THIRD AMENDMENT TO THE AGREEMENT FOR BODY WORN CAMERA AND EVIDENCE MANAGEMENT SYSTEM BETWEEN THE CITY OF SAN JOSE AND AXON ENTERPRISE, INC.

This Third Amendment to the Agreement for Body Worn Camera and Evidence Management System between the City of San José (hereinafter "City"), a municipal corporation, and Axon Enterprise, Inc., formerly Taser International, Inc., a Delaware corporation authorized to do business in California (hereinafter "Contractor"), is entered into on the date of execution by City ("Effective Date"). Each of City and Contractor are sometimes hereinafter referred to as a "Party" and collectively as the "Parties."

RECITALS

WHEREAS, on June 24, 2016, City and Contractor entered into an agreement entitled "Agreement for Body Worn Camera and Evidence Management System between the City of San José and Taser International, Inc." ("Agreement") for the implementation of a Body Worn Camera and Evidence Management System for the San José Police Department; and

WHEREAS, on October 4, 2016, City entered into Change Order 1 to add additional subscription licenses and hardware, accelerate the deployment of body worn cameras, and increase the maximum amount of compensation to $4,551,929; and

WHEREAS, on April 5, 2017, Contractor officially changed its name to Axon Enterprise, Inc.; and

WHEREAS, on July 18, 2017, City and Contractor entered into Change Order 2 to add additional hardware at no additional cost; and

WHEREAS, on September 25, 2017, City and Contractor entered into Change Order 3 to add additional subscription licenses and hardware, and increase the maximum amount of compensation to $4,817, 684; and

WHEREAS, on June 12, 2018, City and Contractor entered into Change Order 4 to add additional hardware at no additional cost; and

WHEREAS, on June 19, 2018, City and Contractor entered into a First Amendment to the Agreement to add additional subscription licenses and hardware and increase the maximum amount of compensation to $5,196,697; and

WHEREAS, on November 17, 2018, City and Contractor entered into Change Order 5 to add additional hardware and increase the maximum amount of compensation to $5,203,964; and

WHEREAS, on February 1, 2021, City and Contractor entered into Change Order 6 to add additional licenses and data storage and increase the maximum amount of compensation to $5,272,564; and

WHEREAS, on June 18, 2021, City and Contractor entered into a Second Amendment to replace the five one-year option terms with one five-year option term through June 30, 2026;

WHEREAS, City and Contractor now desire to amend the amended Agreement to revise the title of the Agreement, add scope for the lease of portable automated license plate reader cameras, and add a five-year option term through June 30, 2031;

NOW, THEREFORE, the Parties agree to amend the Agreement as follows:

SECTION 1. Section 1 of the Agreement entitled "Agreement Documents" is amended to read as set forth below:

EXHIBIT A - Scope of Services
- Appendix 1 – Hardware and System Specifications
- Appendix 2 – Preliminary Project Schedule
- Appendix 3 – Evidence.com Plans
- Appendix 4 – Milestone and Deliverables Acceptance Form
- Appendix 5 – Final System Acceptance Certificate
- Appendix 6 – Price List

EXHIBIT B - Compensation/Payment Schedule
EXHIBIT C - Insurance Requirements
EXHIBIT D - Evidence.com Terms of Use
EXHIBIT E - Taser Assurance Plan
EXHIBIT F - Axon Integration Services
EXHIBIT G - Change Order Form
EXHIBIT H - Notice of Exercise of Option to Extend Agreement Form
EXHIBIT I - Taser Proposal Response (incorporated by reference)
EXHIBIT J - City of San José RFP #15-16-12 Body Worn Camera and Evidence Management System for the San José Police Department (incorporated by reference)
EXHIBIT K - Information Technology and Security Requirements
- Appendix 1 – Privacy and Disclosure Policy

EXHIBIT L - Axon Fleet Appendix
EXHIBIT M - Axon Application Programming Interface Appendix
EXHIBIT N - Axon Respond Appendix
EXHIBIT O - Axon Cloud Services Privacy Policy
EXHIBIT P - Supplemental Work Order Form

SECTION 2. Section 2.2 of the Agreement entitled "Options to Extend" is amended to read as set forth below:

2.1 Option to Extend

After the Initial Term, the City reserves the right, at its sole discretion, to extend the term of this Agreement for two five-year option terms through June 30, 2031 ("Option Period"), subject to the City's annual appropriation of funds.

SECTION 3. Section 31 of the Agreement entitled "Miscellaneous" is hereby amended to add Subsection 31.5 Entitled "Information Technology and Security Requirements" as set forth below:

31.5 Information Technology and Security Requirements

Contractor agrees to perform the work set forth in this Agreement in accordance with the City's Information Technology and Security Requirements, which are attached hereto as Exhibit K and incorporated herein.

31.5.1 Privacy and Disclosure Policy

Contractor agrees in the performance of the Services provided herein to comply with the City's Privacy and Disclosure Policy (the "Policy") as set forth in Exhibit K, Appendix 1, which is attached hereto and incorporated herein. Contractor shall ensure that all webpages that it creates are consistent with this Policy. Contractor further agrees that it shall treat all information received through this Agreement in strict accordance with the Policy.

SECTION 4. Exhibit A – Scope of Services, is amended as set forth in Addendum 1 to Exhibit A – Scope of Services, which is attached hereto and incorporated herein.

SECTION 5. Eighth Revised Exhibit A, Appendix 6, "Price List" is amended to read as set forth in Ninth Revised Exhibit A, Appendix 6, which is attached hereto and incorporated herein.

SECTION 6. Ninth Revised Exhibit B, "Compensation/Payment Schedule" is amended to read as set forth in Tenth Revised Exhibit B, which is attached hereto and incorporated herein.

SECTION 7. Exhibit C, "Insurance Requirements" is amended to read as set forth in Revised Exhibit C, which is attached hereto and incorporated herein.

SECTION 8. Exhibit K, "Information Technology and Security Requirements" is hereby added to the Agreement and is attached hereto and incorporated herein.

SECTION 9. Exhibit K, Appendix 1, "Privacy and Disclosure Policy" is hereby added to the Agreement and is attached hereto and incorporated herein.

SECTION 10. Exhibit L, "Axon Fleet Appendix" is hereby added to the Agreement and is attached hereto and incorporated herein.

SECTION 11. Exhibit M, "Axon Application Programming Interface Appendix" is hereby added to the Agreement and is attached hereto and incorporated herein.

SECTION 12. Exhibit N, "Axon Respond Appendix" is hereby added to the Agreement and is attached hereto and incorporated herein.

SECTION 13. Exhibit O, "Axon Cloud Services Privacy Policy" is hereby added to the Agreement and is attached hereto and incorporated herein.

SECTION 14. Exhibit P, "Supplemental Work Order Form" is hereby added to the Agreement and is attached hereto and incorporated herein.

SECTION 15. The title of the Agreement is hereby amended to read "Agreement for an Evidence Management Solution Including Related Hardware and Accessories."

SECTION 16. All terms and conditions of the Agreement not specifically modified by this Third Amendment shall remain in full force and effect.

WITNESS THE EXECUTION HEREOF on the day and year set forth beneath the respective name below.

City of San José,
a municipal corporation

Albie Udom
Email: albie.udom@sanjoseca.gov
Date: 03/14/2024 PDT

By_____
Albie Udom
Deputy Director of Finance and Chief Procurement Officer
Purchasing and Risk Management Division

Axon Enterprise, Inc.,
a Delaware corporation authorized to conduct business in California

Robert Driscoll
Email: bobby@axon.com
Date: 03/12/2024 PDT

By_____
Robert Driscoll
Deputy General Counsel

APPROVED AS TO FORM:

Diana Yuan
Email: diana.yuan@sanjoseca.gov
Date: 03/14/2024 PDT

Diana Yuan
Senior Deputy City Attorney

Isaiah Fields
Email: isaiah@axon.com
Date: 03/14/2024 PDT

By_____
Isaiah Fields
Chief Legal Officer

ADDENDUM 1 TO EXHIBIT A – SCOPE OF SERVICES

The following Scope of Services defines the principal activities and responsibilities of Contractor and the City for a Vehicle-Mounted Automatic License Plate Reader ("ALPR") Solution.

To the extent not inconsistent with the Agreement between the City and Contractor, City's RFP PUR-RFP2022.10.10129 (including all addenda and updates) issued on November 21, 2022, Contractor's proposal response dated January 3, 2023, and Contractor's Second Best and Final Offer (BAFO) response dated March 14, 2023 are incorporated herein by reference to provide context and supplemental information.

1 **General Requirements for Automatic License Plate Readers**

1.2 Contractor must assign a project manager to implement the Solution.

1.3 Solution must utilize Criminal Justice Information Services-compliant cloud storage and include unlimited storage for all ALPR camera footage and audio data for a period of at least one year.

1.4 All City data must be hosted and retained in the United States.

1.5 Contractor shall comply with all IT and Security Requirements as specified in Exhibit K – Information Technology and Security Requirements.

1.6 Software Requirements: Contractor's software (provided with the Solution) shall meet or exceed all requirements as specified below:

1.6.1 usable by City staff to search vehicle images to collect evidence that may be used in criminal investigations;

1.6.2 cloud-based, browser agnostic, software as a service compatible with the latest manufacturer-supported versions of Apple Safari, Google Chrome, Microsoft Edge, and Mozilla Firefox, at a minimum;

1.6.3 collects and processes footage captured from Contractor-provided ALPR cameras;

1.6.4 includes optical character recognition and image recognition for captured footage and allow for unlimited searches for whole or partial license plate numbers, vehicle make/model/type/color, and distinguishing characteristics (e.g., vehicle damage, window stickers, aftermarket wheels, etc.);

1.6.5 includes integration with the California Stolen Vehicle System and National Center for Missing and Exploited Children to receive AMBER Alerts;

1.6.6 provides the ability for users to create and manage custom hot lists of license plates associated with vehicles of interest for real-time detection and alerting;

1.6.7 provides the ability to share user created hot-lists, without footage and audio files, as-needed with other law enforcement agencies;

1.6.8 provides automatic alerting to selected users and/or user groups for real-time vehicle identification and system events (e.g., AMBER alerts, custom hot-list detection, etc.);

1.6.9 software must include custom reporting and auditing such as use and access by City users;

1.6.10 software must integrate with Axon's evidence.com to provide users the ability to transfer captured footage and any other relevant data from the Solution to evidence.com that may be used in criminal investigations (e.g., date/time, location, etc.) as-needed; and

1.6.11 must include a public-facing dashboard that details the applicable City policies and automatically updated metrics including number of ALPR reads by location and a San José specific map for visualization.

1.7 Training Requirements

1.7.1 Contractor shall work with the City to develop a mutually agreed upon training schedule. Training may be conducted virtually or in-person at San José Police Department facilities.

1.7.2 Contractor must provide City-specific training curriculum, manuals, and documentation for all training in electronic format for City's review and acceptance.

1.7.3 Contractor must allow or provide, in a format pre-approved by the City, recordings of training sessions at no additional cost to the City.

1.7.4 Contractor's training must include both user and administrator training, including, but not limited to, security settings, system set-up/configuration, and use of all product features.

1.8 Maintenance and Support:

1.8.1 Contractor must provide support and maintenance on all provided software and hardware throughout the term of the Agreement which includes all on-site maintenance, routine servicing, repairs as required, and full replacement as necessary.

1.8.2 Contractor must maintain a website that provides 24x7x365 access to technical information and software patches.

1.8.3 Contractor must have an online trouble reporting system that tracks open trouble tickets and includes automatic escalation and notification based on service level requirements and issue progress.

1.8.4 Contractor must provide technical support 24x7x365 by phone, email, and online portal.

1.8.5 Technical support must include unlimited incidents.

1.8.6 Technical support shall be provided in accordance with the following service levels:

Severity Level	Definition	Maximum Response Time	Target Resolution Time
1	• System down. • Operations have been severely disrupted. • No work around available.	15 minutes	2 hours
2	• Major functionality is severely impaired. • A temporary work around is available. • Operations can continue in a restricted fashion, although long-term productivity may be adversely affected. • Persistent service degradation (i.e., unacceptably slow response times).	1 hours	4 hours
3	• Partial, non-critical loss of functionality. • Problem causing minor loss of features/functionality. • Impaired operations of some components, but still usable. • A temporary workaround is available.	4 hours	24 hours

1.8.7 Contractor must provide guaranteed minimum 99.99% uptime for the Solution, excluding scheduled maintenance.

1.8.8 Contractor must pay penalties to the City, such as service credits, liquidated damages, etc., for any failure to meet these Service Levels and minimum uptime.

