your possession, access, or use of the Products does not transfer any ownership of the Products or any intellectual property rights to you.

3. USE OF CLIENT SOFTWARE. You may use the Client Software installed on your Devices only in accordance with your agreement with Customer and the terms under this document, and only in connection with the Software Services, provided to you by Customer. The terms of this document permanently and irrevocably supersede the terms of any Microsoft End User License Agreement that may be presented in electronic form during the installation and/or use of the Client Software.

4. USE OF REDISTRIBUTION SOFTWARE. In connection with the Software Services provided to you by Customer, you may have access to certain "sample," "redistributable" and/or software development software code and tools (individually and collectively "Redistribution Software"). You may use, copy and/or install the Redistribution Software only in accordance with the terns of your agreement with Customer and this document and/or your agreement with Customer.

5. COPIES. You may not make any copies of the Products; provided, however, that you may (a) make one copy of Client Software on your Device as expressly authorized by Customer; and (b) you may make copies of certain Redistribution Software in accordance with Paragraph 4 (Use of Redistribution Software). You must erase or destroy all such Client Software and/or Redistribution Software upon termination or cancellation of your agreement with Customer, upon notice from Customer or upon transfer of your Device to another person or entity, whichever occurs first. You may not copy any printed materials accompanying the Products.

6. LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the Products, except and only to the extent that applicable law, notwithstanding this limitation, expressly permits such activity.

7. NO RENTAL. You may not rent, lease, lend, pledge, or directly or indirectly transfer or distribute the Products to any third party, and may not permit any third party to have access to and/or use the functionality of the Products except for the sole purpose of accessing the functionality of the Products in the form of Software Services in accordance with the terms of this agreement and any agreement between you and Customer.

8. TERMINATION. Without prejudice to any other rights, Customer may terminate your rights to use the Products if you fail to comply with these terms and conditions. In the event of termination or cancellation of your agreement with Customer or Customer's agreement with Microsoft under which the Products are licensed, you must stop using and/or accessing the Products, and destroy all copies of the Products and all of their component parts within thirty (30) days of the termination of your agreement with Customer.

9. NO WARRANTIES, LIABILITIES OR REMEDIES BY MICROSOFT. Microsoft disclaims, to the extent permitted by applicable law, all warranties and liability for damages by Microsoft or its suppliers for any damages and remedies whether direct, indirect or consequential, arising from the Software Services. Any warranties and liabilities are provided solely by Customer and not by Microsoft, its affiliates or subsidiaries.

10. PRODUCT SUPPORT. Any support for the Software Services is provided to you by Customer or a third party on Customer's behalf and is not provided by Microsoft, its suppliers, affiliates or subsidiaries.

11. NOT FAULT TOLERANT. The Products are not fault tolerant and are not guaranteed to be error free or to operate uninterrupted. You must not use the Products in any application or situation where the Product(s) failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage ("High Risk Use").

12. EXPORT RESTRICTIONS. The Products are subject to U.S. export jurisdiction. Customer must comply with all SPLA2013CustomerLicenseTerms(WW)(ENG)(Apr2014) Page 2 of 2 applicable laws including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. For additional information, see http://www.microsoft.com/exporting/.

13. LIABILITY FOR BREACH. In addition to any liability you may have to Customer, you agree that you will also be legally responsible directly to Microsoft for any breach of these terms and conditions.

14. INFORMATION DISCLOSURE. You must permit Customer to disclose any information requested by Microsoft under the Customer's Agreement. Microsoft will be an intended third party beneficiary of your agreement with Customer, with the right to enforce provisions of your agreement with Customer and to verify your compliance.

