

From: R B
To: [Patti Chacker](#)
Subject: OPRA request - ALPR Information
Date: Monday, December 1, 2025 3:49:15 PM

CAUTION: This email originated from outside of Cherry Hill Township. DO NOT reply, click links or open attachments unless you recognize the sender and know the content is safe.

Dear Cherry Hill Township,

Please accept this electronic request for public records made under OPRA and the common law right of access. I am not required to fill out an official form or use a particular software platform to submit my request per NJSA 47:1A-6(f), which states that an email from a requestor including all of the information required on the adopted form shall suffice in place of a completed form as a valid government record request.

I HAVE NOT been convicted of any indictable offense under the laws of New Jersey, any other state, or the United States.

I WILL NOT use the requested government records for a commercial purpose.

I AM NOT seeking records in connection with a legal proceeding.

Records requested:

Contracts with ALPR (Automated License Plate Reader) Vendors: All contracts, agreements, memoranda of understanding, or other documents between the Cherry Hill Police Department and any company providing ALPR technology or services, including but not limited to Flock Safety, Vigilant Solutions, Rekor Systems, or any other ALPR vendor. This includes any amendments, renewals, or extensions of such contracts executed or effective between January 1, 2023, and November 15, 2025.

Policies on ALPR Data Access: All policies, procedure manuals, training materials, or other documentation, effective or revised between January 1, 2023, and November 15, 2025, that describe who within the Cherry Hill Police Department (e.g., specific roles, ranks, or units) is authorized to search or access license plate data collected by any ALPR vendor, regardless of whether the data is stored by the vendor or Cherry Hill.

Policies on ALPR Search Logs and Audits: All policies, procedure manuals, or other documentation, effective or revised between January 1, 2023, and November 15, 2025, that describe:

- The maintenance of logs recording who searches ALPR data, when, and the stated reason or purpose for each search.
- The process, frequency, and criteria for auditing such logs to ensure compliance with Cherry Hill Police Department policies or state/federal law, including any reports or documentation summarizing audit procedures.

My preferred delivery method for response(s) to this request is by E-mail as attachments. Please confirm you have received this request. If you are not the custodian of records, please forward my request to that person and provide their email address to me for future reference.

Yours faithfully,

R B

Please deliver records electronically via email to the below UNIQUE address for all replies to this request:

XXXXXXXXXXXXXXXXXXXXXXXXXXXX@XXXXXXXXXXXXXXXXXXXX

Is XXXXXXX@XXXX.XXX the wrong address for OPRA requests to Cherry Hill Township? If so, please contact us using this form:

https://linkprotect.cudasvc.com/url? a=https%3a%2f%2fopramachine.com%2fchange_request%2fnew%3fbody%3dcherry_hill_township&c=E.1Jhr73Y_j2dJTZgSUrcIt8uORi0I193hA_dh6KKuV2vsFvGXpy2VxqOEDMZjcQICa6olVcGiVrlf14lrTn: tXSzy1Y8BxjlgaAiZen_unrdqrrPbfgfBSw...&typo=1

Disclaimer: This message and any reply that you make will be published on the internet. Our privacy and copyright policies:

https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fopramachine.com%2fhelp%2fofficers&c=E.1w4WWu87orAPMt-8OPgfcUj1_KpPO8JqXH8W_JaJSAHqWqs-mVcl2nHAVYfZC- 9D2oZ5wbr_4IDMSnQOOmln9Y1zM86gQUImjipdM3LHMzQz44mAI0wKB7GA...&typo=1

View this OPRA request & responses online:

https://linkprotect.cudasvc.com/url? a=https%3a%2f%2fopramachine.com%2frequest%2falpr_information&c=E.1kSnz_VpKy6fKRzctIMdpXsFC1gsnHmVGBRwqO_dshaX2h9p4wVoAV9f0EOzvkgkfPE5vx_AsSg3RkQ6XNc429OFicSKOgogb3PLla9ZO...&typo=1

Please note that in some cases publication of requests and responses will be delayed.

If you find this service useful as an OPRA custodian, please ask your web manager to link to us from your organisation's website.

"OPRAMachine's mission is to give people easy and affordable access to New Jersey public records.

For more information, contact us at: (732) 707-1628 or PO Box 3180, New Brunswick, NJ 08903."

		
SUBJECT: AUTOMATED LICENSE PLATE RECOGNITION (ALPR)	ORDER # 12-04	
EFFECTIVE DATE: 04-11-23	NUMBER OF PAGES: 18	
ACCREDITATION STANDARDS:	BY THE ORDER OF: Chief of Police	

PURPOSE: The purpose of this directive is to establish a uniform policy and procedure for the use of automated license plate recognition (ALPR).

POLICY: It is the policy of the Cherry Hill Police Department to utilize ALPR technology to the extent possible in accordance with the New Jersey Attorney General Law Enforcement Directive 2022-12 (**Appendix A**).

PROCEDURE:

Definitions/Terms:

1. **Agency ALPR Coordinator** – The main point of contact within a law enforcement or public safety agency or authority, designated by the law enforcement executive who will be the external point of contact for agency ALPR-related items such as information sharing and audits, internally oversee the agency's ALPR program, including training and approving access requests (may delegate approval authority to other supervisors), and designate authorized users within the agency who can use ALPRs and access stored data.
2. **Alert Data** - Information captured by an ALPR relating to a license plate that matches the license plate on a BOLO list.
3. **Automated License Plate Recognition (ALPRs)**- Technology that uses optical character recognition on images to read vehicle registration plates to create vehicle location data. ALPR can be a system consisting of a camera, or cameras, and related equipment that automatically and without direct human control locates, focuses on, and photographs license plates and vehicles that come into range of the device, that automatically converts digital photographic images of scanned license plates into electronic text documents, that is capable of comparing scanned license plate text data with data files for vehicles on a BOLO (be on the lookout) list that notifies law enforcement, whether by an audible alert or by other means when a scanned license plate matches the license plate on the BOLO list. The term includes both devices that are placed at a stationary location (whether permanently mounted or portable devices positioned at a stationary location) and mobile devices affixed to a police vehicle and capable of operating while the vehicle is in motion.
4. **ALPR Camera(s)** – This refers to, but is not limited to, high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, handheld devices or attached to patrol vehicles.
5. **ALPR System** - Refers to any software platform or ALPR device (portable or fixed) which connects to a data repository.
6. **ALPR Vendor** - Any business or company providing ALPR solutions or technology systems including, but not limited to, cameras, hardware, software, maintenance, license, data storage, and associated equipment.
7. **Authorized User** - A sworn or civilian employee who has successfully completed ALPR training designed and disseminated by the State ALPR Coordinator and any training on ALPR policy provided by their agency and has been authorized to operate an ALPR or to access and use ALPR stored data. Employees of a law enforcement agency, public safety agency, or Attorney General's or county prosecutor's office can be authorized users. Authorization shall be given by the Agency ALPR Coordinator for each respective agency.
8. **BOLO (Be on the Lookout)** - Refers to a determination by a law enforcement agency that there is a legitimate and specific law enforcement reason to identify or locate a particular vehicle, or any person(s) who are reasonably believed to be associated with that vehicle.
9. **BOLO List** - Sometimes referred to colloquially as a "hot list," is a compilation of one or more license plates, or partial license plates, of a vehicle or vehicles for which a BOLO situation exists. The list is automatically imported into the vehicle's electronic memory or processor on a regular basis, updated at a minimum every 24 hours, or as appropriate to have the latest information. The device will alert if it captures the image of a license plate that matches a

license plate included on the BOLO list. The term also includes a compilation of one or more license plates or partial license plates that are compared against stored license plate data that had previously been scanned and collected by an ALPR, including scanned license plate data stored in a separate data storage device or system.