1.8.9 Solution updates must be supported for the term of the Agreement and are included as part of maintenance and support.

1.8.10 Contractor must notify the City at least five business days in advance of deploying any potentially service-impacting modifications (excluding emergency patches/fixes) and at least 15 business days in advance of its intent to release any major improvements or Solution enhancements, including a description of the intended enhancements or improvements.

1.8.11 Contractor must provide 24x7x395 remote monitoring of the Solution and must proactively alert the City of issues.

2 Vehicle-Mounted ALPR Specific Requirements

In addition to the General Requirements specified in Section 1, the following additional requirements are specific to the Vehicle-Mounted ALPR Solution:

2.1 The City shall lease Vehicle-Mounted ALPR Solution hardware.

2.2 During initial implementation, Contractor shall provide and install Vehicle-Mounted ALPR cameras on designated City-owned vehicles.

2.3 After implementation, Contractor shall provide documentation and training as necessary to ensure City staff has the knowledge and ability to install ALPR cameras.

2.4 Vehicle-Mounted ALPR cameras must be able to simultaneously capture footage in front of and behind the vehicle they are mounted to.

2.5 Vehicle-Mounted ALPR cameras must capture clear, full color images of vehicles traveling up to 100 miles per hour in variable lighting and weather conditions, including nighttime.

2.6 Each Vehicle-Mounted ALPR camera must upload captured footage to Contractor's software in real-time.

NINTH REVISED EXHIBIT A, APPENDIX 6 – PRICE LIST

This Ninth Revised Exhibit A, Appendix 6 – Price List supersedes and replaces Seventh Revised Exhibit A, Appendix 6 – Price List as previously amended and restated by the Second Amendment to the Agreement.

A. INITIAL TERM PRICING (7/1/2016 – 6/30/2021)

Description of Cost Elements	Qty	Year 1 (7/1/16 – 6/30/17)	Year 2 (7/1/17 – 6/30/18)	Year 3 (7/1/18 – 6/30/19)	Year 4 (7/1/19 – 6/30/20)	Year 5 (7/1/120 – 6/30/21)
SECTION A: SYSTEM IMPLEMENTATION						
1. Professional Services for Implementation:		$15,000				
- Implementation						
- CAD Integration						
- Training						
- Testing & Final Acceptance						
- Go- Live						
2. Accelerated Deployment (Change Order 1)		27,530				
3. Additional Axon Clip Mounts (Change Order 1)	247	3,107.26				
4. Additional Molle Mounts (Change Order 1)	164	3,291.48				
TOTAL (Section A)	**411**	**$48,929**				

SECTION B: ONGOING SERVICES						
1. Software License/SaaS Subscription – Evidence.com Unlimited License – Evidence.com CAD/RMS Integration License	963	$761,244	$912,924	$912,924	$912,924	$912,924
Additional quantity (Change Order 1)	20	14,220	18,960	18,960	18,960	18,960
Additional quantity (Change Order 3)	74		52,614	70,152	70,152	70,152
Additional quantity (Amendment 1)	143		4,345	102,700	135,564	135,564
Subtotal (Subsection B.1)	**1,300**	**$775,464**	**$988,843**	**$1,104,736**	**$1,137,600**	**$1,137,600**
2. Evidence.com Standard	43	Included	Included	Included	Included	Included
Additional quantity (Change Order 1)	20	Included	Included	Included	Included	Included
Additional quantity	100					10,500

Description of Cost Elements	Qty	Year 1 (7/1/16 – 6/30/17)	Year 2 (7/1/17 – 6/30/18)	Year 3 (7/1/18 – 6/30/19)	Year 4 (7/1/19 – 6/30/20)	Year 5 (7/1/120 – 6/30/21)
(Change Order 6)						
Subtotal (Subsection B.2)	**163**	**Included**	**Included**	**Included**	**Included**	**Included**
3. Evidence.com Pro	40	Included	Included	Included	Included	Included
Subtotal (Subsection B.3)	**40**	**Included**	**Included**	**Included**	**Included**	**Included**
4. Unlimited Axon Video and Capture Storage	963	Included	Included	Included	Included	Included
Additional quantity (Change Order 1)	20	Included	Included	Included	Included	Included
Additional quantity (Change Order 3)	74	Included	Included	Included	Included	Included
Additional quantity (Amendment 1)	143	Included	Included	Included	Included	Included
Subtotal (Subsection B.4)	**1,200**	**Included**	**Included**	**Included**	**Included**	**Included**
5. Disaster Recovery		Included	Included	Included	Included	Included
Subtotal (Subsection B.5)		Included	Included	Included	Included	Included
6. Taser Assurance Plan	963	Included	Included	Included	Included	Included
Additional quantity (Change Order 1)	20	Included	Included	Included	Included	Included
Additional quantity (Change Order 2)	59		Included	Included	Included	Included
Additional quantity (Change Order 3)	79		Included	Included	Included	Included
Additional quantity (Change Order 4)	90		Included	Included	Included	Included
Additional quantity (Amendment 1)	143		Included	Included	Included	Included
Subtotal (Subsection B.6)	**1,354**	**Included**	**Included**	**Included**	**Included**	**Included**
7. Redaction Assistant Agency-wide License	1					$58,100
Subtotal (Subsection B.7)	1					**$58,100**
TOTAL (Section B)	**2,758**	**$775,464**	**$988,843**	**$1,104,736**	**$1,137,600**	**$1,206,200**

SECTION C: BODY WORN CAMERAS/DOCKING STATIONS						
1. Body Worn Camera	963	Included	Included	Included	Included	Included
Additional quantity (Change Order 1)	20	Included	Included	Included	Included	Included
Additional quantity (Change Order 2) (does not require purchase of additional Evidence.com Unlimited license)	59	Included	Included	Included	Included	Included

Description of Cost Elements	Qty	Year 1 (7/1/16 – 6/30/17)	Year 2 (7/1/17 – 6/30/18)	Year 3 (7/1/18 – 6/30/19)	Year 4 (7/1/19 – 6/30/20)	Year 5 (7/1/120 – 6/30/21)
Additional quantity (Change Order 3)	74	Included	Included	Included	Included	Included
Additional quantity (Change Order 3) (spare cameras; does not require purchase of additional Evidence.com Unlimited license)	5	Included	Included	Included	Included	Included
Additional quantity (Change Order 4) (does not require purchase of additional Evidence.com Unlimited)	90	Included	Included	Included	Included	Included
Additional quantity (Amendment 1)	143	Included	Included	Included	Included	Included
Subtotal (Subsection C.1)	**1,354**	**Included**	**Included**	**Included**	**Included**	**Included**
2. Docking Station	983	Included	Included	Included	Included	Included
Additional quantity (Change Order 4)	15	Included	Included	Included	Included	Included
Subtotal (Subsection C.2)	**998**	**Included**	**Included**	**Included**	**Included**	**Included**
TOTAL (Section C)	**4704**	$0	$0	$0	$0	$0

SECTION D: OTHER ITEMS						
- Additional order (Change Order 2) - (Axon Rapidlock Mounts, Cables, etc.)			$0			
Additional order (Change Order 3) (Axon Rapidlock Mounts, Cables, Wall Mount Brackets, Axon Starter, etc.)			2,685			
Additional order (Change Order 4) (Axon Rapidlock Mounts, Cables, Wall Mount Brackets, etc.)			Included			
Additional order (Amendment 1) (Wall mount brackets)			350	490		
Additional order (Change Order 4) (Axon Rapidlock Mounts, Cables, Wall Mount Brackets, etc.)			Included	Included	Included	Included
Additional order (Change Order 5)				7,267		

Description of Cost Elements	Qty	Year 1 (7/1/16 – 6/30/17)	Year 2 (7/1/17 – 6/30/18)	Year 3 (7/1/18 – 6/30/19)	Year 4 (7/1/19 – 6/30/20)	Year 5 (7/1/120 – 6/30/21)
(Wall Mount Bracket, Dock 2 Annual Plan, Molle Mount, Belt Clip, Powercord, etc.)						
Additional order (Change Order 6) (10 GB Evidence.com a-la-cart Storage)	100					Included
TOTAL (Section D)	**100**	**$0**	**$3,035**	**$7,757**	**$0**	**$0**

TOTAL FOR INITIAL TERM (Sections A – D)	**7,973**	**$824,393**	**$991,878**	**$1,112,493**	**$1,137,600**	**$1,206,200**

B. 5-YEAR OPTION 1 PRICING (7/1/2021 – 6/30/2026)
(Revised this 3rd Amendment)

Description of Cost Elements	Qty	Year 6 (7/1/21-6/30/22)	Year 7 (7/1/22-6/30/23)	Year 8 (7/1/23-6/30/24)	Year 9 (7/1/24-6/30/25)	Year 10 (7/1/25-6/30/26)
1. Evidence.com unlimited Axon device storage	1,200	$325,680	$325,680	$325,680	$325,680	$325,680
2. 10 GB evidence.com a-la-cart storage	11,823	32,035	32,035	32,035	32,035	32,035
3. Evidence.com license (Professional)	1,283	525,900	525,900	525,900	525,900	525,900
4. Evidence.com license (Basic)	100	18,000	18,000	18,000	18,000	18,000
5. Redaction assistant user access license	1,200	99,600	99,600	99,600	99,600	99,600
6. Auto tagging license	1,200	Included	Included	Included	Included	Included
7. Performance license	1,200	129,600	23,748	23,748	23,748	23,748
8. Tech assurance plan body 3 camera	1,259	47,562	169,615	169,615	169,615	169,615
9. Tech assurance plan 8-bay body 3 dock	139	50,952	50,952	50,952	50,952	50,952
10. Transferred Warranty AB3 Camera	59	Included	Included	Included	Included	Included
11. Transferred AB3 camera tap warranty	1,200	Included	Included	Included	Included	Included
12. Transferred AB3 multi-bay dock tap warranty	139	Included	Included	Included	Included	Included
13. Auto tagging license	1,200	Included	Included	Included	Included	Included
14. ALPR Camera, including all hardware and installation (Added this 3rd Amendment)	**20**	**n/a**	**n/a**	**28,124***	**28,124***	**28,124***
15. ALPR Maintenance and Support (Added this 3rd Amendment)	**20**	**n/a**	**n/a**	**18,557***	**18,557***	**18,557***
16. ALPR Software Subscription including Maintenance and Support and Unlimited data storage (Added this 3rd Amendment)	**1,500**	**n/a**	**n/a**	**Included**	**Included**	**Included**
Estimated Taxes		9,112	20,402	24,486	24,486	24,486
5-YEAR OPTION TERM ESTIMATED MAXIMUM COMPENSATION		**$1,238,441**	**$1,265,932**	**$1,316,697**	**$1,316,697**	**$1,316,697**

*Invoicing pursuant to vendor quote #Q-508510-45301.847RH which is attached hereto and incorporated herein.