EXHIBIT 3

NON-DISCRIMINATION AND EQUAL EMPLOYMENT OPPORTUNITY AFFIDAVIT

STATE OF Ohio

COUNTY/PARISH OF Franklin

GILES TIPSWORD being first
(Printed Name)

duly sworn, deposes and says that they are MSSSI Vice President
(President, Secretary, Etc.)

of WatchGuard Video Inc, that such party as contractor does not and shall not discriminate against any employee or applicant for employment because of race, religion, color, sex, or national origin. If awarded the contract, said party shall take affirmative action to insure that applicants are employed and that employees are treated, during employment, without regard to their race, religion, color, sex, or national origin. If successful as the lowest and best bidder under the foregoing bids, this party shall post non-discrimination notices in conspicuous places available to employees and applicants for employment, setting forth the provisions of this affidavit.

Signature

Giles Tipsword
Affiant

WatchGuard Video Inc
Company/Corporation

350 Worthington Road, Suite C
Address

Westerville, Ohio 43082
City/State/Zip Code

Sworn to and subscribed before me this 31st day of January, 2022.

Notary Public

My Commission expires on November 20, 2023.
(Seal)

NOTARIAL SEAL
STATE OF OHIO

GREGORY A. BROWN
Notary Public
In and for the State of Ohio
My Commission Expires
November 20, 2023

EXHIBIT 4

DELINQUENT PERSONAL PROPERTY TAX AFFIDAVIT

This sworn affidavit should be properly completed by the authorized representative of your firm and will be incorporated as a portion of the bids and resulting contract for the following:

Project: Service Contract and SaaS Agreement between WatchGuard Video Inc and Franklin County Board of Commissioners

Department: Franklin County Sheriff's Office

State of Ohio County of Franklin, ss:

GILES TIPSWORD Being first duly sworn, deposes and says that he/she is the
(Name)

MSSSI Vice President of WatchGuard Video Inc
(Title)

with offices located at 350 Worthington Road, Suite C, Westerville, Ohio 43082,

and as it's duly, authorized representative states that effective this day of 1/31/2022,

(X) is not charged with delinquent property taxes on the general list of personal property in Franklin County, Ohio, or any other counties containing property in the taxing districts under the jurisdiction of the Auditor of Franklin County, Ohio.

(   ) is charged with delinquent personal property taxes on the general list of personal property in Franklin County, Ohio, or any other counties containing property in the taxing districts under the jurisdiction of the Auditor of Franklin County, Ohio.

County	Amount: (include total amount and any penalties and interest thereon)
Franklin	$
	$
	$

Giles Tipsword
(Affiant)

Sworn to and subscribed this 31st day of January, 2022.

(Notary Public)

Section 5719.042 O.R.C.

My Commission expires November 20, 2023
(Seal)

NOTARIAL SEAL
STATE OF OHIO

GREGORY A. BROWN
Notary Public
In and for the State of Ohio
My Commission Expires
November 20, 2023

Exhibit 5

FRANKLIN COUNTY TRAVEL POLICY

A. AUTHORIZATION TO TRAVEL

1. Each County agency, court, board, and/or commission should ensure that all requests for travel are necessary and essential before authorizing travel on County business. Managers should make every effort to limit both in-county and out-of-county travel when other alternatives are available (e.g. conference calls, video conferencing, webinars, carpooling, use of county-owned vehicles, etc.). **The employee's management is responsible for ensuring that the expenses listed are appropriate for the travel and meet the travel policy requirements contained herein.**

2. Requests for travel requiring an overnight stay, approved by the employee's management, should be submitted on a "Request for Authorization to Travel on County Business" form (copy attached). Every effort should be made to take advantage of early or advance registration discounts. The conference brochure or a similar document must accompany the travel authorization form, as well as any request for payment associated with the trip.

3. The Board of Commissioners shall routinely approve all travel requiring an overnight stay, where expenses are anticipated to be incurred by Franklin County officials or employees. **All such travel expenses shall be encumbered in accordance with the County's purchase order policy, and except for emergency travel the purchase order must be approved prior to the date of travel.** The purchase order must include all of the costs associated with the travel, including any conference registration fees.