10. **BOLO query** - Refers to the process of querying and comparing a BOLO list against stored non-alert data.
11. **Commercial ALPR Data** - Refers to data collected by an entity for commercial purposes.
12. **County ALPR Coordinator** - The main point of contact within a County Prosecutor's Office, designated by the county Prosecutor for ALPR-related responsibilities. A County Prosecutor's Office utilizing a Sheriff's Department or Public Safety Agency to maintain ALPR data will have County ALPR Co-coordinators. In this circumstance, a County Prosecutor's Office is encouraged to allow the Sheriff's Department or Public Safety Agency the ability to maintain certain ALPR-related responsibilities as long as the Prosecutor's Office maintains audit authority.
13. **Crime Scene Query** - The process of accessing and reviewing stored non-alert ALPR data that had been originally scanned at or about the time and in the vicinity of a reported criminal event for the purpose of identifying vehicles or persons that might be associated with that specific criminal event as suspects, witnesses, or victims.
14. **Crime Trend Analysis** - refers to the analytical process by which agencies may access and use stored non-alert data where such access, which may be automated, might reasonably lead to the discovery of evidence or information relevant to an investigation that is not related to a specific criminal event. Such access must be approved by the Agency ALPR Coordinator or their designee. The analysis shall not result in the disclosure of personal identifying information (such as name, address, SSN, vehicle operator's license number) to an authorized user or any other person unless (a) there exist "specific and articulable facts that warrant further investigation" of possible criminal or terrorist activity by the driver or occupants of a specific vehicle and access has been approved by a designated supervisor; or (b) disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena. Any crime trend analysis shall document the nature and purpose of the crime trend analysis; the authorized users who accessed stored non-alert data; the designated supervisor who approved access; and where personal identifying information was disclosed, (a) the specific and articulable facts that warrant further investigation and (b) the designated supervisor who approved the disclosure of personal identifying information; or, where applicable, the fact that a grand jury subpoena authorized access to personal identifying information.
15. **Criminal Event** - A specific incident, or series of related specific incidents, that would constitute an indictable crime under the laws of the State of New Jersey, whether or not the incident(s) have occurred or will occur within the State of New Jersey. The term includes an attempt or conspiracy to commit a crime, or actions taken in preparation for the commission of the crime, such as conducting a surveillance of the location to identify and evade or thwart security measures or conducting a rehearsal of a planned crime. The term includes two or more separate criminal acts or episodes that are linked by common participants or that are reasonably believed to have been undertaken by a criminal organization or as part of an ongoing conspiracy.
16. **Designated Supervisor** – A sworn supervisor who is an ALPR "authorized user", assigned by the Agency ALPR Coordinator who can approve access to crime trend analysis and the disclosure of PII. A law enforcement agency may have more than one designated supervisor.

17. **Handheld ALPR** - A handheld device with loaded ALPR-based software.
18. **Immediate Alert** - An alert that occurs when a scanned license plate matches the license plate on an initial BOLO list and that is reported to the officer operating the ALPR, by means of an audible alarm or by any other means, at or about the time that the subject vehicle was encountered by the ALPR and its license plate was scanned by the ALPR.
19. **Law Enforcement ALPR Data** - Data collected by ALPRs deployed by law enforcement.
20. **Mobile ALPR** - An ALPR camera(s) mounted on a motor vehicle.
21. **Non-encounter Alert**-An immediate alert where the officer operating the ALPR is instructed to notify the agency that put out the BOLO without initiating an investigative detention of the subject vehicle or otherwise revealing to the occupant(s) of that vehicle that its location has been detected or that it is the subject of law enforcement attention.
22. **NJ's ALPR Data Sharing Agreement** - Refers to Directive 2022-12, which is a data sharing agreement between any state, county and local law enforcement agency and/or authority operating in NJ, which allows unfettered access into ALPR captured read data and amongst law enforcement agencies.
23. **NJ SNAP (New Jersey's Statewide Networked ALPR Program)**-The interconnected, state ALPR technological framework to establish access to all NJ LE ALPR data and the interface which allows authorized users to query all current and historical connected ALPR data.
24. **Permanent Fixed ALPR** - ALPR camera(s) mounted in a way that it is not easily moved and is generally affixed to a pole, traffic standard, etc.
25. **Personal identifying information (PII)** - Defined as any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. PII refers to information that identifies one or more specific individuals, including an individual's name, address, social security number, vehicle operator's license number, or biometric records. This includes data comprising a BOLO list and information gained by comparison to the Motor Vehicle Commission (MVC) database or any other data system.
26. **Point of Interest (POI)** - Refers to a person and/or vehicle designated on a POI BOLO list entered by an authorized user. When the POI is created, NJ SNAP pushes the POI to all NJ SNAP certified vendors and immediately returns known locate notifications. After the POI is created, NJ SNAP sends out future notification(s) to the investigator via text or email with near real-time information obtained about any POI. An authorized user must designate a supervisor in order to create a POI and a copy of the POI information is sent to their designated supervisor. A stolen motor vehicle-related POI expires after 48 hours. All other POIs expire within 30 days unless the authorized user designates an alternate expiration date. POIs can be removed before the expiration date by the authorized user who created the POI, their designated supervisor or an administrator. POIs can be extended in NJ SNAP by the authorized user who created the POI, their designated supervisor or an administrator. If not extended, the POI will automatically expire.
27. **Portable Fixed ALPR Camera(s)** - ALPR camera(s) that are fixed to a moveable object or are easily attached and removed from an immovable object. Examples include ALPR cameras that are attached to a trailer or a "quick connect" ALPR camera that is easily removed from a fixed

object, like a telephone pole.

28. **Public-Private Partnership ALPR Data** - ALPR data collected by a private entity that has entered a public-private partnership with law enforcement.
29. **Scan** -The process by which an ALPR automatically focuses on, photographs, utilizes optical character recognition (OCR), or converts to digital text the license plate of a vehicle that comes within the range of the ALPR device "reading" the plate characters.
30. **Statewide ALPR Program Coordinator**- The coordinator, assigned by the Attorney General, in consultation with the NJSP ROIC Commander, tasked with overseeing the Statewide ALPR Program.
31. **State ALPR Repository** - The repository of NJSP ALPR data. This repository is owned and maintained by the New Jersey State Police (NJSP) Regional Operations & Intelligence Center (ROIC).
32. **Statewide API-NJ**-SNAP's series of developed APIs (application program interface) that allows real-time access to an agency's stored ALPR data wherever it resides.
33. **Stored Data** - Refers to all information captured by an ALPR and stored in the device's memory or in a separate data storage device or system. The term includes the recorded image of a scanned license plate and optical character recognition data, a contextual photo (i.e., a photo of the scanned vehicle and/or occupants), global positioning system ("GPS") data (when the ALPR is equipped with a GPS receiver) or other location information, and the date and time of the scan. The term applies to both alert data and non-alert data that has been captured and stored by an ALPR or in a separate data storage device or system.