C. 5-YEAR OPTION 2 PRICING (7/1/2026 – 6/30/2031)
(Added this 3rd Amendment)

Description of Cost Elements	Qty	Year 11 (7/1/26-6/30/27)	Year 12 (7/1/27-6/30/28)	Year 13 (7/1/28-6/30/29)	Year 14 (7/1/29-6/30/30)	Year 15 (7/1/30-6/30/31)
1. Software License/SaaS Subscription	1,200	$989,649	$1,019,338	$1,049,918	$1,081,415	$1,113,858
2. Evidence.com unlimited Axon device storage – Included with SaaS Subscription	1,200	Included	Included	Included	Included	Included
3. 10 GB evidence.com a-la-cart storage – Included with SaaS Subscription	11,823	Included	Included	Included	Included	Included
4. Evidence.com license (Professional) – Included with SaaS Subscription	1,200	Included	Included	Included	Included	Included
5. Evidence.com license (Professional) – additional non-BWC users	83	42,081	43,343	44,643	45,982	47,361
6. Evidence.com license (Basic)	100	20,160	20,765	21,388	22,030	22,691
7. Redaction assistant user access license	1,200	111,552	114,899	118,346	121,896	125,553
8. Auto tagging license	1,200	Included	Included	Included	Included	Included
9. Performance license	1,200	145,152	149,507	153,992	158,612	163,370
10. Tech assurance plan body 3 camera	59	189,969	195,668	201,538	207,584	213,812
11. Tech assurance plan 8-bay body 3 dock	139	57,066	58,778	60,541	62,357	64,228
12. Transferred Warranty AB3 Camera	59	Included	Included	Included	Included	Included
13. Transferred AB3 camera tap warranty	1,200	Included	Included	Included	Included	Included
14. Transferred AB3 multi-bay dock tap warranty	139	Included	Included	Included	Included	Included
15. Fleet 3 ALPR Purchased Camera, including all hardware and installation	20	29,837	30,732	31,654	32,604	33,582
16. Fleet 3 ALPR Purchased Hardware Maintenance and Support	20	19,687	20,278	20,886	21,513	22,158
17. ALPR Software Subscription including Maintenance and Support and Unlimited data storage	1,500	Included	Included	Included	Included	Included

Description of Cost Elements	Qty	Year 11 (7/1/26-6/30/27)	Year 12 (7/1/27-6/30/28)	Year 13 (7/1/28-6/30/29)	Year 14 (7/1/29-6/30/30)	Year 15 (7/1/30-6/30/31)
Estimated Taxes		26,641	27,440	28,263	29,111	29,984
5-YEAR OPTION TERM ESTIMATED MAXIMUM COMPENSATION		**$1,513,240**	**$1,558,637**	**$1,605,395**	**$1,653,557**	**$1,703,164**

Axon Enterprise, Inc.
17800 N 85th St.
Scottsdale, Arizona 85255
United States
VAT: 86-0741227
Domestic: (800) 978-2737
International: +1.800.978.2737

Q-508510-45301.847RH

Issued: 01/10/2024

Quote Expiration: 02/15/2024

Estimated Contract Start Date: 04/15/2024

Account Number: 107592

Payment Terms: N30

Delivery Method:

SHIP TO	BILL TO
San Jose Police Dept. 201 W Mission St San Jose, CA 95110-1701 USA	San Jose Police Dept. - CA 201 W Mission St San Jose CA 95110-1701 USA Email:

SALES REPRESENTATIVE	PRIMARY CONTACT
Megan Hardisty Phone: +1 4802537854 Email: mhardisty@axon.com Fax:	Judith Torrico Phone: 4088349911 Email: judith.torrico@sanjoseca.gov Fax:

Quote Summary

Program Length	27 Months
TOTAL COST	$140,039.60
ESTIMATED TOTAL W/ TAX	$145,757.54

Discount Summary

Average Savings Per Year	$46,365.24
TOTAL SAVINGS	$104,321.80

Payment Summary

Date	Subtotal	Tax	Total
Mar 2023	$20,502.00	$0.00	$20,502.00
Mar 2024	$26,176.12	$1,905.84	$28,081.96
Jun 2024	$46,680.74	$1,906.04	$48,586.78
Jun 2025	$46,680.74	$1,906.06	$48,586.80
Total	**$140,039.60**	**$5,717.94**	**$145,757.54**

Quote Unbundled Price:	$244,361.40
Quote List Price:	$165,829.20
Quote Subtotal:	$140,039.60

Pricing

All deliverables are detailed in Delivery Schedules section lower in proposal

Item	Description	Qty	Term	Unbundled	List Price	Net Price	Subtotal	Tax	Total
Program									
80460	TRUE UP - FLEET 3 BUNDLE TRUE UP	20	27		$78.00	$23.38	$12,623.60	$1,183.47	$13,807.07
Fleet3B	Fleet 3 Basic	20	27	$300.47	$155.04	$168.41	$90,941.40	$4,534.47	$95,475.87
A la Carte Software									
80401	AXON FLEET 3 - ALPR LICENSE - 1 CAMERA	20	27		$62.94	$67.55	$36,474.60	$0.00	$36,474.60
A la Carte Services									
100159	AXON FLEET 3 - SERVICES - ALPR API INTEGRATION	2			$3,000.00	$0.00	$0.00	$0.00	$0.00
Total							**$140,039.60**	**$5,717.94**	**$145,757.54**

Jun 2025						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Total				$46,680.74	$1,906.06	$48,586.80

TENTH REVISED EXHIBIT B – COMPENSATION / PAYMENT SCHEDULE

This Tenth Revised Exhibit B – Compensation/Payment Schedule supersedes and replaces Tenth Revised Exhibit B – Compensation/Payment Schedule as previously amended and restated by the Second Amendment to the Agreement

1 Compensation

1.1 The maximum amount payable for all products and services provided under this Agreement shall not exceed **Five Million Two Hundred Seventy-Two Thousand Five Hundred Sixty-Four Dollars ($5,272,564)** during the initial five-year term. Any additional services requested by the City that would exceed the preceding maximum amount will be addressed in accordance with the Change Order Procedures. No additional services will be performed unless both parties execute a Change Order outlining the services requested and the compensation agreed for such services.

1.2 Progress payments shall be made to Contractor by City based on net 30 days payment terms, following receipt of invoices that may be issued after acceptance of designated milestones as shown below in Table B1-Payment Schedule. All payments are based upon City's acceptance of Contractor's performance as evidenced by successful completion of all of the deliverables as set forth for each milestone. City shall have no obligation to pay unless Contractor has successfully completed and City has approved the Milestone for which payment is due.

1.3 Payment for any part or parts of the System provided hereunder, or inspection or testing thereof by City, shall not constitute acceptance or relieve Contractor of its obligations under this Agreement. City may inspect the components of the System when delivered and reject upon notification to Contractor any and all the System, which does not conform to the Specifications or other requirements of this Agreement. Components of the System, which are rejected shall be promptly corrected, repaired or replaced by Contractor. If City receives components of the System with defects or nonconformities not reasonably apparent on inspection, then City reserves the right to require prompt correction, repair or replacement by Contractor in accordance with Contractor's warranty obligations.

2 Project Performance & Payment Schedule

2.1 Work shall commence immediately upon execution of the Agreement.

2.2 Invoicing procedure: The City agrees to compensate Contractor for the Services performed in accordance with the terms and conditions of this Agreement. Contractor shall send invoices to the City according to Table B1 listed below. The actual dates of completion for each milestone may vary from the estimated completion date indicated in Table B1 and the Preliminary Project Schedule (Exhibit A-1, Appendix 2). Milestone completion date may be updated and revised as mutually agreed upon between City and Contractor. Payment shall be made based on City acceptance of milestones and SOS deliverables.

2.3 For ongoing cloud subscription and storage services after the implementation period (see Table B2), City shall prepay for the Services provided under this Agreement at the beginning of each annual renewal. In the event of early termination of the Agreement, Contractor shall refund the City any fees not expended and paid in advance on a prorated basis.

2.4 Contractor shall submit invoices to designated SJPD contact.

Table B1: Compensation/Payment Schedule (Initial Term)

Milestone/Item	Scope of Services Deliverables (Exhibit A-1)	Estimated Completion Date	Payment Amount	% of Year 1 Total
A. YEAR 1 IMPLEMENTATION:				
1. Phase 1- Project Planning, Implementation, Training & Go-Live (approximately 387 cameras)	Section 9	8/2/16	$249,559	30.3%
2. Phase 2- Implementation, Training & Go-Live (approximately 192 cameras)	Section 10.1-10.4	8/25/16	123,812	15%
3. Accelerated Deployment	Change Order 1	9/28/16	27,530	3.3%
4. Phase 3- Implementation, Training & Go-Live (approximately 192 cameras)	Section 10.1-10.4	9/28/16	123,812	15%
5. Phase 4- Implementation & Training (approximately 192 cameras)	Section 10.1-10.5	10/26/16	123,812	15%
6. Additional Cameras	Change Order 1	10/26/16	14,220	1.7%
7. Additional Axon Clip Mounts	Change Order 1	10/26/16	3,107.26	.38%
8. Additional Molle Mounts	Change Order 1	10/26/16	3,291.48	.4%
9. Final Go-Live	Section 10.4.1-10.4.2	10/27/16	77,624	9.4%
10. Post Go-Live and Final System Acceptance	Section 10.4.4-10.4.5	12/11/16	77,625	9.4%
Total Year 1 (initial license, installation, setup)			$824,393	**100%**
B. ONGOING SERVICES			**Payment Amount**	
Year 2 (cloud subscription & storage services)			$988,843	
Year 3 (cloud subscription & storage services)			1,104,736	
Year 4 (cloud subscription & storage services)			1,137,600	
Year 5 (cloud subscription & storage services)			1,206,200	
Year 6 (cloud subscription & storage services**)			1,139,927	
Year 7 (cloud subscription & storage services**)			1,045,366	
Year 8 (cloud subscription & storage services**)			1,045,366	
Year 9 (cloud subscription & storage services**)			1,045,366	
Year 10 (cloud subscription & storage services**)			1,045,366	
Total Ongoing Services			$9,758,770	
C. ONE TIME PURCHASES			**Payment Amount**	
Change Order 2	See Second Revised Exhibit A, Appendix 6	8/31/17	$0	
Change Order 3	See Third Revised Exhibit A, Appendix 6	8/31/17	2,685	
Change Order 4	See Fourth Revised Exhibit A, Appendix 6	7/15/18	0	
Amendment 1	See Fifth Revised Exhibit A, Appendix 6	10/31/19	840	
Change Order 5	See Sixth Revised Exhibit A, Appendix 6	12/1/18	7,267	
Year 6 (Hardware)	See Eighth Revised Exhibit A, Appendix 6	7/1/2021	98,513	
Year 7 (Hardware)	See Eighth Revised Exhibit A, Appendix 6	7/1/2022	220,567	
Year 8 (Hardware)	See Eighth Revised Exhibit A, Appendix 6	7/1/2023	220,567	
Year 9 (Hardware)	See Eighth Revised Exhibit A, Appendix 6	7/1/2024	220,567	
Year 10 (Hardware)	See Eighth Revised Exhibit A, Appendix 6	7/1/2025	220,567	
Total Additional Purchases			$991,573	
MAXIMUM COMPENSATION			**$11,574,736**	

*All amounts stated above are in United States Currency.

**Includes applicable taxes.

Table B2: Compensation/Payment Schedule (5-Year Option 1 Term)

Option Description	Payment Due By	Estimated Payment Amount
Year 1 of 5-Year Option Term (7/1/21 – 6/30/22)	7/1/21	$1,238,441
Year 2 of 5-Year Option Term (7/1/22 – 6/30/23)	7/1/22	1,265,933
Year 3 of 5-Year Option Term (7/1/23 – 6/30/24) **(Revised this 3rd Amendment)**	7/1/23	1,316,697
Year 4 of 5-Year Option Term (7/1/24 – 6/30/25) **(Revised this 3rd Amendment)**	7/1/24	1,316,697
Year 5 of 5-Year Option Term (7/1/25 – 6/30/26) **(Revised this 3rd Amendment)**	7/1/25	1,316,697
ESTIMATED MAXIMUM COMPENSATION FOR 5-YEAR OPTION 1 TERM		**$6,454,465**

3 **Renewal Period Compensation (Revised this 3rd Amendment)**

City shall provide Contractor prior written notice in the form of Exhibit H of its intention to exercise its option for the next term prior to the end of the then current term. Rates for the next option term will be based on on Tables B and C of the Ninth Revised Exhibit A, Appendix 6 – Price List. The City's Director of Finance or designee is authorized to exercise options on behalf of the City.

4 **Additional Purchases (Revised this 3rd Amendment)**

4.1 Should the City require additional subscription licenses, Contractor shall provide them at the per unit rates currently billed at the time of the request based on Tables B and C of the Ninth Revised Exhibit A, Appendix 6 – Price List.

4.2 Should the City require additional On-site training, Contractor shall provide the training at a rate of $2,000 per day.