4. In the event a purchase order cannot be approved prior to the overnight travel event, emergency travel may be temporarily authorized by a Commissioner or the highest level administrative person available at the time the travel is deemed necessary. This authorization is evidenced by the signature of a Commissioner, County Administrator, or Deputy County Administrator on the travel authorization form and must be obtained prior to the date of travel. The Board of Commissioners must approve subsequent reimbursement for these expenses.

5. As used in this policy, references to reimbursement and payment in advance includes use of a procurement card for the payment of the applicable expenses. Please refer to the Procurement Card Program Policy and Procedures for additional detail and requirements.

Exhibit 5

B. PROHIBITIONS

1. No employee or official of Franklin County shall solicit or receive travel expenses, or accept payment of registration fees and/or lodging for their attendance at a conference, from a party that is interested in matters before, regulated by, or doing or seeking to do business with the particular department or agency involved.

2. Employees or officials of Franklin County are prohibited from accumulating, for personal use, “frequent flyer” miles earned on official travel that is paid for or reimbursed by the government. Any employees or officials of Franklin County must use such miles earned for future official travel for that employee or another employee of Franklin County, or forfeit such miles. This ruling is mandated per Ohio Ethics Commission Advisory Opinion No. 91-010 and cited in the Auditor of State’s Ohio Compliance Supplement Manual.

3. Under no circumstance will entertainment or alcoholic beverages be reimbursed. If a charge for alcoholic beverages is included in the event’s registration or conference fee, that cost must be deducted from the fee.

Exhibit 5

C. TRAVEL WITHOUT AN OVERNIGHT STAY

1. Expenses that are eligible for reimbursement without an overnight stay are registration or conference fees, mileage, fuel for a County-owned vehicle, parking, and tolls.

2. While a “Request for Authorization to Travel on County Business” form is not required to be completed for travel reimbursements that do not involve an overnight stay, it is recommended that County offices use the form or other appropriate documentation to monitor and approve these types of travel reimbursements.

3. Registration or conference fees may be paid directly by the County in advance of the event. The payment of the fee may be made through a purchase order, or by direct voucher if the payment qualifies under the guidelines set forth in the Franklin County Purchasing Policy.

4. A separate blanket purchase order may be opened for the purpose of paying for registration fees associated with travel without an overnight stay. However, in no event may such a blanket purchase order be used for the payment of a registration fee that does involve an overnight stay.

5. Some seminars and conferences include the price of a meal as part of the program. In those cases, meal purchases as part of the registration are allowable. When the meal is being provided by the conference but the employee chooses to eat elsewhere, reimbursement will not be made for the other meal.

6. Employees are encouraged to contact Fleet Management at 525-3412 for the use of a pool vehicle. When use of a pool vehicle is not practicable, travel by privately-owned vehicle is permissible if the owner is insured under a policy of liability insurance, and the driver has a valid driver’s license.

7. Reimbursement for mileage, parking, fuel for a County-owned vehicle, and tolls is made through the employing agency’s payroll department, does not require a purchase order and does not need to be submitted to the Auditor’s Office. Effective January 1, 2012, mileage is reimbursable at the standard mileage rate established by the IRS for business expenses or fifty cents ($0.50) per mile, whichever is less. Reimbursement shall be made to only one of two or more County employees traveling in the same privately-owned automobile. The names of all persons traveling in the same privately-owned automobile should be listed on the Employee Reimbursement Request form.

Exhibit 5

8. Travel during on-duty hours must utilize the most direct route unless an alternate route would be less time consuming and/or more effective. During on-duty hours, employees shall not deviate from the route of travel or stop along the route of travel to conduct personal business or engage in any activity that is not within their assigned or required duties.

9. For travel outside of the County, the total reimbursable mileage for the trip is equal to the lesser of:

   a) The distance from the individual's workplace to the destination, and back to the individual's workplace.

   b) The distance from the individual's place of residence to the destination, and back to the individual's place of residence.

10. When it is necessary for an employee to travel from his/her normal work location to any other location for purposes of conducting assigned or required duties, the mileage reimbursement rate shall apply for the actual miles driven. Employees must maintain a record of daily travel documenting the locations and the distance between, for which reimbursement is being sought.