I. General

- A. Agency - The law enforcement executive of each agency using an ALPR or its data shall designate an Agency ALPR Coordinator who will:
 1. Be the external point of contact for agency ALPR-related items such as information sharing and audits.
 2. Internally oversee the agency's ALPR program, including training and approving access requests (may delegate approval authority to other supervisors).
 3. Designate authorized users within the agency who can use ALPRs and access stored data (such users must complete the trainings mandated by this Directive).
 4. Currently the Cherry Hill Police Department Agency ALPR Coordinator is the Technical Services Unit Commander.
- B. ALPR and the data that are collected by these devices stored for future use shall only be used in accordance with Attorney General Directive 2022-12, the manufacturer's use manual, and this directive.
 1. ALPRs and ALPR-generated data shall only be used for bona fide public safety purposes.
- C. These procedures apply to any ALPR data that is collected by another law enforcement agency and provided to this agency or collected by this agency and provided to another law

enforcement agency.

- D. An ALPR and data generated by an ALPR shall only be used for official and legitimate law enforcement business and should be interpreted and applied to achieve the following objectives:
1. To ensure that BOLO lists that are programmed into the internal memory of an ALPR or that are compared against stored ALPR data are comprised only of license plates that are associated with specific vehicles or persons for which or whom there is a legitimate and documented law enforcement reason to identify and locate or for which there is a legitimate and documented law enforcement reason to determine the subject vehicle's past location(s) through the analysis of stored ALPR data.
 2. To ensure that data that is captured by an ALPR can only be accessed by appropriate law enforcement personnel and can only be used for legitimate, specified, and documented law enforcement purposes.
 3. To permit a thorough analysis of stored ALPR data to detect crime and protect the homeland from terrorist attack while safeguarding the personal privacy rights of motorists by ensuring that the analysis of stored ALPR data is not used as a means to disclose personal identifying information about an individual unless there is a legitimate and documented law enforcement reason for disclosing such personal information to a law enforcement officer or civilian crime analyst.
 4. To ensure that stored ALPR data is purged after a reasonable period of time so as to minimize the potential for misuse or accidental disclosure.
- E. ALPR shall be used in a consistent manner to assist department personnel in accomplishing its mission in homeland security, suspect interdiction, stolen property recovery, detection of crime, enforcement of State law and local ordinances, identification of stolen vehicles, stolen license plates, wanted and missing persons, AMBER Alert assistance, crime prevention and other traffic related matters.
- F. Information obtained through ALPR use shall only be released or disseminated in accordance with NJCJIS User Agreement protocols, applicable State Statutes, and applicable Court Rules. Unauthorized release of any information obtained through an ALPR is subject to criminal, civil, and administrative sanctions.
- G. ALPR is more than an enforcement tool. ALPR should be deployed to capture the license plates of vehicles in the area of a major crime or an area of repeated minor offenses. Captured data can be analyzed and utilized in criminal investigations or in the assignment of staffing based on empirical data.
- H. Designated supervisors shall:
1. Provide or oversee the training of all officers and civilian employees who are authorized to operate an ALPR or to access or use ALPR stored data;
 2. Review and approve requests to access and use stored ALPR data to conduct crime trend analyses and/or to access personal identifying information based upon crime trend analyses.
 3. Ensure compliance with this directive and AG Directive 2022-12.

- I. The Chief or Police or his/her designee shall designate all authorized users. No officer or civilian employee will be authorized to operate an ALPR, or access or use ALPR stored data, unless the officer or civilian employee has received training by the agency on the proper operation of these devices, and on the provisions of this directive and AG Directive 2022-12.

II. Deployment

- A. **Official Use Only** - An ALPR and the data it generates shall only be used for official and legitimate law enforcement purposes. The agency's law enforcement executive or designee must authorize deployment of each ALPR.
- B. Scanning is limited to vehicles exposed to public view - An ALPR shall only be used to scan license plates or vehicles that are exposed to public view (e.g., vehicles on a public road, street, or that are on private property but are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shopping mall or other business establishment).
- C. Sharing deployment information - The following data must be shared with the State ALPR Coordinator prior to installing or relocating a permanent fixed ALPR unit:
 1. Camera name (pursuant to convention specified by State ALPR Coordinator).
 2. Location (latitude and longitude).
 3. Survey provided by ALPR vendor, including projected size of ALPR data.
 4. When deploying or relocating a portable fixed ALPR unit, agencies must provide updated latitude and longitude data to the State ALPR Coordinator.
- D. Deconfliction - Agency ALPR Coordinators shall deconflict with the County and State ALPR Coordinator about deployment locations to avoid duplication of efforts.
- E. An ALPR shall not be deployed in the field unless the deployment has been authorized by the Chief of Police, or designated supervisor, or by the Attorney General or designee, or a County Prosecutor or designee. Such authorization may be given for repeated or continuous deployment of an ALPR (e.g., mounting the device on a particular police vehicle, or positioning the ALPR at a specific stationary location), in which event the deployment authorization shall remain in force and effect unless and until rescinded or modified by the Chief of Police or designated supervisor, or the Attorney General or County Prosecutor or designee(s).
- F. Sworn officers or civilian employees of the agency may operate an ALPR or access or use ALPR stored data only if the person has been designated as an authorized user by the Chief of Police, or by the Attorney General or designee, or a County Prosecutor, or designee, and has received training from the agency on the proper use and operation of ALPRs, the requirements of Attorney General Law Enforcement Directive 2022-12, and this directive.
- G. Personnel must ensure that the lenses are free from obstructions before operations. If safe to do so, personnel shall remove obstructions such as snow, mud, paper, etc. Under no circumstances are the camera lenses to be wiped with anything other than a clean, soft cloth.
- H. Any damage to the ALPR systems or any problems with the operation of an ALPR system

should be immediately reported to the Technical Services Unit via a support request to [REDACTED]

- I. Personnel authorized to use a mobile ALPR shall ensure that the system is operating properly and used during the officer's shift. Officers shall log-in to the system in the following manner:
 1. Depending on the vehicle the user will log into the PAGIS or Axon Fleet 3 systems.
 2. Ensure all cameras are in working order.
 3. At the end of the shift, the officer shall log out of the ALPR system until the next time the system is deployed. Users of the PAGIS system must select end shift to clear all local reads before logging out.
 4. Any authorized ALPR user who is assigned a vehicle with ALPR capabilities, must have the system activated during their shift.

III. Maintenance of Records

- A. The Agency Coordinator, or Coordinator's designee, shall maintain a written or electronic record that documents the following information:
 1. Date and time when the ALPR was deployed.
 2. Whether the ALPR was mobile, or was stationed at a fixed specified location.
 3. The identity of the operator(s).
 4. Whether ALPR data was transferred to any other database or data storage device or system.
- B. The Agency Coordinator, or Coordinator's designee shall maintain a record of all access to stored ALPR data. The agency's ALPR data record keeping system, which may be automated, shall document the following information:
 1. The date and time of access, and in the case of access to stored non-alert data, the type of access authorized (e.g., post-scan BOLO query, crime scene query, or crime trend analysis).
 2. The authorized user who accessed the stored data.
 3. Whether an automated software program was used to analyze stored data.
 4. The designated operator who reviewed and approved any disclosure of personal identifying information based upon crime trend analysis when such approval is required.
 5. The designated operator who approved any use of an automated crime trend analysis computer program that would automatically alert and disclose personal identifying information.
 6. Any other information required to be documented.

- C. All written or electronic records of ALPR activity and access to ALPR data shall be maintained by the agency for a period of three years and shall be kept in a manner that makes such records readily accessible to any person authorized by this directive to audit the agency's use of ALPRs and ALPR generated data. If an automated system is used to record any information that is required to be documented pursuant to this directive, it shall not be necessary to maintain duplicate records of any events or transactions that are documented by the automated record-keeping system.
- C. All stored data and required documentation and decisions shall be kept in a place and in a manner as to facilitate a review and audit of the agency's ALPR program by the County Prosecutor or by the Attorney General or designee(s).