4.3 Should the City require additional storage (data not uploaded from Axon body worn cameras), Contractor shall provide the storage at a rate of $45,000 per year for 60 TB.

4.4 The City reserves the right to make additional purchases for next generation equivalents and products/services not otherwise listed, including warranty, support, and maintenance, at the rates provided below:

4.4.1 Next generation items shall be provided at no less than 4% off of the list price for the associated SKU.

4.4.2 Body Camera Bundle Plans not listed (including where hardware/software are bundled together) - 5% off the total current list price at the time of purchase for the associated SKU.

4.4.3 Other Hardware not listed - 4% off of the total current list price at the time of purchase for the associated SKU.

4.4.4 Other Software moduals/add-ons not listed - 4% off of the total current list price at the time of purchase for the associated SKU.

4.5 Quotes must be approved by the City through an executed Supplemental Work Order Form (Exhibit F).

REVISED EXHIBIT C – INSURANCE REQUIREMENTS

This Revised Exhibit C – Insurance Requirements supersedes and replaces Exhibit C – Insurance Requirements.

Contractor, at Contractor's sole cost and expense, shall procure and maintain for the duration of this Agreement, insurance against claims for injuries to persons or damages to property which may arise from, or in connection with, the performance of the services hereunder by Contractor, its agents, representatives, employees or subcontractors or suppliers.

I. Minimum Scope and Limit of Insurance

There shall be no endorsements reducing the scope of coverage required below unless approved by the City's Risk Manager.

Type of Insurance	Minimum Limit
1 Commercial General Liability The coverage provided by Insurance Services Office "occurrence" form CG 0001, including coverages for contractual liability, personal injury/advertising injury, products/completed operations, broad form property damage, independent contractors, products and completed operations.	$1,000,000 per occurrence for bodily injury, personal injury and property damage or $2,000,000 annual aggregate.
2 Automobile Liability The coverage provided by Insurance Services Office form number CA 0001. Coverage shall be included for all owned, non-owned and hired automobiles.	$1,000,000 combined single limit per accident for bodily injury and property damage.
3 Workers' Compensation and Employer Liability A: Workers Compensation as required by Statute and as required by the Labor Code of the State of California. B: Employers' Liability	Coverage A: Statutory Coverage B: $1,000,000 each accident/ each employee injury by disease
4 Technology Errors and Omissions Including coverages for negligent acts, errors, or omissions arising from professional services provided under this contract.	Not less than $2,000,000 each claim and annual aggregate.
5 Cyber Liability Data recovery and privacy liability insurance covering liabilities for financial loss resulting or arising from acts, errors, or omissions, in rendering products provided under this agreement. This may be met through a standalone policy or included as a component in a Commercial General Liability Policy.	Not less than $5,000,000 each claim and annual aggregate.

Any limits requirement may be met with any combination of primary and excess coverage so long as

the excess coverage is written on a "follow form" or umbrella basis.

II. Deductibles and Self-Insured Retentions

Any deductibles or self-insured retentions must be declared to the City's Risk Manager.

III. Other Insurance Provisions

The policies are to contain, or be endorsed to contain, the following provisions:

1. General Liability and Automobile Liability Coverages

a. The City, its officials, employees, and agents are to be covered as additional insureds as respects: liability arising out of activities performed by, or on behalf of, Contractor; products and completed operations of Contractor; premises owned, leased or used by Contractor; or automobiles owned, leased, hired or borrowed by Contractor. The coverage shall contain no special limitations on the scope of protection afforded to the City, its officials, employees, and agents.

b. Contractor's insurance coverage shall be primary insurance as respects the City, its officials, employees, and agents. Any insurance or self-insurance maintained by the City, its officials, employees, and agents shall be excess of Contractor's insurance and shall not contribute with it.

c. Any failure to comply with reporting provisions of the policies shall not affect coverage provided to the City, its officials, employees, or agents.

d. Coverage shall state that Contractor's insurance shall apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of the insurer's liability.

e. Coverage shall contain a waiver of subrogation in favor of the City, its officials, employees, and agents.

2. Workers' Compensation and Employers Liability

Coverage shall be endorsed to state carrier waives its rights of subrogation against the City, its officials, and agents.

3. Claims Made Coverages

If coverage is obtained on a "claims made" policy form, the retroactive date shall preceed the date services were initiated with the City and the coverage shall be maintained for a periof of 3 years after termination of services under this Agreement.

4. All Coverages

Each insurance policy required by this clause shall be endorsed to state that coverage shall not be suspended, voided, canceled, reduced in coverage or in limits except after

30 days' prior written notice has been given to the City; except that 10 days' prior written notice shall apply in the event of cancellation for non-payment of premium.

IV. Acceptability of Insurance

Insurance is to be placed with insurers acceptable to the City's Risk Manager.

V. Verification of Coverage

Contractor shall furnish the City with certificates of insurance and with endorsements affecting coverage required by this clause. The certificates and endorsements for each insurance policy are to be signed by a person authorized by that insurer to bind coverage on its behalf.

Copies of all the required ENDORSEMENTS shall be attached to the CERTIFICATE OF INSURANCE which shall be provided by Contractor's insurance company as evidence of the stipulated coverages.

Proof of insurance shall be emailed in pdf format to: Riskmgmt@sanjoseca.gov:

Certificate Holder
City of San José – Finance Department
Risk & Insurance
200 East Santa Clara St., 14th Floor
San José, CA 95113-1905

VI. Subcontractors

Contractor shall include all subcontractors as insureds under its policies or shall obtain separate certificates and endorsements for each subcontractor.

EXHIBIT K - INFORMATION TECHNOLOGY AND SECURITY REQUIREMENTS

The requirements below define additional City Information Technology and Security Requirements as they pertain to this Agreement. Contractor shall comply with the following requirements in providing all Information Technology-related software, services, and equipment.

1 Privacy and Disclosure

Contractor shall in the performance of services provided under this Agreement comply with City's Privacy and Disclosure Policy, Appendix 1 – Privacy and Disclosure Policy.

2 Security Requirements

2.2 Privileged Information

Contractor shall provide any and all SOC2 reports under privileged access, or a similar level of protection, in order to guard against revealing potential security issues that put the City, citizens, and businesses at risk.

2.3 Secure Transmission

Contractor shall provide any and all information systems security findings, recommendations, and work materials via a secure file transfer method accessible by the City.

2.4 Secure Access

Contractor shall have all equipment, materials, and support necessary to remotely connect to the City servers and computers via a secure connection per City access protocols. The City will provide secure VPN access into the network to the Contractor as required. On-site access will also be provided as needed and as mutually agreed by the parties.

2.5 Security Policy and Standards

Contractor shall adhere to the City's *Information and System Security Policy* and *Information Security Standard Handbook* or any other similar standard such as NIST SP800-53, ISO 27001, CIS, or COBIT, in providing the services.

2.6 Security Controls

Contractor shall implement security controls in accordance with the City's Security Policy and Standards or any other acceptable standard to assess any solution prior to first release or release of any major improvement or enhancement. Contractor's solution must be audited by a third party at least once a year and results shall be share with City along with regular updates on risk mitigation.

2.7 Limited Access

If necessary for the fulfillment of the Agreement, City may provide Contractor with non-exclusive, limited access to the City's information technology infrastructure. Contractor shall abide by all City policies, standards, regulations, and restrictions regarding access and usage of City's information and communication technology resources. Contractor shall enforce all such policies, standards, regulations, and restrictions with all Contractor's employees, agents, and any tier of subcontractor granted access in the performance of this

Agreement and shall only grant such access as may be necessary for the purpose of fulfilling the requirements of this Agreement.

2.8 Incident Response

Contractor shall develop and maintain an incident response plan and contacts for providing notification, containing, eradicating, and recovering from a significant incident that impacts the operations of the City or the services the Contractor provides. The City may request a copy and/or verbal explanation of the Contractor's incident response plan, and the Contractor must provide the requested materials/explanations within 30 days or request an extension in writing from the City.

2.9 Compromised Security

In the event that Data collected or obtained by the Contractor in connection with this Agreement is believed to have been compromised, lost, accessed by an unauthorized party, or otherwise breached as defined by NIST as a "data breach" (collectively "Data Breach"), Contractor shall notify the City immediately. Contractor shall investigate their systems of any suspected Data Breach in accordance with Contractor's incident response plan and report findings to the City.

Contractor agrees to reimburse the City for any costs the City incurs to resolve potential breaches incurred due to the Contractor, including, where applicable, the cost of identifying and assisting individuals who may be impacted by the Contractor's breach, legal fees and fines associated with the data breach, and legal requirements issued by a local, state, or federal court.

2.10 Contingency Planning

Contractor shall develop and maintain a contingency plan for providing resiliency and redundancy to the Solution.

2.11 Enclave Security

Contractor managing a Local Area Network, Wide Area Network, Infrastructure As A Service, or Platform As A Service on behalf of the City shall implement/integrate the Enclave with existing City security technology including, but not limited to, the following as applicable and as may be updated from time to time:

- 2.11.1 Firewalls (Check Point)
- 2.11.2 Security Operations Center (NuHarbor)
- 2.11.3 Log Consolidation and Reduction (Cribl)
- 2.11.4 Security Incident and Event Monitoring (Splunk)
- 2.11.5 Server Advanced Protection (Microsoft MDE)
- 2.11.6 Endpoint protection (Microsoft MDE)
- 2.11.7 Incident Response (IR Plan)
- 2.11.8 Disaster Recovery Plan (DR Plan)
- 2.11.9 Emergency Operations Center

EXHIBIT K, APPENDIX 1 - PRIVACY AND DISCLOSURE POLICY

The purpose of this document is to define the City of San José's policy and the requirements of its Contractors with regard to the collection and use of personally identifiable information (PII) collected, processed, or otherwise used in the course doing business with the City. Non-PII (i.e., anonymous information) and PII are defined below, followed by the requirements for City contracts where PII is used in the course of doing business with the City.

1 Anonymous Information

This type of information does not identify specific individuals and is automatically transmitted and consists of:

- The URL (Uniform Resource Locator or address) of the web page a user previously visited.
- Unique "session IDs" randomly assigned to a user when accessing City WiFi. These IDs do not connect to the IP address (i.e., digital PII) of the device used to access the Internet and are randomly generated each time an individual logs on to City WiFi.
- The browser version users are using to access the site.

This information is used to help improve the City's systems, and none of the information can be linked to an individual.

2 Personally Identifiable Information (PII)

Personally identifiable information (PII) includes any information that can directly or indirectly identify an individual, such as one's name or address. Refer to the table below for types of PII. A more extensive list of PII can be found in the Appendix attached to the end of this policy.

Category of PII	**Sub-categories**
Personal Data	Full name; Home address; Email address; Phone number; Phone, laptop, or other device internet protocol (IP) address; Government-Issued ID # (e.g., Driver's License, Passport, Social Security Number, FEIN); Employer ID number; License Plate; Credit or debit card information; Bank account, brokerage account or other financial information; Date of birth; Place of birth; Other written or scanned information that can directly tie to an individual or household
Sensitive PII or demographic-related PII	Biometric data; Genetic data; Physical identifiable characteristics; Other health records; Race or ethnic origin; Nationality;

Category of PII	Sub-categories
	Immigration status; Religious affiliation; Political affiliation; Voter status; Education records; Criminal records; Online activity and tracking, including cookies, pixels, usernames and passwords, or other online activity; Other sensitive information traditionally kept confidential ***NOTE:** Data is not considered PII if only shared in aggregate of a population larger than 1,000[1] (e.g., # of registered voters in San José)
Image data	Picture that can identify an individual by their face or other physical and contextual information[2]
Recording data	Video that can identify an individual by their face or other physical and contextual information; Audio that can identify an individual by their voice or other contextual information
Geolocation data	Data affiliated with a vehicle, computer, or other device that can be used to identify an individual's physical location
Other sensitive information as determined by the City	

The City may determine, in its sole discretion, that other information is sensitive or PII. If the City determines information that is collected, processed, or otherwise used in the course of doing business with the City is PII, Contractor shall treat new pieces of this information as PII no later than 60 days following written notification from the City unless an extension is approved in writing. Following this written notification, all future information of this type shall be considered PII.