11. When assigned or required duties make it necessary for an employee to travel from his/her home to any other location which is not his/her normal work location, or

    When assigned or required duties make it necessary for an employee to travel from his/her normal work location to any other location prior to proceeding home, then

    The employees will be reimbursed only for the mileage in excess of that which would have been incurred by the employee's normal commute. Under no circumstances will an employee be reimbursed for mileage attributable to the employee's normal commute, regardless of the day's business travel requirements.

Exhibit 5

D. OVERNIGHT TRAVEL – TRAVEL STATUS

1. Authorized travel status generally begins when the employee departs to the event from the employee's normal work location, or start of the workday if departing from the employee's place of residence. However, employees arriving up to two hours prior to a plane's departure are considered to be on authorized travel status.

2. Authorized travel status generally ends upon the earliest of a) the return of the employee to Franklin County, or b) the return of the employee to the county of the employee's place of residence.

3. In some instances, a lower fare for travel by airplane may be obtained with extended or weekend travel, but which will result in additional lodging, meal, or other travel costs. An employee may request approval of such extended or weekend travel arrangements where it can be demonstrated that the fare savings exceed the additional travel costs incurred for lodging and meals. Such travel time is on the employee's own time, and may not be credited towards overtime or compensatory/administrative time calculations. If additional travel time is needed due to the above extended personal layover, then this time must be charged to the employee's accrued leave balances (excluding sick leave) when the travel time occurs during the work day.

4. If the first scheduled event of a conference or seminar is scheduled to begin at or before 11:00 A.M. (Eastern Time), an employee may depart the day prior to the event. If the first scheduled event begins after 11:00 A.M. (Eastern Time), an employee is expected to depart that same day unless the employee can document either a) the savings as required by the requirements for extended travel above, b) that no flight was available that same day, or c) a reasonable justification that is approved by the employee's supervisor at the time the travel is authorized. The documentation should be prepared at the time the travel is authorized or flight reservation is made and must be provided to the Auditor's Office at time of submission for reimbursement.

5. If the last scheduled event of a conference or seminar is scheduled to conclude by 5:00 P.M. (Eastern Time), an employee is expected to return that same day unless the employee can document either a) the savings as required by the requirements for extended travel above, or b) that no flight was available that same day, or c) a reasonable justification that is approved by the employee's supervisor at the time the travel is authorized. The documentation should be prepared at the time the travel is authorized or flight reservation is made and must be provided to the Auditor's Office at time of submission for reimbursement.

Exhibit 5

E. OVERNIGHT TRAVEL – REGISTRATION FEES

1. Reimbursement is authorized for registration fees associated with a conference or event associated with travel. Registration fees may also be paid directly by the County in advance. These fees must be included in the purchase order requesting authorization for travel and reimbursement of expenses, and is not to be paid prior to this authorization. A separate purchase order shall not be opened solely for the purpose of paying registration fees associated with overnight travel without providing the detail of the other expenses associated with the travel.

2. In addition to the receipt submitted for reimbursement under this section, the proper evidentiary matter submitted to the Auditor's office must include the agenda or itinerary of the conference or event.

3. If a charge for alcoholic beverages is included in the registration fee for the conference or event, that cost must be deducted from the reimbursement request.

4. Both the employee and the employee's management are responsible for ensuring that no alcoholic beverages are purchased and consumed under this section. The signatures on the Employee Reimbursement Request form certify that no alcoholic beverages were included in the registration fee for the conference or event.

Exhibit 5

F. TRAVEL BY AIRPLANE

1. Out of County travel by airplane is authorized at the lowest logical rate, taking advantage of early reservation discounts wherever possible, and includes reimbursement of any reasonable baggage fees (no more than two bags each way). The determination of the lowest rate can include the savings associated with the reduction in travel time in selecting a nonstop flight. The purchase of a ticket through a travel agent shall be deemed to be at the lowest available rate, and includes reimbursement of any associated service fees.