IV. Content and Approval of BOLO Lists

- A. Standard for including license plate in BOLO list - A license plate number may be included in a "be on the lookout" or BOLO list (a compilation of license plates or partial plates for which a BOLO situation exists) for input into an ALPR system only if there is a legitimate and specific law enforcement reason to identify or locate that particular vehicle, or any person(s) who are reasonably believed to be associated with that vehicle. Examples of legitimate and specific reasons include but are not limited to:
 - 1. Persons who are subject to an outstanding arrest warrant.
 - 2. Missing persons.
 - 3. AMBER/SILVER alerts.
 - 4. Vehicles and/or persons involved in prior suspicious activity, such as groups of vehicles travelling together suspected of criminal activity, or subjects trying to open doors to random cars.
 - 5. Stolen vehicles.
 - 6. Vehicles reasonably believed to be involved in the commission of a crime or disorderly persons offense.
 - 7. Vehicles registered to or reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list.
 - 8. Vehicles with expired registrations or other Title 39 violations.
 - 9. Persons who are subject to a restraining order or curfew issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements.
 - 10. Persons wanted by a law enforcement agency who are of interest in a specific investigation, whether or not such persons are themselves suspected of criminal activity.
 - 11. Persons who are on any watch list issued by a state or federal agency responsible for homeland security.
- B. **Batch Downloading.** BOLO list information may be downloaded in batch form from other databases, including but not limited to the National Crime Information Center (NCIC), National Insurance Crime Bureau, United States Department of Homeland Security, and

Motor Vehicle Commission database.

C. Updating BOLO List

1. All ALPR systems must provide an Application Program Interface (API) or web service to update in real-time a BOLO list(s) through methods approved by the State ALPR Coordinator, including AMBER/SILVER alerts that remain on the list until expired or withdrawn.
2. A departmental BOLO list may be revised at any time and will be pushed to ALPR units in real time.
3. All supervisors and certain designated users have BOLO list modification access and the authority to update, add, or delete information from the departmental hotlist.
4. These users will only enter partial or full license plates into the departmental hotlist for which a BOLO situation exists and for which there is a legitimate and specific law enforcement reason to identify or locate that particular vehicle, or any person or persons who are reasonably believed to be associated with that vehicle.
5. When a partial or full license plate is entered into the departmental hotlist the user making the entry shall be sure to provide the correct license plate, the vehicle make, model and color (when known). The identity of the user making the entry and the date of the entry shall be documented in the hotlist when using the BOSS system. The user shall also provide specific, concise information as to the purpose for the entry, and the actions that should be taken in response to an alert, so as to make any user receiving the alert aware of the situation and provide them with the requisite information to respond appropriately.
6. The user entering partial or full license plate information for which a BOLO situation exists into the departmental hotlist shall also be responsible for purging the partial or full license plate from the departmental hotlist when the BOLO is satisfied or when the legitimate and specific law enforcement reason that necessitated the entry ceases to exist.
7. Users of the PAGIS software must be aware that entering a BOLO in the vehicle software is limited to their vehicle. It will be purged upon hitting end of shift in the software.

V. Actions in Response to an Immediate Alert

- A. A BOLO match with an ALPR scan may be programmed to trigger an immediate alert. The reason for including the vehicle on the BOLO list shall be disclosed to the officer who will react to an immediate alert. The officer should determine whether the alert has been designated as a non-encounter alert (meaning officers should not encounter the vehicle) and, if so, follow any instructions included in the alert for notifying the originating agency.
- B. When officers operating a vehicle equipped with ALPR receive an immediate alert, the officer shall take such action in response to the alert as is appropriate in the circumstances. Officer(s) alerted to the fact that an observed motor vehicle's license plate is on the BOLO list may be required to make a reasonable effort to confirm that a wanted person is actually in the vehicle before the officer would have a lawful basis to stop the vehicle. (State v. Parks, 288 N.J. Super. 407 App. Div. 1996). Police do not have reasonable suspicion to justify a stop based on a computer check that shows that the operator's license of the registered owner of the

vehicle is suspended unless the driver generally matches the owner's physical description (e.g., age and gender).

- C. An officer reacting to an immediate alert shall consult the database to determine the reason why the vehicle had been placed on the BOLO list and whether the alert has been designated as a non-encounter alert. In the event of a non-encounter alert, the officer shall follow any instructions included in the alert for notifying the law enforcement or homeland security agency that had put out the BOLO.
- D. Due to the delayed nature of the updating of NCIC, DMV, and Federal databases, confirmation of alerts based on this data shall be confirmed via an MDC or dispatch to ensure the alert is still valid before taking any action.

VI. Storage and Security of ALPR Data

- A. Storage of ALPR data. All ALPR data shall be stored securely and maintained electronically with access restricted to authorized users. ALPR data shall be the property of the agency and not any ALPR vendor. Agencies may jointly store their ALPR data. Commercially obtained ALPR data shall not be co-mingled with law enforcement data. Data being used in an investigatory process shall be maintained in accordance with the agency's evidence or records management procedures.
- B. Stored ALPR data access records. Agencies that store ALPR data shall maintain an automated record-keeping of all access to stored ALPR data (in the case of county storage, the county may keep access records instead), including the following:
 - 1. Date and time of access, and for non-alert data, the justification for access.
 - 2. Authorized accessor name.
 - 3. Whether an automated software program was used to analyze the data.
 - 4. Designated supervisor who approved disclosure of personal identifying information based upon crime trend analysis.
 - 5. Instances of testing or troubleshooting an ALPR system.
 - 6. Any other information required to be documented under this directive.
- C. All ALPR stored data shall be kept in a secure data storage system with access restricted to authorized persons. Access to this stored data shall be limited to the purposes described in Section IX. To comply with this mandate data warehoused by the department from PAGIS systems will be secured in the department's BOSS server. All AXON Fleet 3 or Flock data is secured by the vendors in their Government Cloud approved platforms. Access based roles shall be set in all systems based on the principle of least privilege access.
- D. Stored ALPR data shall be maintained electronically in such a manner as to distinguish alert data from non-alert data so as to ensure that access to and use of non-alert data and any disclosure of personal identifying information resulting from the analysis of non-alert data occurs only as authorized pursuant to Section IX. Positive alert data may, as appropriate, be transferred to the appropriate active investigation file and if appropriate be placed into evidence in accordance with the agency's evidence or records management procedures.

VII. Retention Period and Purging of Stored Data

- A. ALPR stored data shall be retained for a period of three years, after which, the data shall be purged from the agency's data storage device or system. The system is designed to automatically purge on the first day, after the third year of retention.
- B. Any ALPR data transferred to another agency shall indicate the date on which the data had been collected by the ALPR so that the receiving agency may comply with the three-year retention and purging schedule established in AG Directive 2022-12.