3 Protection and Access to Personally Identifiable Information

The City and Contractor shall make every reasonable effort to protect City and individual privacy. The City and Contractor will only collect personally identifiable information that is required to provide services and in accordance with the Axon Cloud Services Privacy Policy (Exhibit O). Users can decline to provide any personal information. However, if a user declines to provide requested information, the City and Contractor may not be able to provide the user with services dependent upon the collection of that information.

[1] Based on reporting requirements used for anonymity by the U.S. Department of Health and Human Services AFCARS Foster Care Dataset; refer to the 2021 codebook, element #6.

[2] An example of "contextual information" being used to identify someone could include a picture of a license plate or a picture of someone's back next to a house with a visible address.

The City does not intentionally disclose any personal information provided by the Contractor to any third parties or outside the City except as required by law or by the consent of the person providing the information.

Access to personally identifiable information in the City's public records is controlled primarily by the California Public Records Act (Government Code Section 6250, et. seq.). Information that is generally available under the Public Records Act may be posted for electronic access through the City's Web Site. While the Public Records Act sets the general requirements for access to City records, other sections of the California code, as well as federal laws, also deal with confidentiality issues. Additional access to PII may be granted under the direction of local, state, or federal courts or under the direction of the San José City Council in compliance with local, state, or federal laws.

4 Security

The City of San José is committed to data security and the data quality of personally identifiable information that is either available from or collected by City systems and has taken reasonable precautions to protect such information from loss, misuse, or alteration. When handling sensitive personally identifiable information, Contractor shall follow security measures outlined in relevant law and the City's security standards, as well as the City's Information Technology and Security Requirements specified in Exhibit K - Information Technology and Security Requirements.

5 Requirements for contractors when handling data

"Data" shall be as defined in Section 24 of the Agreement.

To the extent permissible by law, Contractor shall adhere to the following requirements for protecting individual privacy while collecting, storing, sharing, processing, or otherwise handling any information they may have access to in the course of doing business with the City:

5.1 Notice to End User (hereinafter "User")

Outside the domain of first responder emergency response efforts, Contractor shall provide "notice at collection" as defined by the California Consumer Privacy Act, listing all PII collected, used, and shared by the data subject. Contractor shall provide such notice in terms that a layperson can understand them. Contractor must provide notice in at least the following languages: English.

If the Contractor does not collect PII on behalf of the City, such as in the case of a database management system with no collection service, the Contractor is not required to provide any notice.

5.2 Minimization

Contractors shall only collect, process, and share the minimum amount of PII required to carry out the designated services on behalf of the City and in accordance with the Axon Cloud Services Privacy Policy (Exhibit O). If the City determines the Contractor is handling

more PII than is required, the Contractor must reduce PII collection to the amount that is appropriate as agreed upon by both parties. All PII that was previously collected that is not deemed necessary by the City for the designated services shall be purged. Failure to reduce and purge data within 30 days of request will be considered a breach of contract unless the City grants an extension.

5.3 Accountability

Contractors shall maintain and provide evidence of compliance with this Privacy and Disclosure Policy upon request by the City.

5.4 Accuracy

Unless otherwise prohibited by local, state or federal law, rule or regulation, a User and the legal guardians of a User of the Contractor's services will be granted by the Contractor the ability to access and correct personally identifiable information used or stored by the Contractor after the Contractor verifies the User is the subject of the relevant personally identifiable information.

If the Contractor is notified by the City or a User of a discrepancy in its information handled on behalf of the City, Contractor shall provide City access to its Cloud Services to verify its existing information and, if found incorrect, correct or delete the inaccurate information within 30 days of notification or request an extension from the City in writing.

5.5 Equity

Contractor shall take reasonable steps to advance equity and mitigate the impact of algorithmic bias through its data and information services while ensuring that PII is only used in accordance with this Agreement. "Reasonable steps" are those set forth in the National Institute of Technology's "Proposal for Identifying and Managing Bias in Artificial Intelligence" and follow-on published technical guidance starting in 2022, referenced herein and incorporated by reference. The City may at any time audit all information, processes, and analyses or request the Contractor anaylze the potential areas of algorithmic bias within or related to the services the Contractor provides to the City.

5.6 Monitoring and Auditing of Contractor Security and Privacy Performance

The City retains the right to observe or audit any relevant work processes, services, or documents in the course of doing business with the City to confirm that the Contractor (and any relevant sub-contractors) is complying with this Privacy and Disclosure Policy. Contractor shall provide access to information, documentation, and personnel required to complete this audit at no additional cost to the City.

6 REQUIRED Disclaimer

City systems provided through a Contractor shall contain a User disclaimer (terms of use) substantially containing the following information:

6.1 Provision of Service

The City of San José ("City") is not liable for any delays, inaccuracies, errors, or omissions relating to material contained or posted on this website, system, or within the services

provided (collectively the "City Systems"). City Systems and all materials contained on them are distributed and transmitted "as is" without warranties of any kind, either express or implied, including without limitations, warranties of title, or implied warranties of merchantability or fitness for a particular purpose. The City is not responsible for any special, indirect, incidental, or consequential damages that may arise from the use of, or the inability to use, the City Systems and/or the materials contained on the City Systems whether the materials contained on the City Systems are provided by the City or a third party. The City is neither responsible nor liable for any viruses or other contamination of user's system.

6.2 Access to Information

Unless otherwise prohibited by state or federal law, rule or regulation, user will be granted the ability to access and correct any personally identifiable information. The City and/or its Contractors will verify user's identity before granting such access. Each service provided that collects personally identifiable information will allow for review and, upon verification, update of that information.

6.3 Non-City Systems

Non-City Systems may be linked through City Systems. The City is not responsible for any non-City Systems, which may or may not be subject to the Public Records Act and may or may not be subject to the San José Municipal Code, California law, or federal law. Visitors to such websites are advised to check the privacy statements of such sites and to be cautious about providing personally identifiable information without a clear understanding of how the information will be used.

6.4 City Liability

The City is not responsible for, and accepts no liability for, the availability of non-City Systems and/or resources. Linked systems are not under the control of, nor maintained by, the City, and the City is not responsible for the content of these systems, which may change frequently. In addition, inclusion of the linked systems does not constitute an endorsement or promotion by the City of any persons or organizations affiliated with the linked systems.

Appendix: PII Reference List

This PII Reference List includes 6 categories and types of PII and subsets of PII that are included when the City refers to "personal" or "sensitive" data or information.

Personally Identifiable Information (PII)
First Name
Last Name
Alias Name
Maiden Name
Full Home Street Address
Zip Code
Date of Birth
Date of Death
Email Address
Photograph
Internet Protocol (IP) Address
Marital Status
Beneficiary Name
Beneficiary Contact Phone Number
Beneficiary Contact Address
Employee ID
Identifying Marks (e.g. tattoos, birth marks, etc.)
Identifying information of children, youth, minors under 18 year old
SSN (full 9 digits)
Driver's License Number
Vehicle Information (license plate #, vehicle ID# (VIN))
Passport Number
State or City ID Number
Criminal Justice Number (arrestee or prisoner numbers)
Username/ID
User Hint Question and Answer
Biometric ID Data (fingerprint, iris scan, faceprint, etc.)
Voter ID Number
FEIN (Federal Employer Identification Number)
Alien Registration Number

Demographics Subset
Citizenship Status
Nationality
Sexual Orientation
Gender Identity

Background Check/Investigation Details or Results
Drug and Alcohol Abuse Information
Criminal Offenses/Convictions
Physical Characteristics
Political Party Affiliation
Political Party Affiliation
Military / Veteran Status
Race / Ethnic Origin
Religious / Philosophical Beliefs

Other Sensor Information
Audio Recordings
Phone Call Recordings
Video Recordings
Social Network Profile, Family Network Research and/or Friends/Contacts/Followers
Computer Use or Website Tracking/ Monitoring (cookies, web beacons, web widgets)
Location Tracking (individual or vehicle, geo-location, RFID Tracking, cell tower data)
Behavioral Pattern Mapping (e.g. physical, psychological, online, etc.)
Item or Identifier Scanning (contraband recognition, license plate reader, RFID reader)
Other Electronic Signatures or Monitoring (other cell phone signal, device sensors monitoring usage not previously stated)
Other Sensory Data (visual, audio, olfactory, or biometric not previously stated)
Other uncategorized surveillance information or data

Health Information Subset
Relative / Emergency Contact Name
Relative / Emergency Contact Phone Number
Relative / Emergency Contact Email
Relative / Emergency Contact Address
Disability Description
Health Diagnosis or Condition for Physical / Mental Health (non-substance use)
Health Diagnosis (substance use)
Health Services Provided
Medical Record Number
Health Plan / Insurance ID Number or Policy (inc. Medicaid & Medicare)
Medical Payments or Health Insurance Payments (incl. Medicaid & Medicare)
Health Policy Group Number
Patient ID Number
Medical Records
Prescriptions / Medications

Financial Information Subset
Bank or Financial Account Number

Credit Card / Debit Card Number
Other Credit / Debit Card Data (eg. Expiration date, security code)
Personal Identification Number (PIN)
Personal Check Data or Scanned Images
Income/Salary/Wage Data
Socio-Economic Status
Credit Score, Credit Grade, or Credit History

Other Sensitive Information (organizational, children, unstructured)
Intellectual Property or Proprietary Information
Budgets, Financial Statements / Forecasts
Organizational Strategy, Business Decision, or Design Info
Legal Documents, Contracts, Vendor Agreements
Other Children's Information not previously stated
Other Confidential Information not previously covered
Any Unstructured Data that might include any of the above types of information

EXHIBIT L

AXON FLEET APPENDIX

This Axon Fleet Appendix is Exhibit L to the Agreement between the City of San José and Axon Enterprise, Inc. for Body Worn Camera and Evidence Management System ("Agreement").

For purposes of this Exhibit L, the term "Agency" shall have the same meaning as "City" as referenced in the Agreement.

For purposes of this Exhibit L, the term "Axon" shall have the same meaning as "Contractor" as referenced in the Agreement.

Each of City and Contractor are sometimes hereinafter referred to as a "Party" and collectively as the "Parties."

This Axon Fleet Appendix shall apply to, and only to, Agency's licensing and use of the Axon Fleet Software and will control and take precedence over the Agreement with respect to the terms of use of the Software.

1 **Agency Responsibilities.** Agency must ensure its infrastructure and vehicles adhere to the minimum requirements to operate Axon Fleet 2 or Axon Fleet 3 (collectively, "Axon Fleet") as established by Axon during the qualifier call and on-site assessment at Agency and in any technical qualifying questions. If Agency's representations are inaccurate, the Quote is subject to change.

2 **Cradlepoint.** If Agency purchases Cradlepoint Enterprise Cloud Manager, Agency will comply with Cradlepoint's end user license agreement. The term of the Cradlepoint license may differ from the Axon Evidence Subscription. If Agency requires Cradlepoint support, Agency will contact Cradlepoint directly.

3 **Third-party Installer.** Axon will not be liable for the failure of Axon Fleet hardware to operate per specifications if such failure results from installation not performed by, or as directed by Axon.

4 **Wireless Offload Server.**

4.1 **License Grant**. Axon grants Agency a non-exclusive, royalty-free, worldwide, perpetual license to use Wireless Offload Server ("**WOS**"). "Use" means storing, loading, installing, or executing WOS solely for data communication with Axon Devices for the number of licenses purchased. The WOS term begins upon the start of the Axon Evidence Subscription.

4.2 **Restrictions**. Agency may not: (a) modify, alter, tamper with, repair, or create derivative works of WOS; (b) reverse engineer, disassemble, or decompile WOS, apply any process to derive the source code of WOS, or allow others to do so; (c) access or use WOS to avoid incurring fees or exceeding usage limits; (d) copy WOS in whole or part; (e) use trade secret information contained in WOS; (f) resell, rent, loan or sublicense WOS; (g) access WOS to build a competitive device or service or copy any features, functions or graphics of WOS; or (h) remove, alter or obscure any confidentiality or proprietary rights notices (including copyright and trademark

notices) of Axon or Axon's licensors on or within WOS.