2. The County will allow payment directly to travel agents or airlines in advance of the travel date. Reimbursement to employees may also be made prior to the travel date if the employee has paid for the tickets in advance and can provide documentation to that effect.

3. In cases where a trip is cancelled and the airline processes a travel voucher/airline credit in lieu of a refund, the employee may still be reimbursed for the expenses incurred in purchasing that ticket. The travel voucher/airline credit should only be used on a subsequent business trip authorized by agency management and the Board of Commissioners. If the employee desires to use the travel voucher/airline credit for personal use, the employee may purchase the travel voucher/airline credit by reimbursing the County for the original amount of the ticket. Agency management is responsible for the managing and tracking of proper use of travel vouchers/airline credits.

4. Requests to travel by personal vehicle where travel by airplane is the most efficient means may be authorized only where the employee can document a cost savings over the lowest available fare, or is willing to accept reimbursement of travel costs equal to those that would have been incurred by the lowest advance purchase fare. Where such travel arrangements result in additional travel time, the employee shall charge this additional time to his/her vacation or other accumulated leave balances (excluding sick leave).

Exhibit 5

G. OVERNIGHT TRAVEL – TRAVEL BY VEHICLE

1. County-owned Vehicles - Employees who are authorized or required to operate a County-owned vehicle must have a valid driver's license. For travel in a County-owned vehicle, the total cost of gasoline and oil shall be reimbursed upon the submittal of receipts, after the employee's management verifies the reasonableness of the costs incurred. A copy of the Fleet Management logbook indicating the odometer readings supporting the miles driven shall be completed for all trips and shall accompany requests for reimbursement of gasoline.

2. Employees are encouraged to contact Fleet Management at 525-3412 for the use of a pool vehicle. When use of a pool vehicle is not practicable, travel by privately-owned vehicle is permissible if the owner is insured under a policy of liability insurance, and the driver has a valid driver's license.

3. Mileage is reimbursable at the standard mileage rate established by the IRS for business expenses or fifty cents ($0.50) per mile, whichever is less. Reimbursement shall be made to only one of two or more County employees traveling in the same privately-owned automobile. The names of all persons traveling in the same privately-owned automobile should be listed on the "Request for Authorization to Travel on County Business" form. The total reimbursable mileage for the trip is equal to the lesser of:

   a) The distance from the individual's workplace to the destination, and back to the individual's workplace.

   b) The distance from the individual's place of residence to the destination, and back to the individual's place of residence.

   ”Proper evidentiary matter”, such as MapQuest Directions, will need to be submitted with the Employee Reimbursement Request form to the Auditor's Office.

4. Travel during on-duty hours must utilize the most direct route unless an alternate route would be less time consuming and/or more effective. During on-duty hours, employees shall not deviate from the route of travel or stop along the route of travel to conduct personal business or engage in any activity that is not within their assigned or required duties.

5. Reimbursement is authorized for parking charges, highway tolls, and other reasonable travel expenses directly related to the authorized travel.

6. Reimbursement for mileage and other travel by vehicle expenses associated with overnight travel is to be processed by the Auditor's Office rather than the employing agency's payroll department.

Exhibit 5

H. MEALS AND INCIDENTALS

1. Reimbursement for meals and incidentals is authorized only when overnight lodging is required while the employee is on official travel status (see Section D). The reimbursement of meals and incidentals is designed to offset the additional cost of travel, and not to entirely pay for the employee's meal and incidental expenses while on authorized travel status.

2. Reimbursement for meals and incidentals shall be made based on a $40 "per diem" or allowance for each full day of travel, which is considered reasonable.

3. Reimbursement for the first and last day that an employee is on authorized travel status will be $30, which is 75 percent of the full per diem amount.

4. The per-diem allowance cannot under any circumstances be used to pay for entertainment or alcoholic beverages, nor any tax or gratuity associated with such purchase.