VIII. Limitations on Access to and Use of Stored ALPR Data

- A. Authorized users may access and use stored ALPR Alert Data as part of an active investigation or for any other legitimate law enforcement purpose including, but not limited to a BOLO query, a crime scene query, or crime trend analysis.
 - 1. A record shall be made of all access to ALPR data, which may be an automated record that documents the date of access and the identity of the authorized user and for non-alert data the record should include the justification for access. Once stored data has been accessed and transferred to an investigation file by an authorized user, it shall not be necessary after that to document further access or use of that data pursuant to New Jersey Attorney General Law Enforcement Directive 2022-12.
 - 2. An authorized user does not need to obtain approval from the Chief of Police or designated supervisor for each occasion on which he or she accesses and uses stored ALPR data. Once positive alert data has been accessed and transferred to an investigation file, it shall not be necessary thereafter to document further access or use of that data pursuant to this directive.
- B. Access to and use of stored Non-Alert ALPR Data is limited to the following three purposes:
 - 1. A BOLO query.
 - 2. A crime-scene query.
 - 3. Crime trend analysis (system test and troubleshooting are also acceptable purposes).
- C. An authorized user does not need to obtain approval from the Chief of Police or a designated supervisor for each occasion on which he or she accesses and uses stored non-alert data pursuant to this directive.
- D. **BOLO Query** - Agencies may compare a BOLO list against stored non-alert data where the results of the query might reasonably lead to the discovery of evidence or information relevant to any active investigation or ongoing law enforcement operation or where the subject vehicle might subsequently be placed on an active BOLO list (for example, may review data to determine whether a specific vehicle was present at the time and place where the ALPR data was initially scanned to check an alibi defense or to develop lead information for the purpose of locating a specified vehicle or person; or to determine whether a vehicle that was only recently added to a BOLO list had been previously observed in the jurisdiction before being placed on the list).
- E. **Crime Scene Query** - Agencies may access and use stored non-alert data where such access might reasonably lead to the discovery of evidence or information relevant to the investigation of a specific criminal event (i.e., incident that would constitute an indictable crime

under New Jersey law). Such queries may not be conducted to review data based on general crime patterns (e.g., to identify persons traveling in or around a “high crime area”). A record shall be kept of the specific crime(s) justifying the query, including the crime date and location.

- F. **Crime Trend Analysis** - Agencies may access and use stored non-alert data where such access, which may be automated, might reasonably lead to the discovery of evidence or information relevant to an investigation that is not related to a specific criminal event. Such access must be approved by the Agency ALPR Coordinator or their designee.

Crime trend analysis shall not result in the disclosure of personal identifying information (such as name, address, SSN, vehicle operator's license number) to an authorized user or any other person unless (a) there exist “specific and articulable facts that warrant further investigation” of possible criminal or terrorist activity by the driver or occupants of a specific vehicle and access has been approved by a designated supervisor; or (b) disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena.

Any crime trend analysis shall document:

1. The nature and purpose of the crime trend analysis.
 2. The authorized users who accessed stored non-alert data.
 3. The designated supervisor who approved access.
 4. Where personal identifying information was disclosed, (a) the specific and articulable facts that warrant further investigation and (b) the designated supervisor who approved the disclosure of personal identifying information; or, where applicable, the fact that a grand jury subpoena authorized access to personal identifying information.
- G. For the purposes of this Section, the specific and articulable facts that warrant a further investigation standard required for the disclosure of personal identifiers, based upon crime trend analysis of stored non-alert data, is intended to be comparable to the specific and articulable facts that warrant heightened caution standard developed by the New Jersey Supreme Court in *State v. Smith*, 134 N.J. 599, 616-19 (1994) (establishing the level of individualized suspicion required before an officer may order a passenger to exit a motor vehicle stopped for a traffic violation).

IX. Shared Law Enforcement Access to Stored ALPR Data

- A. **Statewide API** - the State ALPR Coordinator shall implement a “Statewide API” (application program interface) that allows access to stored ALPR data across agencies, and specify the method by which all ALPRs used by New Jersey agencies must provide real-time access to ALPR data through the API. Agencies may also share data regionally with other New Jersey agencies pursuant to the mandates of this Directive, and ALPR data collected by a private entity that has entered into an agreement with New Jersey law enforcement can be shared with New Jersey agencies. All ALPRs must make data available to the Statewide API by the effective date of this Directive, and subsequent ALPRs must do so within 45 days of deployment. ALPR systems must be programmed to capture data parameters and meet minimum requirements for accuracy and performance as specified by the State ALPR Coordinator.

- B. Sharing with agencies not covered by Attorney General Law Enforcement Directive 2022-12. An agency may enter into a written agreement to share ALPR data with, or receive data from, a law enforcement agency outside of New Jersey or otherwise not covered by this Directive with the approval of the State ALPR Coordinator. Only federally recognized law enforcement agencies may receive access to a New Jersey agency's ALPR data. The State ALPR Coordinator may agree to share ALPR data with a law enforcement agency outside of New Jersey if the out of state agency agrees in writing to use the data only for documented, legitimate law enforcement purposes and to follow other restrictions required by the State ALPR Coordinator in order to achieve the objectives of this Directive. Private entities may provide ALPR data to New Jersey agencies but cannot receive law enforcement-owned ALPR data.
- C. Stored ALPR data may be combined with ALPR data collected by two or more law enforcement agencies (e.g., collection of stored data by the State Police Regional Operations Intelligence Center); provided that such aggregated data shall only be retained, accessed, and used in accordance with the provisions of AG Directive 2022- 12 and this directive.
- D. When ALPR data is made accessible to or otherwise shared with or transferred to another law enforcement agency, the ALPR Coordinator shall document the identity of the other agency and the specific officer(s) or civilian employee(s) of that agency who were provided the information and ensure that the other agency has an approved ALPR policy. In order to comply with this mandate, the authorized user should document the release of ALPR data in an "Assist Agency" offense report.

X. Discovery

- A. Criminal investigatory records - Stored ALPR data shall be treated as "criminal investigatory records" within the meaning of N.J.S.A. 47:1A- 1 et seq., and shall not be shared with or provided to any person, entity, or government agency other than a law enforcement agency, unless a subpoena or court order authorizes such disclosure or unless such disclosure is required by court rules governing discovery in criminal matters.
 - 1. Any agency receiving a subpoena or court order for the disclosure of ALPR data shall, before complying with the subpoena or court order, provide notice to the County Prosecutor (or Director of the Division of Criminal Justice (DCJ)).
- B. Release of ALPR data. If ALPR data is accessed as part of an investigation—including but not limited to a BOLO query, a crime scene query, or crime trend analysis—a record of the access, which may be automated, and corresponding data shall be included in the agency's investigative file (electronic or physical). If the investigation results in criminal charges, the ALPR records shall be turned over in discovery pursuant to applicable court rules and case law his or her sole discretion deems appropriate to ensure compliance with this Directive.

XI. Compliance

- A. **Establishing a policy.** Agencies that possess or use an ALPR or its data shall establish or conform existing standing operating procedures, directives, or orders that govern ALPRs and stored ALPR data consistent with this Directive before the Directive takes effect (ninety days after issuance). The law enforcement executive shall provide a copy of the agency's ALPR policy to the County Prosecutor (or DCJ Director) and County and State ALPR Coordinator at or before the time of promulgation, including any subsequent policy amendments.