4.3 **Updates**. If Agency purchases WOS maintenance, Axon will make updates and error corrections to WOS ("**WOS Updates**") available electronically via the Internet or media as determined by Axon. Agency is responsible for establishing and maintaining adequate Internet access to receive WOS Updates and maintaining computer equipment necessary for use of WOS. The Quote will detail the maintenance term.

4.4 **WOS Support**. Upon request by Axon, Agency will provide Axon with access to Agency's store and forward servers solely for troubleshooting and maintenance.

5 **Axon Vehicle Software.**

5.1 **License Grant**. Axon grants Agency a non-exclusive, royalty-free, worldwide, perpetual license to use ViewXL or Dashboard (collectively, "Axon Vehicle Software".) "Use" means storing, loading, installing, or executing Axon Vehicle Software solely for data communication with Axon Devices. The Axon Vehicle Software term begins upon the start of the Axon Evidence Subscription.

5.2 **Restrictions**. Agency may not: (a) modify, alter, tamper with, repair, or create derivative works of Axon Vehicle Software; (b) reverse engineer, disassemble, or decompile Axon Vehicle Software, apply any process to derive the source code of Axon Vehicle Software, or allow others to do so; (c) access or use Axon Vehicle Software to avoid incurring fees or exceeding usage limits; (d) copy Axon Vehicle Software in whole or part; (e) use trade secret information contained in Axon Vehicle Software; (f) resell, rent, loan or sublicense Axon Vehicle Software; (g) access Axon Vehicle Software to build a competitive device or service or copy any features, functions or graphics of Axon Vehicle Software; or (h) remove, alter or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices) of Axon or Axon's licensors on or within Axon Vehicle Software.

6 **Acceptance Checklist**. If Axon provides services to Agency pursuant to any statement of work in connection with Axon Fleet, within 7 days of the date on which Agency retrieves Agency's vehicle(s) from the Axon installer, said vehicle having been installed and configured with tested and fully and properly operational in-car hardware and software identified above, Agency will receive a Professional Services Acceptance Checklist to submit to Axon indicating acceptance or denial of said deliverables.

7 **Axon Fleet Upgrade.** If Agency has no outstanding payment obligations and has purchased the "Fleet Technology Assurance Plan" (Fleet TAP), Axon will provide Agency with the same or like model of Fleet hardware ("Axon Fleet Upgrade") as schedule on the Quote.

7.1 If Agency would like to change models for the Axon Fleet Upgrade, Agency must pay the difference between the MSRP for the offered Axon Fleet Upgrade and the MSRP for the model desired. The MSRP is the MSRP in effect at the time of the upgrade. Agency is responsible for the removal of previously installed hardware and installation of the Axon Fleet Upgrade.

7.2 Within 30 days of receiving the Axon Fleet Upgrade, Agency must return the original Axon Devices to Axon or destroy the Axon Devices and provide a certificate of destruction to Axon, including serial numbers of the destroyed Axon Devices. If Agency does not destroy or return the Axon Devices to Axon, Axon will deactivate the

serial numbers for the Axon Devices received by Agency.

8 **Axon Fleet Termination.** Axon may terminate Agency's Fleet subscription for non-payment. Upon any termination:

8.1 Axon Fleet subscription coverage terminates, and no refunds will be given.

8.2 Axon will not and has no obligation to provide the Axon Fleet Upgrade.

8.3 Agency will be responsible for payment of any missed payments due to the termination before being allowed to purchase any future Fleet TAP.

EXHIBT M

AXON APPLICATION PROGRAMMING INTERFACE APPENDIX

This Axon Application Programming Interface Appendix is Exhibit M to the Agreement between the City of San José and Axon Enterprise, Inc. for Body Worn Camera and Evidence Management System ("Agreement").

For purposes of this Exhibit M, the term "Agency" shall have the same meaning as "City" as referenced in the Agreement.

For purposes of this Exhibit M, the term "Axon" shall have the same meaning as "Contractor" as referenced in the Agreement.

Each of City and Contractor are sometimes hereinafter referred to as a "Party" and collectively as the "Parties."

This Axon Application Programming Interface Appendix shall apply to, and only to, Agency's licensing and use of the Application Programming Interface and will control and take precedence over the Agreement with respect to the terms of use of the Software.

1 **Definitions.**

1.1 "**API Client**" means the software that acts as the interface between Agency's computer and the server, which is already developed or to be developed by Agency.

1.2 "**API Interface**" means software implemented by Agency to configure Agency's independent API Client Software to operate in conjunction with the API Service for Agency's authorized Use.

1.3 "**Axon Evidence Partner API, API or AXON API**" (collectively "**API Service**") means Axon's API which provides a programmatic means to access data in Agency's Axon Evidence account or integrate Agency's Axon Evidence account with other systems.

1.4 "**Use**" means any operation on Agency's data enabled by the supported API functionality.

2 **Purpose and License.**

2.1 Agency may use API Service and data made available through API Service, in connection with an API Client developed by Agency. Axon may monitor Agency's use of API Service to ensure quality, improve Axon devices and services, and verify compliance with this Agreement. Agency agrees to not interfere with such monitoring or obscure from Axon Agency's use of API Service. Agency will not use API Service for commercial use.

2.2 Axon grants Agency a non-exclusive, non-transferable, non-sublicensable, worldwide, revocable right and license during the Term to use API Service, solely for Agency's Use in connection with Agency's API Client.

2.3 Axon reserves the right to set limitations on Agency's use of the API Service, such as a quota on operations, to ensure stability and availability of Axon's API. Axon will use reasonable efforts to accommodate use beyond the designated limits.

3 **Configuration.** Agency will work independently to configure Agency's API Client with API Service for Agency's applicable Use. Agency will be required to provide certain information (such as identification or contact details) as part of the registration. Registration information provided to Axon must be accurate. Agency will inform Axon promptly of any updates. Upon Agency's registration, Axon will provide documentation outlining API Service information.

4 **Agency Responsibilities.** When using API Service, Agency and its end users may not:

4.1 use API Service in any way other than as expressly permitted under this Agreement;

4.2 use in any way that results in, or could result in, any security breach to Axon;

4.3 perform an action with the intent of introducing any viruses, worms, defect, Trojan horses, malware, or any items of a destructive nature to Axon Devices and Services;

4.4 interfere with, modify, disrupt or disable features or functionality of API Service or the servers or networks providing API Service;

4.5 reverse engineer, decompile, disassemble, or translate or attempt to extract the source code from API Service or any related software;

4.6 create an API Interface that functions substantially the same as API Service and offer it for use by third parties;

4.7 provide use of API Service on a service bureau, rental or managed services basis or permit other individuals or entities to create links to API Service;

4.8 frame or mirror API Service on any other server, or wireless or Internet-based device;

4.9 make available to a third-party, any token, key, password or other login credentials to API Service;

4.10 take any action or inaction resulting in illegal, unauthorized or improper purposes; or

4.11 disclose Axon's API manual.

5 **API Content.** All content related to API Service, other than Agency Content or Agency's API Client content, is considered Axon's API Content, including:

5.1 the design, structure and naming of API Service fields in all responses and requests;

5.2 the resources available within API Service for which Agency takes actions on, such as evidence, cases, users, or reports; and

5.3 the structure of and relationship of API Service resources; and

5.4 the design of API Service, in any part or as a whole.

5.5 Prohibitions on API Content. Neither Agency nor its end users will use API content returned from the API Interface to:

5.6 scrape, build databases, or otherwise create permanent copies of such content, or keep cached copies longer than permitted by the cache header;

5.7 copy, translate, modify, create a derivative work of, sell, lease, lend, convey, distribute, publicly display, or sublicense to any third-party;

5.8 misrepresent the source or ownership; or

5.9 remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices).

6 **API Updates.** Axon may update or modify the API Service from time to time ("API Update"). Agency is required to implement and use the most current version of API Service and to make any applicable changes to Agency's API Client required as a result of such API Update. API Updates may adversely affect how Agency's API Client access or communicate with API Service or the API Interface. Each API Client must contain means for Agency to update API Client to the most current version of API Service. Axon will provide support for 1 year following the release of an API Update for all depreciated API Service versions.

EXHIBIT N

AXON RESPOND APPENDIX

This Axon Respond Appendix is Exhibit N to the Agreement between the City of San José and Axon Enterprise, Inc. for Body Worn Camera and Evidence Management System ("Agreement").

For purposes of this Exhibit N, the term "Agency" shall have the same meaning as "City" as referenced in the Agreement.

For purposes of this Exhibit N, the term "Axon" shall have the same meaning as "Contractor" as referenced in the Agreement.

Each of City and Contractor are sometimes hereinafter referred to as a "Party" and collectively as the "Parties."

This Axon Response Appendix shall apply to, and only to, Agency's licensing and use of the Axon Response Software and will control and take precedence over the Agreement with respect to the terms of use of the Software.

1 **Axon Respond Subscription Term.** If Agency purchases Axon Respond as part of a bundled offering, the Axon Respond subscription begins on the later of the (1) start date of that bundled offering, or (2) date Axon provisions Axon Respond to Agency. If Agency purchases Axon Respond as a standalone, the Axon Respond subscription begins the later of the (1) date Axon provisions Axon Respond to Agency, or (2) first day of the month following the Effective Date. The Axon Respond subscription term will end upon the completion of the Axon Evidence Subscription associated with Axon Respond.

2 **Scope of Axon Respond.** The scope of Axon Respond is to assist Agency with real-time situational awareness during critical incidents to improve officer safety, effectiveness, and awareness. In the event Agency uses Axon Respond outside this scope, Axon may initiate good-faith discussions with Agency on upgrading Agency's Axon Respond to better meet Agency's needs.

3 **Axon Body 3 LTE Requirements.** Axon Respond is only available and usable with an LTE enabled body-worn camera. Axon is not liable if Agency utilizes the LTE device outside of the coverage area or if the LTE carrier is unavailable. LTE coverage is only available in the United States, including any U.S. territories. Axon may utilize a carrier of Axon's choice to provide LTE service. Axon may change LTE carriers during the Term without Agency's consent.

4 **Axon Fleet 3 LTE Requirements.** Axon Respond is only available and usable with a Fleet 3 system configured with LTE modem and service. Agency is responsible for providing LTE

service for the modem. Coverage and availability of LTE service is subject to Agency's LTE carrier.

5 **Axon Respond Service Limitations.** Agency acknowledges that LTE service is made available only within the operating range of the networks. Service may be temporarily refused, interrupted, or limited because of: (a) facilities limitations; (b) transmission limitations caused by atmospheric, terrain, other natural or artificial conditions adversely affecting transmission, weak batteries, system overcapacity, movement outside a service area or gaps in coverage in a service area and other causes reasonably outside of the carrier's control such as intentional or negligent acts of third parties that damage or impair the network or disrupt service; or (c) equipment modifications, upgrades, relocations, repairs, and other similar activities necessary for the proper or improved operation of service.

5.1 With regard to Axon Body 3, Partner networks are made available as-is and the carrier makes no warranties or representations as to the availability or quality of roaming service provided by carrier partners, and the carrier will not be liable in any capacity for any errors, outages, or failures of carrier partner networks. Agency expressly understands and agrees that it has no contractual relationship whatsoever with the underlying wireless service provider or its affiliates or contractors and Agency is not a third-party beneficiary of any agreement between Axon and the underlying carrier.

6 **Termination.** Upon termination of this Agreement, or if Agency stops paying for Axon Respond or bundles that include Axon Respond, Axon will end Axon Respond services, including any Axon-provided LTE service.

EXHIBIT O

AXON CLOUD SERVICES POLICY

This Axon Respond Appendix is Exhibit N to the Agreement between the City of San José and Axon Enterprise, Inc. for Body Worn Camera and Evidence Management System ("Agreement").

For purposes of this Exhibit O, the term "Customer" shall have the same meaning as "City" as referenced in the Agreement.

For purposes of this Exhibit O, the term "Axon" shall have the same meaning as "Contractor" as referenced in the Agreement.

Each of City and Contractor are sometimes hereinafter referred to as a "Party" and collectively as the "Parties."

This Axon Response Appendix shall apply to, and only to, Agency's licensing and use of the Axon Response Software and will control and take precedence over the Agreement with respect to the terms of use of the Software.