5. Reimbursement for meals shall be made on the Employee Reimbursement Request form. Receipts are not required to be submitted to the Auditor's office for the employee to receive reimbursement, however a copy of the flight schedule, conference agenda, or other document demonstrating the dates of travel are required as proper evidentiary matter.

Exhibit 5

I. LODGING

1. Reimbursement for lodging shall be at the actual cost for the lowest available room rate. Every attempt should be made to reduce the cost of lodging, such as requesting the government rate, membership, or conference discounts, room sharing when appropriate, etc. Lodging accommodations should be appropriate for the proposed trip.

2. The maximum reimbursement for lodging to cities in the Continental United States is limited to the Federal per-diem rates listed on the U.S. General Services Administration (GSA) website (http://www.gsa.gov/perdiem) which is updated periodically. In addition, reimbursement is authorized for any associated hotel, lodging, or other taxes associated with the lodging.

3. Notwithstanding the limitation above, reimbursement may be authorized above the Federal per-diem lodging rates if the room is a) located at or proximate to the event site, or b) purchased through a travel agent, including reimbursement of any associated service fees. This does not preclude selection of an alternative location that would result in a lower cost of lodging to the County.

4. Approval is also given for direct payment to the lodging facility; an employee must present a bill from the facility in order to pay for the lodging in advance. Reimbursement to employees may also be made prior to the travel date if the employee has paid for the lodging in advance and can provide documentation to that effect.

5. Lodging costs will not be reimbursed when incurred at a lodging facility located within sixty-five (65) miles of the closer of either the employee's normal work location or official residence. Exceptions to this policy may be made in cases of severe inclement weather, or when the employee has provided a reasonable justification that is approved by the employee's supervisor at the time the travel is authorized.

Exhibit 5

J. TRANSPORTATION

1. Reimbursement is authorized for transportation expenses, such as public transportation, shuttle service, or taxi fares. Every attempt should be made to reduce the cost of transportation, such as sharing taxi fares when appropriate. Transportation expenses should be appropriate for the proposed trip.

2. Eligible transportation expenses authorized under this section include:

   a) Travel between the airport and the place of lodging, conference, or other event;

   b) Travel between the place of lodging and the conference or event when the conference or event is not on the same premises as the place of lodging;

   c) Travel between a business-related meeting and the place of lodging, conference, or other event;

3. The amount of reimbursement may include a tip or gratuity associated with the transportation expense, which is expected to be reasonable. A tip or gratuity of approximately 20% is generally accepted as reasonable, but may vary depending on the situation.

4. Each County agency, court, board, and/or commission shall be responsible for determining whether the transportation expenses submitted for reimbursement are reasonable and appropriate.

5. All receipts submitted for reimbursement under this section shall include the point of origin and the destination. For travel to or from a business-related meeting at a restaurant, the proper evidentiary matter submitted to the Auditor's office must include either an agenda or confirmation from the official of attendance at the meeting with the employee.

6. Reimbursement for rental cars is permissible when the out-of-county lodging is not proximate to the conference location, more economical than any other type of transportation, public transportation is not available, and transportation between facilities is not provided by the conference. Reimbursement shall not be made at the luxury or large vehicle rate (i.e., reimbursement shall be made for a compact, standard, or mid-size sedan), except that a large vehicle may be reimbursed if the number of travelers accommodated warrants a larger vehicle. The names of all persons traveling in the same rental vehicle shall be listed on the "Request for Authorization to Travel on County Business" form.

Exhibit 5

K. MISCELLANEOUS PROVISIONS

1. Reimbursement is authorized for other reasonable and business-related expenses, such as internet access at the place of lodging and telephone expenses, including one safety/arrival long distance phone call upon arrival at the destination (not to exceed two minutes). However, employees should make their best effort to minimize the expense by using calling cards or cell phones rather than using hotel room phone rates.

2. Since it is not possible to anticipate every travel potentiality that might arise, either before or during authorized travel, requests for reimbursements that vary from the above guidelines will be addressed on a case by case basis by the County Administrator or Deputy County Administrator. However, it is anticipated that such cases will be rare.