- B. The County ALPR Coordinator and Co-Coordinators shall collect all Agency ALPR policies and forward to the State ALPR Coordinator.
- C. **Violations**-Any employee of the Cherry Hill Police Department who violates this policy, AG directive 2022-12, or applicable law, shall be subject to discipline.
- D. All significant violations of this Directive or agency policy, including but not limited to unauthorized access or use of ALPR stored data, must be reported to the County Prosecutor (or DCJ Director) and County and State ALPR Coordinator upon discovery. Unless the County Prosecutor or DCJ elects to conduct or oversee the investigation of the violation, such notification of the violation shall be followed up with a report, approved by the law enforcement executive and with notification to the State ALPR Coordinator, explaining to the County Prosecutor or to the Director, the circumstances of the violation, and the steps that are being taken to prevent future similar violations.
- E. Any complaints about an agency's ALPR program made by any citizen or entity shall be forwarded to the appropriate County Prosecutor (or DCJ Director), for appropriate review and handling, as well as notification to the County and State ALPR Coordinator. The County Prosecutor or Director may conduct an investigation or direct the agency that is the subject of the complaint to conduct an investigation and report back to the County Prosecutor or DCJ with notification to the State ALPR Coordinator.
- F. The County ALPR Coordinator shall maintain a record of any reports of significant violations and citizen complaints to include:
 - 1. Those made directly to the County Prosecutor's Office;
 - 2. Those made directly to any law enforcement agency in the respective county; and
 - 3. Those made directly to any agency falling under the County ALPR Coordinator's responsibility.
- G. **Audits**-By January 31 each year, the Agency ALPR Coordinator shall perform an audit of their agency's ALPR program and provide it to the County and State ALPR Coordinator. That audit shall certify the following:
 - 1. Agency has an ALPR policy in place;
 - 2. Only authorized users have accessed ALPR data;
 - 3. Date of each authorized user's last ALPR training;
 - 4. That a random survey of ALPR accesses revealed no misuse; and
 - 5. A description of any known significant violations and citizen complaints and whether they have been forwarded to the County Prosecutor or DCJ Director.

Once the Agency ALPR Coordinator submits their audit to their County ALPR Coordinator by January 31 each year, the County Coordinator must forward it to the State ALPR Coordinator.

The County ALPR Coordinator or State ALPR Coordinator may conduct an audit of an agency's ALPR program at any time.

- H. **Training.** The State ALPR Coordinator shall design and disseminate training on ALPR technology—including the application of the New Jersey Attorney General Law Enforcement Directive 2022-12 and privacy and security considerations generally—that shall be a prerequisite for an individual being designated an authorized user under Directive 2022-12. Authorized users must complete refresher training every two years, as determined by the State ALPR Coordinator.

XII. Sanctions for Non-Compliance

- A. If the Attorney General, County Prosecutor or designee has reason to believe that a law enforcement agency or officer or civilian employee is not complying with or adequately enforcing the provisions of New Jersey Attorney General's Directive 2022-12, the Attorney General may temporarily or permanently suspend or revoke the authority of the department, or any officer or civilian employee, to operate an ALPR, or to gain access to or use ALPR stored data. The Attorney General or designee may initiate disciplinary proceedings and may take such other actions as the Attorney General in his or her sole discretion deems appropriate to ensure compliance with this Directive.

XIII. Authority of Attorney General to Grant Exemptions or Special Use Authorizations

- A. **Attorney General exemptions.** ALPRs, and all ALPR stored data, shall only be used and accessed as authorized by this Directive. However, the Attorney General or their designee may authorize the specific use of an ALPR or the data it generates that is not expressly authorized by this Directive. Any request by a department to use an ALPR or ALPR-generated data for a purpose or in a manner not authorized by this Directive shall be made to the Attorney General or their designee through the DCJ Director. Such requests shall be made in writing unless the circumstances are exigent, in which case approval or denial may be given orally and memorialized in writing as soon thereafter as is practicable.

XIV. Security Policy: Cybersecurity Best Practices, Supply Chain Risk Management, ALPR Configuration Management, and Physical Security

A. Cybersecurity Best Practices

As per the New Jersey Statewide ALPR Coordinator, agencies shall implement cybersecurity best practices and controls that reasonably conform to the most recent version of one or more of the following industry-recognized cybersecurity control families:

1. the New Jersey Statewide Information Security Manual;
2. the Center for Internet Security Critical Security Controls for Effective Cyber Defense; or
3. the Criminal Justice Information Security Policy

ALPR security standards must specifically address supply chain risk management, configuration management, and physical access control.

B. Supply Chain Risk Management

Agencies shall implement Supply Chain Risk Management (SCRM) processes to help protect system components, products, and services that are part of ALPR systems and infrastructures. SCRM controls help ensure that security and privacy requirements, threats,

and other concerns are addressed throughout the ALPR system's life cycle and the national and international supply chains.

To mitigate supply chain risks, agencies shall comply with Section 889 of Public Law 115-232, the John S. McCain National Defense Authorization Act, and 2 CFR 200.216, which prohibits agencies from obligating or expending federal grant funds to:

1. Procure or obtain;
2. Extend or renew a contract to procure or obtain; or
3. Enter into a contract (or extend or renew a contract) to procure or obtain systems, equipment or services that include components from the following companies:
 - a. Huawei Technologies Company,
 - b. ZTE Corporation,
 - c. Hytera Communications Corporation,
 - d. Hangzhou Hikvision Digital Technology Company,
 - e. Dahua Technology Company
 - f. Any of subsidiaries or affiliates of these companies.

Currently the only authorized ALPR vendors used by the Cherry Hill Police Department are Neology (PIPS, BOSS, PAGIS) Axon, and Flock Safety. Any changes or updates to these systems will be vetted by the Cherry Hill Police Technical Services Unit.

Supplemental Guidance: An assessment and review of supplier risk includes security and supply chain risk management processes, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors.

Agencies can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits.

Agencies should review the US Department of Commerce Bureau of Industry and Security Lists of Parties of Concern, the International Trade Association Consolidated Screening List, and the National Defense Authorization Act (NDAA) Section 889 prior to contracting with a supplier. In general, the NJ Office of Homeland Security and Preparedness prohibits agencies from purchasing systems, system components, and services from companies on these lists due to threats they pose to the State and/or Nation. Agencies should contact the NJCCIC for further guidance.

C. *ALPR Configuration Management*

1. Agencies shall establish, document, and implement security configuration settings of ALPR systems that reflect the most restrictive mode consistent with their operational requirement. Each ALPR system and component shall be hardened to provide only necessary ports, protocols, and services to meet business needs and

have in place supporting technical controls such as: Endpoint Detection and Response (EDR) software and security event logging, as feasible.

2. Supplemental Guidance: Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections.
3. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors. Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency.
4. Agencies may refer to the following resources for common security configuration settings.
 - a). Center for Internet Security (CIS) benchmarks: <https://benchmarks.cisecurity.org/downloads/benchmarks/>
 - b). United States government Configuration Baselines: <https://csrc.nist.gov/projects/united-states-government-configuration-baseline>
 - c). NIST recommended configurations and checklists: <http://checklists.nist.gov/>
 - d). National Security Agency (NSA) configuration guides: <https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/index.cfm>

D. ***Physical Security***

1. Establish physical controls and procedures that limit access to ALPR systems, equipment, and the respective operating environments to only authorized individuals.

E. ***Other Security Best Practices***

1. All ALPR technology hardware and software installation and use must comply with security controls set forth in GO 96-06 Security of Computer Based Systems.

flock safety

FLOCK GROUP INC. SERVICES AGREEMENT ORDER FORM

This Order Form together with the Terms (as defined herein) describe the relationship between Flock Group Inc. ("Flock") and the customer identified below ("Customer") (each of Flock and Customer, a "Party"). This order form ("Order Form") hereby incorporates and includes the "GOVERNMENT AGENCY CUSTOMER AGREEMENT" attached (the "Terms") which describe and set forth the general legal terms governing the relationship (collectively, the "Agreement"). The Terms contain, among other things, warranty disclaimers, liability limitations and use limitations.