*This Axon Cloud Services Privacy Policy ("**Policy**") applies only to the information that Axon Enterprise, Inc. ("**Axon**") collects and you or your employer (collectively, "**Customer**") provide to Axon in connection with Customer's use of Axon Cloud Services (as defined below). Axon's marketing sites and other public websites are governed by the Axon Privacy Policy. Usage of Axon Citizen is governed by the Axon Citizen Privacy Policy.*

Unless otherwise provided in this Policy, this Policy is subject to the terms of the Master Services Purchasing Agreement, or other similar agreement, if any, between Axon and Customer ("**Agreement**"). A concept or principle covered in this Policy shall apply and be incorporated into all other provisions of the Agreement in which the concept or principle is also applicable, notwithstanding the absence of any specific cross-reference thereto. All capitalized and defined terms referenced, but not defined, in this Policy shall have the meanings assigned to them in the Agreement.

1 Definitions

1.1 "**Axon Cloud Services**" means Axon's web services hosted on evidence.com including Axon Evidence, Axon Records, and Axon Dispatch, and other related offerings, including, without limitation, interactions between Axon Cloud Services and Axon Products (as defined below).

1.2 "**Axon Products**" means:
(1) Axon Cloud Services;
(2) devices sold by Axon (including, without limitation, conducted energy weapons,

cameras, sensors, and docking systems) (collectively, "**Axon Devices**");
(3) other software offered by Axon (including, without limitation, Axon Investigate, Axon Capture, Axon Evidence SYNC, Axon Device Manager, Axon View, Axon Interview, Axon Commander, Axon Uploader XT, and Axon View XL) (collectively, "**Axon Client Applications**"); and
(4) ancillary hardware, equipment, software, services, cloud-based services, documentation, and software maintenance releases and updates. Axon Products do not include any third-party applications, hardware, warranties, or the 'my.evidence.com' services.

1.3 "**Customer Data**" means:
(1) "Customer Content", which means data uploaded into, ingested by, or created in Axon Cloud Services within Customer's tenant, including, without limitation, media or multimedia uploaded into Axon Cloud Services by Customer ("Evidence"); and
(2) "Non-Content Data", which means:
(a) "Customer Entity and User Data", which means Personal Data and non-Personal Data regarding Customer's Axon Cloud Services tenant configuration and users;
(b) "Customer Entity and User Service Interaction Data" which means data regarding Customer's interactions with Axon Cloud Services and Axon Client Applications;
(c) "Service Operations and Security Data", which means data within service logs, metrics and events and vulnerability data, including, without limitation: (i) application, host, and infrastructure logs; (ii) Axon Device and Axon Client Application logs; (iii) service metrics and events logs; and (iv) web transaction logs;
(d) "Account Data", which means information provided to Axon during sign-up, purchase, or administration of Axon Cloud Services, including, without limitation, the name, address, phone number, and email address Customer provides, as well as aggregated usage information related to Customer's account and administrative data associated with the account; and
(e) "Support Data", which means the information Axon collects when Customer contacts or engages Axon for support, including, without limitation, information about hardware, software, and other details gathered related to the support incident, such as contact or authentication information, chat session personalization, information about the condition of the machine and the application when the fault occurred and during diagnostics, system and registry data about software installations and hardware configurations, and error-tracking files.

For purposes of clarity, Customer Content does not include Non-Content Data, and Non-Content Data does not include Customer Content.

1.4 **"Data Controller"** means the natural or legal person, public authority, or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data (as defined below).

1.5 **"Data Processor"** means a natural or legal person, public authority or any other body which processes Personal Data on behalf of the Data Controller.

1.6 **"Personal Data"** means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.7 "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.8 **"Sub-processor"** means any third party engaged by the Data Processor to assist in data processing activities that the Data Processor is carrying out on behalf of the Data Controller.

2 Axon's Role

2.1 Axon is a Data Processor of Customer Content. Customer is a Data Controller and controls and owns all right, title, and interest in and to Customer Content and Axon obtains no rights to the Customer Content. Customer is solely responsible for the uploading, sharing, withdrawal, management and deletion of Customer Content. Customer grants Axon limited access to Customer Content solely to provide and support Axon Cloud Services to and for Customer and Customer's end-users. Customer represents and warrants to Axon that: (1) Customer owns Customer Content; (2) and Customer Content, and Customer's end-users' use of Customer Content and Axon Cloud Services, does not violate this Policy or applicable data protection laws and regulations. Axon is not responsible for Customer's privacy practices as a Data Controller. You should consult the Privacy Policy of the relevant customer to review these.

2.2 Axon may also collect, control, and process Non-Content Data. Axon is a Data Controller for Non-Content Data. Axon collects, controls, and processes Non-Content Data to provide Axon Cloud Services and to support the overall delivery of Axon Products including business, operational, and security purposes. With Non-Content Data, Axon may analyze and report anonymized and aggregated data to communicate with external and internal stakeholders. In regard to Customer Entity & User Data, Axon is a Data Controller and Customer is an independent Data Controller, not a joint Data Controller.

3 Data Collection Purposes and Processing Activities

3.1 CUSTOMER CONTENT

3.1.1 Axon will only use Customer Content to provide Customer Axon Cloud Services. Axon will not use Customer Content for any advertising or similar commercial purposes.

3.1.2 Axon periodically upgrades or changes Axon Cloud Services to provide customers with new features and enhancements in alignment with the Axon Evidence Maintenance Schedule. Axon communicates such upgrades or changes to customers one week prior to release via mechanisms outlined in the Maintenance Schedule. Changes to Axon

Cloud Services may increase the capabilities of the service and ways in which Customer Content can be processed.

4 NON-CONTENT DATA

4.1 Non-Content Data includes data, configuration, and usage information about customer's Axon Cloud Services tenant, Axon Devices, Axon Client Applications, and users that is transmitted or generated when using Axon Products. Non-Content Data includes the following:

4.2 Customer Entity And User Data

4.2.1 Customer Entity and User Data includes personal and non-personal data regarding Customer's Axon Cloud Services tenant configuration and users. Axon uses Customer Entity and User Data to: (1) provide Axon Cloud Services, including, without limitation, user authentication and authorization functionality; (2) improve the quality of Axon Products or provide enhanced functionality and features; (3) contact Customer to provide information about its account, tenant, subscriptions, billing, and updates to Axon Cloud Services, including, without limitation, information about new features, security and other technical issues; and (4) market our products or services to Customer via email, by sending promotional communication including targeted advertisements, or presenting a Customer with relevant offers.

4.2.2 Customer cannot unsubscribe from non-promotional communications but may unsubscribe from promotional communications at any time such as by clicking on an unsubscribe button at the bottom of such communications.

4.3 Customer Entity and User Service Interaction Data

Customer Entity and User Service Interaction Data includes data regarding Customers' interactions with Axon Cloud Services and Axon Client Applications. Axon uses Customer Entity and User Service Interaction Data to improve the quality of Axon Products and provide enhanced functionality and features.

4.4 Service Operations and Security Data

Axon uses Service Operations and Security Data to provide service operations and monitoring.

4.5 Account Data

Axon uses Account Data to provide Axon Cloud Services, manage Customer's accounts, market to, and communicate with Customer.

4.6 Support Data

4.6.1 Axon uses Support Data to resolve Customer’s support incident, and to operate, improve, and personalize Axon Products. If Customer shares Customer Content to Axon in a support scenario, the Customer Content will be treated as Support Data but will only be used for resolving support incidents.

4.6.2 Axon may provide support through phone, email, or online chat. With Customer's permission, Axon may use Guest Access ("GA") to temporarily navigate Customer's Axon Cloud Service's tenant to view data in order to resolve a support incident. Phone conversations, online chat sessions, or GA sessions with Axon support professionals may be recorded and/or monitored for efforts such as training, future support, and evidentiary purposes.

5 Server and Data Location

5.1 CUSTOMER CONTENT

5.1.1 Axon offers Axon Cloud Services in numerous geographic regions. Before creating an account in Axon Cloud Services, Customer determines where Axon will store Customer Content by designating an economic area.

REGION CODE	ECONOMIC AREA	3RD PARTY INFRASTRUCTURE SUB-PROCESSORS	DATA CENTER LOCATION(S)
AU	Southeast Asia	Microsoft Azure	Canberra, ACT
LA	South America	Microsoft Azure	Sao Paulo, Brazil & Texas, United States
CA	Canada	Microsoft Azure	Toronto, ON & Quebec City, QC
EU	European Union	Amazon Web Services	Ireland **new customers will not be added to this region*
EUR	European Union	Microsoft Azure	Netherlands, Ireland
UK	United Kingdom	Microsoft Azure and Amazon Web Services	London, England & Cardiff, Wales
US	United States	Microsoft Azure and Amazon Web Services	Texas, Virginia & Oregon, United States
US	United States (Federal Region)	Microsoft Azure	Texas & Virginia, United States
ENT	Global	Microsoft Azure	Washington & Wyoming, United States

5.1.2 Axon ensures that all Customer Content in Axon Cloud Services remains within the selected economic area, including, without limitation, all backup data, replication sites, and disaster recovery sites. Customer selected economic areas can be determined through review of Customer's Axon Cloud Services URL. Customer URLs conform to the *<youragency>.<regioncode>.evidence.com* scheme with the exception of US customers where the scheme may exclude the region code and is *<youragency>.evidence.com*. US Federal customers conform to the scheme *<youragency>.us.evidence.com*

5.2 NON-CONTENT DATA

5.2.1 Customer Entity and User Data

Customer Entity and User Data is located in Customer's selected economic area for Customer Content. Customer Entity and User Data may be copied or transferred to the United States.

5.2.2 Customer Entity and User Service Interaction Data

Customer Entity and User Service Interaction Data is located in Customer's selected economic area for Customer Content and the United States.

5.2.3 Service Operations and Security Data

Service Operations and Security Data is located in Customer's selected economic area for Customer Content and the United States.

5.2.4 Account Data and Support Data

Account and Support Data is located in the United States and may be located in Customer's selected economic area for Customer Content.

6 Information Sharing

6.1 Axon may share data with its subsidiaries, service providers and other partners to help us operate, including for providers to facilitate: (1) user account management, authentication, analytics, and communication, (2) product features, e.g. geolocation services, product development, and error analytics, (3) customer service and support, and (4) security monitoring and investigation.

6.2 In addition, Axon shares data with Axon's sub-processors as described in the "Axon Sub-Processors" section below.

6.3 For more information about sharing of Personal Data by Axon, please contact privacy@axon.com.

7 Axon Sub-Processors

7.1 Axon may rely on Sub-processors to provide or enhance Axon Products on its behalf. Axon only permits Sub-processors to use Customer Content to deliver to the Customer services that Axon offers. Axon prohibits Sub-processors from using Customer Content for any other purpose. Ownership of rights, titles and interest in and to Customer Content remain with Customer.

7.2 Axon exercises commercially reasonable efforts in connection with contractual obligations to ensure its Sub-processors are compliant with all applicable data protection laws and regulations surrounding the Sub-processors access and scope of work in connection with Customer Content. Prior to onboarding Sub-processors, Axon audits the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to the scope of their services.

7.3 Axon maintains an up-to-date list of the names and locations of all Sub-processors for Customer Content at https://www.axon.com/privacy/sub-processors-details.

7.4 Axon will give Customer notice of any new Sub-processor before Axon authorizes any new Sub-processor to process Customer Content in connection with the provision of

Customer services through an opt-in notification subscription service at https://go.axon.com/l/636291/2020-09-11/42s1s9.

8 TELECOMMUNICATION SUB-PROCESSORS

8.1 Axon Body 3 includes embedded cellular technologies used to connect to telecommunication networks in order to provide connectivity between Axon Body 3 and Axon Cloud Services. Cellular technologies enable Axon Aware services. Customer's Axon Body 3 cameras will send data to the respective Axon Cloud Services region selected telecommunications providers as needed to enable cellular connectivity. Data includes Personal Data, such as location data. For Axon Body 3, Axon manages all cellular registration and account management associated to the cellular subscription. Personal Data of Customer is not collected by Axon or telecommunications providers for the purposes of cellular account management.

8.2 Outlined below are the telecommunication sub-processors. In regions where there are more than one telecommunication sub-processor, Axon will manage Customers Axon Body 3 cellular registration.