The Agreement will become effective when this Order Form is executed by both Parties (the "Effective Date").

Customer: NJ - Cherry Hill PD

Address: 820 Mercer St
Cherry Hill, New Jersey 8002

Contact Name: Paul Campanna

Phone: 856-488-7828

E-Mail:
pcampana@cherryhillpolice.com

Billing Contact:

Expected Payment Method:

(if different than above)

Initial Term: 24.00

Renewal Term: 24 Months

Pilot period: First 60 days of Initial Term; option to cancel contract at no cost. Initial Term invoice due after Pilot period.

Billing Term: Annual payment due Net 30 per terms and conditions

Name	Price	QTY	Subtotal
Professional Services - Falcon, Standard Implementation	\$350.00	10.00	\$3,500.00
Falcon Camera	\$2,500.00	10.00	\$25,000.00
Flock Safety Advanced Search <25 Falcons	\$2,500.00	1.00	\$2,500.00
Extended data retention	\$250.00	10.00	\$2,500.00

(Includes one-time fees)

Year 1 Total: \$33,500.00

Recurring Total: \$30,000.00

Flock Group Inc.

Order Form

This proposal expires in 30 days.

flock safety

By executing this Order Form, Customer represents and warrants that it has read and agrees all of the terms and conditions contained in the Terms attached. The Parties have executed this Agreement as of the dates set forth below.

Flock Group Inc

By:

DocuSigned by:

Alex Latraverse

D7432021662B461...

Name: Alex Latraverse

Title: Chief Revenue Officer

Date: 5/10/2022

Customer:

By:

Name:

ROBERT KEMPFF

Title:

CHIEF OF POLICE

Date:

5/09/2022

flock safety

GOVERNMENT AGENCY AGREEMENT

This Government Agency Agreement (this “**Agreement**”) is entered into by and between Flock Group, Inc. with a place of business at 1170 Howell Mill Rd NW Suite 210, Atlanta, GA 30318 (“**Flock**”) and the police department or government agency identified in the signature block of the order form (“**Agency**”) (each a “**Party**,” and together, the “**Parties**”).

RECITALS

WHEREAS, Flock offers a software and hardware solution for automatic license plate detection through Flock’s technology platform (the “**Flock Service**”), and upon detection, the Flock Services are capable of capturing audio, image, and recordings data of suspected vehicles (“**Footage**”) and can provide notifications to Agency upon the instructions of Non-Agency End User (“**Notifications**”);

WHEREAS, Agency desires access to the Flock Service on existing cameras, provided by Agency, or Flock provided Hardware (as defined below) in order to create, view, search and archive Footage and receive Notifications, including those from non-Agency users of the Flock Service (where there is an investigative or bona fide lawful purpose) such as schools, neighborhood homeowners associations, businesses, and individual users;

WHEREAS, Flock deletes all Footage on a rolling thirty (30) day basis, Agency is responsible for extracting, downloading and archiving Footage from the Flock System on its own storage devices for auditing for prosecutorial/administrative purposes; and

WHEREAS, Flock desires to provide Agency the Flock Service and any access thereto, subject to the terms and conditions of this Agreement, solely for the awareness, prevention, and prosecution of crime, bona fide investigations by police departments, and archiving for evidence gathering (“**Purpose**”).

AGREEMENT

NOW, THEREFORE, Flock and Agency agree as follows and further agree to incorporate the Recitals into this Agreement.

1. DEFINITIONS

Certain capitalized terms, not otherwise defined herein, have the meanings set forth or cross-referenced in this Section 1.

1.1 "*Agency Data*" will mean the data, media and content provided by Agency through the Services. For the avoidance of doubt, the Agency Data will include the Footage.

1.2. "*Agency Hardware*" shall mean the third-party camera owned or provided by Agency and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Services. The term "*Agency Hardware*" excludes the Embedded Software

1.3 "*Authorized End User(s)*" shall mean any individual employees, agents, or contractors of Agency accessing or using the Services through the Web Interface, under the rights granted to Agency pursuant to this Agreement.

1.4 "*Documentation*" will mean text and/or graphical documentation, whether in electronic or printed format, that describe the features, functions and operation of the Services which are provided by Flock to Agency in accordance with the terms of this Agreement.

1.5 "*Embedded Software*" will mean the software and/or firmware embedded or preinstalled on the Agency Hardware.

1.6 "*Flock IP*" will mean the Services, the Documentation, the Embedded Software, the Installation Services, and any and all intellectual property therein or otherwise provided to Agency and/or its Authorized End Users in connection with the foregoing.

1.7 "*Footage*" means still images captured by the Agency Hardware in the course of and provided via the Services.

1.8 "*Hardware*" or "*Flock Hardware*" shall mean the Flock cameras or device, pole, clamps, solar panel, installation components, and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Flock Services. The term "*Hardware*" excludes the Embedded Software.

1.9 "*Implementation Fee(s)*" means the monetary fees associated with the Installation Services, as defined in Section 1.10 below.

1.10 "*Installation Services*" means the services provided by Flock including any applicable installation of Embedded Software on Agency Hardware.

1.11 "*Non-Agency End User(s)*" shall mean any individual, entity, or derivative therefrom, authorized to use the Services through the Web Interface, under the rights granted to pursuant to the terms (or to those materially similar) of this Agreement.

1.12 "*Services*" or "*Flock Services*" means the provision, via the Web Interface, of Flock's software application for automatic license plate detection, searching image records, and sharing Footage.

1.13 "*Support Services*" shall mean Monitoring Services, as defined in Section 2.9 below.

1.14 "*Unit(s)*" shall mean the Agency Hardware together with the Embedded Software.

1.15 "*Usage Fee*" means the subscription fees to be paid by the Agency for ongoing access to Services.

1.16 "*Web Interface*" means the website(s) or application(s) through which Agency and its Authorized End Users can access the Services in accordance with the terms of this Agreement.

2. SERVICES AND SUPPORT

2.1 **Provision of Access.** Subject to the terms of this Agreement, Flock hereby grants to Agency a non-exclusive, non-transferable right to access the features and functions of the Services via the Web Interface during the Service Term (as defined in Section 6.1 below), solely for the Authorized End Users. The Footage will be available for

Agency's designated administrator, listed on the order form, and any Authorized End Users to access via the Web Interface for thirty (30) days. Authorized End Users will be required to sign up for an account and select a password and username ("*User ID*"). Flock will also provide Agency with the Documentation to be used in accessing and using the Services. Agency shall be responsible for all acts and omissions of Authorized End Users, and any act or omission by an Authorized End User which, if undertaken by Agency, would constitute a breach of this Agreement, shall be deemed a breach of this Agreement by Agency. Agency shall undertake reasonable efforts to make all Authorized End Users aware of the provisions of this Agreement as applicable to such Authorized End User's use of the Services, and shall cause Authorized End Users to comply with such provisions. Flock may use the services of one or more third parties to deliver any part of the Services, including without limitation using a third party to host the Web Interface which makes the Services available to Agency and Authorized End Users. Warranties provided by said third party service providers are the agency's sole and exclusive remedy and flock's sole and exclusive liability with regard to such third-party services, including without limitation hosting the web interface. Agency agrees to comply with any acceptable use policies and other terms of any third-party service provider that are provided or otherwise made available to Agency from time to time.