REGION CODE	ECONOMIC AREA	TELECOMMUNICATION SUB-PROCESSORS
AU	Southeast Asia	Telstra
LA	South America	TBD / TBA
CA	Canada	Telus
EU/EUR	European Union	T-Systems
UK	United Kingdom	BTEE
US	United States	Verizon and AT&T (FirstNet)
US	United States (Federal Region)	Verizon and AT&T (FirstNet)
ENT	Global	Verizon and AT&T (FirstNet)

8.3 Customer URLs conform to the <*youragency*>.<*regioncode*>.*evidence.com* scheme with the exception of US customers where the scheme may exclude the region code and is <*youragency*>.*evidence.com*. US Federal customers conform to the scheme <*youragency*>.*us.evidence.com*

9 Required Disclosures

9.1 Axon will not disclose Customer Content except as required by any law or regulation. If permitted, Axon will notify Customer if any disclosure request is received for Customer Content so Customer may challenge or object.

10 Customer's Access and Choice

10.1 Customer Content

10.1.1 Customer can access Customer's tenant to manage Customer Content.

10.1.2 Axon will work with Customers to provide access to Personal Data that Axon or Sub-processors hold. Axon will also take reasonable steps to enable Customers to correct, amend, or delete Personal Data that is demonstrated to be inaccurate.

10.2 **Non-Content Data**
If at any time after registering an account on Axon Cloud Services you desire to update Personal Data you have shared with us, change your mind about sharing Personal Data with us, desire to cancel your Customer account, or request that Axon no longer use provided Personal Data to provide you services, please contact us at privacy@axon.com.

10.3 If you are in the European Economic Area, ("**EEA**"), United Kingdom or Switzerland, you can consult Your Rights here.

10.4 Certain data processing can be adjusted by Customer based on Axon Product usage, Customer network or device configuration, and administrative settings made available with Axon Cloud Services or Axon Client Applications:

10.5 Axon Body 3 WiFi Positioning

10.5.1 Axon Body 3 cameras offer customers a feature to enhance location services where GPS/GNSS signals may not be available, for instance within buildings or underground. Customer administrators can manage their choice to use this service within the administrative features of Axon Cloud Services. When WiFi Positioning is enabled, Non-Content and Personal Data including location, device and network information data will be sent to Skyhook Holdings, Inc (Skyhook) to facilitate the WiFi Positioning functionality. Skyhook will act as both a data sub-processor (as reflected in this Policy) and as a data controller. Skyhook becomes a data sub-processor for Axon when Skyhook processes data from Axon Body 3 devices to determine a location. Skyhook acts a data controller when it collects data sent from Axon Body 3 cameras to maintain their services and to develop new products, services or datasets. Data controlled by Skyhook is outside the scope of this Policy and is subject to the Skyhook Services Privacy Policy.

10.6 Client Push Notifications

10.6.1 Axon Products leverage push notification services made available by mobile operating system providers (i.e. Google's Cloud Messaging and Apple's Push Notification Service to deliver functional notifications to client applications. Push notification services can be managed by leveraging notification settings made available in both mobile applications and the mobile operating system.

10.7 User Analytics

10.7.1 Customers can opt-out of user analytics tracking on Axon Cloud Services by disabling cookies or preventing Customer's browser or device from accepting new cookies. To prevent data from being collected by Mixpanel, network or device access to *.mixpanel.com should be blocked

10.8 Service Support

10.8.1 Mobile client application crash analytics provide Axon personnel insight to crashes when using Axon client applications. To opt out of crash reporting, network or device access to *.crashlytics.com should be blocked.

10.9 Geolocation Services

10.9.1 Geolocation services are critical to proper user functionality of many Axon products. However, customers can opt out of mapping and geolocation functionality by blocking network or device access to *.mapbox.com and *.arcgisonline.com

11 Data Security Measures

11.1 Axon is committed to help protect the security of Customer Data. Axon has established and implemented policies, programs, and procedures that are commercially reasonable and in compliance with applicable industry practices, including administrative, technical and physical safeguards to protect the confidentiality, integrity and security of Customer Content and Non-Content Data against unauthorized access, use, modification, disclosure or other misuse.

11.2 Axon will take appropriate steps to ensure compliance with the data security measures by its employees, contractors and Sub-processors, to the extent applicable to the respective scope of performance.

11.3 CONFIDENTIALITY

11.3.1 Customer Content and Non-Content Data is encrypted in transit over public networks. Customer Content is encrypted at rest in all Axon Cloud Service regions.

11.3.2 Axon protects all Customer Content and Non-Content Data with strong logical access control mechanisms to ensure only users with appropriate business needs have access to data. Third-party specialized security firms periodically validate access control mechanisms. Access control lists are reviewed periodically by Axon.

11.4 INTEGRITY

11.4.1 As Evidence is ingested into Axon Cloud Services, a Secure Hash Algorithm (“SHA”) checksum is generated on the upload device and again upon ingestion into Axon Cloud Services. If the SHA checksum does not match, the upload will be reinitiated. Once upload of Evidence is successful, the SHA checksum is retained by Axon Cloud Services and is made viewable by users with access to the Evidence audit trail for the

specific piece of Evidence. Tamper-proof audit trails are created automatically by Axon Cloud Services upon ingestion of any Evidence.

11.5 AVAILABILITY

11.5.1 Axon takes a comprehensive approach to ensure the availability of Axon Cloud Services. Axon replicates Customer Content over multiple systems to help to protect against accidental destruction or loss. Axon Cloud Services systems are designed to minimize single points of failure. Axon has designed and regularly plans and tests its business continuity planning and disaster recovery programs.

11.6 ISOLATION

11.6.1 Axon logically isolates Customer Content. Customer Content for an authenticated customer will not be displayed to another customer (unless Customers explicitly create a sharing relationship between their tenants or shared data between themselves). Centralized authentication systems are used across an Axon Cloud Service region to increase uniform data security.

11.6.2 Additional role-based access control is leveraged within Customer's Axon Cloud Service tenant to define what users can interact with or access Customer Content. Customer solely manages the role based access control mechanisms within its Axon Cloud Services tenant.

11.6.3 Within the Axon Cloud Services supporting infrastructure, access is granted based on the principle of least privilege. All access must be approved by system owners and undergo at least quarterly user access reviews. Any shared computing or networking resource will undergo extensive hardening and is validated periodically to ensure appropriate isolation of Customer Content.

11.6.4 Non-Content Data is logically isolated within information systems such that only appropriate Axon personnel have access.

11.7 PERSONNEL

11.7.1 Axon personnel are required to conduct themselves in a manner consistent with applicable law, the company's guidelines regarding confidentiality, business ethics, acceptable usage, and professional standards. Axon personnel must complete security training upon hire in addition to annual and role-specific security training.

11.7.2 Axon personnel undergo an extensive background check process to the extent legally permissible and in accordance with applicable local labor laws and statutory regulations. Axon personnel supporting Axon Cloud Services are subject to additional role-specific security clearances or adjudication processes, including Criminal Justice Information Services background screening and national security clearances and vetting.

12 Data Breach

12.1 NOTIFICATION

12.1.1 If Axon becomes aware that Customer Data has been accessed, disclosed, altered, or destroyed by an unlawful or unauthorized party, Axon will notify relevant authorities (where required) and affected customers.

12.1.2 Axon will immediately notify Customer administrators registered on Axon Cloud Services. Authorities will be notified through Axon's established channels and timelines. The notification will reasonably explain known facts, actions that have been taken, and make commitments regarding subsequent updates. Additional details are available in the Axon Cloud Services Security Incident Handling and Response Statement.

13 Data Portability, Migration, and Transfer Back Assistance

13.1 DATA PORTABILITY

13.1.1 Evidence uploaded to Axon Cloud Services is retained in original format. Evidence may be retrieved and downloaded by Customer from Axon Cloud Services to move data to an alternative information system. Evidence audit trails and system reports may also be downloaded in various industry-standard, non-proprietary formats.

13.2 DATA MIGRATION

13.2.1 In the event Customer's access to Axon Cloud Services is terminated, Axon will not delete any Customer Content during the 90 days following termination. During this 90-day period, Customer may retrieve Customer Content only if Customer has paid all amounts due (there will be no application functionality of the Axon Cloud Services during this 90-day period other than the ability for Customer to retrieve Customer Content). Customer will not incur any additional fees if Customer downloads Customer Content from Axon Cloud Services during this 90-day period. Axon has no obligation to maintain or provide any Customer Content after the 90-day period and thereafter, unless legally prohibited, may delete Customer Content upon termination as part of normal retention and data management instructions from customers. Upon written request, Axon will provide written proof that all Customer Content has been successfully deleted and removed from Axon Cloud Services.

13.3 POST-TERMINATION ASSISTANCE

13.3.1 Axon will provide Customer with the same post-termination data retrieval assistance that is generally made available to all customers.

14 Data Retention, Restitution, and Deletion

14.1 Axon maintains internal disaster recovery and data retention policies in accordance with applicable laws and regulations. The disaster recovery plan relates to Axon's data and extends to Axon Cloud Services and Customer Content stored within. Axon's data retention policies relate to Axon's Non-Content Data. Axon's data retention policies

instruct for the secure disposal of Non-Content Data when such data is no longer necessary for the delivery and support of Axon product and services and in accordance with applicable regulations. We will retain Non-Content Data for as long as needed to provide you services, comply with our legal obligations, resolve disputes, and enforce our agreements. As outlined below, Customer is responsible for adhering to its own retention policies and procedures.

15 **Evidence Retention**

15.1 Customer defines Evidence retention periods pursuant to Customer's internal retention policies and procedures. Customer can establish its retention policies within Axon Cloud Services. Therefore, Customer controls the retention and deletion of its Evidence within Axon Cloud Services. Axon Cloud Services can automate weekly messages summarizing upcoming agency-wide deletions to all customer Axon Cloud Services administrators. Customer users can receive a weekly message regarding Evidence uploaded within their user account to protect against accidental deletions. Customer can recover Evidence up to 7 days after Customer queues such Evidence for deletion. After this 7-day grace period, Axon Cloud Services initiates deletion of Evidence. Data deletion processing may occur asynchronously across storage systems and data centers. During and after data deletion processing, Evidence will not be recovered or recoverable by any party.

16 **Accountability**

16.1 As outlined herein, Axon is committed to maintaining compliance with relevant security and privacy standards to ensure the continued security, availability, integrity, confidentiality, and privacy of Axon Cloud Services and Customer Data stored within.

16.2 In addition to the security efforts outlined herein, Axon will maintain its ISO/IEC 27001:2013 certification or comparable assurances for Axon Cloud Services. Customers may review the certificate.

17 **Insurance**

17.1 Axon will maintain, during the term of the Agreement, a cyber-insurance policy and will furnish certificates of insurance following Customer's written request.

18 **How to Contact Us**

18.1 Axon commits to resolve complaints about Customer privacy and use of Axon Products. Complaints surrounding this Policy can be directed to Customer's local Axon representative or privacy@axon.com. If Customer has any questions or concerns regarding privacy and security of Customer Content or Axon's handling of Customer's Personal Data, please contact privacy@axon.com.

18.2 If Customer is an European Union citizen, an United Kingdom citizen, or a citizen of Switzerland and we are unable to satisfactorily resolve any complaint or if Axon fails to acknowledge Customer's complaint in a timely fashion, Customer can contact the relevant European Union Data Protection Authorities (DPAs), United Kingdom Information Commissioners Office (ICO), or the Switzerland Federal Data Protection and Information Commissioner (FDPIC).

EXHIBIT P
SUPPLEMENTAL WORK ORDER FORM

Date:

Pre-approval required before start of work: _____
(City Project Manager Printed Name)

Supplemental Services (Labor)					
Date	**Time: From/To**	**Hours**	**Hourly Pay Rate**	**Description of Work**	**Amount**
Total Amount Due					**$**

Additional Purchases			
Description	**Unit Price**	**QTY**	**Amount**
Total Purchases			**$**

Pricing and invoicing schedule pursuant to Contractor's Quote _____.

_____ _____
CITY PROJECT MANAGER SIGNATURE **CONTRACTOR SIGNATURE**