2.2 Embedded Software License. Subject to all terms of this Agreement, Flock grants Agency a limited, non-exclusive, non-transferable, non-sublicensable (except to the Authorized End Users), revocable right to use the Embedded Software as installed on the Hardware or Agency Hardware; in each case, solely as necessary for Agency to use the Services.

2.3 Documentation License. Subject to the terms of this Agreement, Flock hereby grants to Agency a non-exclusive, non-transferable right and license to use the Documentation during the Service Term to Agency's in connection with its use of the Services as contemplated herein, and under Section 2.4 below.

2.4 Usage Restrictions.

a. Flock IP. The purpose for usage of the Unit, Documentation, Services, support, and Flock IP are solely to facilitate gathering evidence that could be used in a lawful criminal investigation by the appropriate government agency and not for tracking activities that the system is not designed to capture ("*Permitted Purpose*"). Agency will not, and will not permit any Authorized End Users to, (i) copy or duplicate any of the Flock IP; (ii) decompile, disassemble, reverse engineer or otherwise attempt to obtain or perceive the source code from which any software component of any of the Flock IP is compiled or interpreted, or apply any other process or procedure to derive the source code of any software included in the Flock IP, or attempt to do any of the foregoing, and Agency acknowledges that nothing in this Agreement will be construed to grant Agency any right to obtain or use such source code; (iii) modify, alter, tamper with or repair any of the Flock IP, or create any derivative product from any of the foregoing, or attempt to do any of the foregoing, except with the prior written consent of Flock; (iv) interfere or attempt to interfere in any manner with the functionality or proper working of any of the Flock IP; (v) remove, obscure, or alter any notice of any intellectual property or proprietary right appearing on or contained within any of the Services or Flock IP; (vi) use the Services, support, Unit, Documentation or the Flock IP for anything other than

the Permitted Purpose; or (vii) assign, sublicense, sell, resell, lease, rent or otherwise transfer or convey, or pledge as security or otherwise encumber, Agency's rights under Sections 2.1, 2.2, or 2.3.

b. Flock Hardware. Agency understands that all Flock Hardware is owned exclusively by Flock, and that title to any Flock Hardware does not pass to Agency upon execution of this Agreement. Agency is not permitted to remove, reposition, re-install, tamper with, alter, adjust or otherwise take possession or control of Flock Hardware. Notwithstanding the notice and cure period set for in Section 6.3, Agency agrees and understands that in the event Agency is found to engage in any of the restricted actions of this Section 2.4(b), all warranties herein shall be null and void, and this Agreement shall be subject to immediate termination (without opportunity to cure) for material breach by Agency.

2.5 Retained Rights; Ownership. As between the Parties, subject to the rights granted in this Agreement, Flock and its licensors retain all right, title and interest in and to the Flock IP and its components, and Agency acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Agreement. Agency further acknowledges that Flock retains the right to use the foregoing for any purpose in Flock's sole discretion. There are no implied rights.

2.6 Suspension. Notwithstanding anything to the contrary in this Agreement, Flock may temporarily suspend Agency's and any Authorized End User's access to any portion or all of the Flock IP or Flock Hardware if (i) Flock reasonably determines that (a) there is a threat or attack on any of the Flock IP; (b) Agency's or any Authorized End User's use of the Flock IP disrupts or poses a security risk to the Flock IP or any other Agency or vendor of Flock; (c) Agency or any Authorized End User is/are using the Flock IP for fraudulent or illegal activities; (d) Flock's provision of the Services to Agency or any Authorized End User is prohibited by applicable law; (e) any vendor of Flock has suspended or terminated Flock's access to or use of any third party services or products required to enable Agency to access the Flock IP; or (f) Agency has violated any term of this provision, including, but not limited to, utilizing the Services for anything other than the Permitted Purpose (each such suspension, in accordance with this Section 2.6, a "*Service Suspension*"). Flock will make commercially reasonable efforts, circumstances permitting, to provide written notice of any Service Suspension to Agency (including notices sent to Flock's registered email address) and to provide updates regarding resumption of access to the Flock IP following any Service Suspension. Flock will use commercially reasonable efforts to resume providing access to the Service as soon as reasonably possible after the event giving rise to the Service Suspension is cured. Flock will have no liability for any damage, liabilities, losses (including any loss of data or profits) or any other consequences that Agency or any Authorized End User may incur as a result of a Service Suspension. To the extent that the Service Suspension is not caused by Agency's direct actions or by the actions of parties associated with the Agency, the expiration of the Term will be tolled by the duration of any suspension (for any continuous suspension lasting at least one full day) prorated for the proportion of cameras on the Agency's account that have been impacted.

2.7 Installation Services.

2.7.1 Designated Locations. For installation of Flock Hardware, prior to performing the physical installation of the Units, Flock shall advise Agency on the location and positioning of the Units for optimal license plate image

capture, as conditions and location allow. Flock may consider input from Agency regarding location, position and angle of the Units (each Unit location so designated by Agency, a “*Designated Location*”). Flock shall have final discretion on location of Units. Flock shall have no liability to Agency resulting from any poor performance, functionality or Footage resulting from or otherwise relating to the Designated Locations or delay in installation due to Agency’s delay in confirming Designated Locations, in ordering and/or having the Designated Location ready for installation including having all electrical work preinstalled and permits ready, if necessary. The deployment plan will confirm the Designated Location. After installation, any subsequent changes to the deployment plan (“*Reinstalls*”) will incur a charge for Flock’s then-current list price for Reinstalls, as listed in the then-current Reinstall Policy (available at <https://www.flocksafety.com/reinstall-fee-schedule>) and any equipment charges. These changes include but are not limited to camera re-positioning, adjusting of camera mounting, re-angling, removing foliage, camera replacement, changes to heights of poles, regardless of whether the need for Reinstalls related to vandalism, weather, theft, lack of criminal activity in view, and the like. Flock Safety shall have full discretion on decision to reinstall Flock Hardware.

2.7.2 Agency Installation Obligations. Agency agrees to allow Flock and its agents reasonable access in and near the Designated Locations at all reasonable times upon reasonable notice for the purpose of performing the installation work. Although the Units are designed to utilize solar power, certain Designated Locations may require a reliable source of 120V AC power, as described in the deployment plan. In the event adequate solar exposure is not available Agency is solely responsible for providing a reliable source of 120V AC power to the Units, if necessary. Additionally, Agency is solely responsible for (i) any permits or associated costs, and managing the permitting process of installation of cameras or AC power; (ii) any federal, state or local taxes including property, license, privilege, sales, use, excise, gross receipts or other similar taxes which may now or hereafter become applicable to, measured by or imposed upon or with respect to the installation of the Hardware, its use (excluding tax exempt entities), or (iii) any other supplementary cost for services performed in connection with installation of the Hardware, including but not limited to contractor licensing, engineered drawings, rental of specialized equipment or vehicles, third-party personnel (i.e. Traffic Control Officers, Electricians, State DOT-approved poles, etc., if necessary), such costs to be approved by the Agency (“*Agency Installation Obligations*”). In the event that a Designated Location for a Unit requires permits, Flock will provide the Agency with a temporary alternate location for installation pending the permitting process. Once the required permits are obtained, Flock will relocate the Units from the temporary alternate location to the permitted location at no additional cost. Flock will provide options to supply power at each Designated Location. If Agency refuses alternative power supply options, Agency agrees and understands that Agency will not be subject to any reimbursement, tolling, or credit for any suspension period of Flock Services due to low solar. Flock will make all reasonable efforts within their control to minimize suspension of Flock Services. Any fees payable to Flock exclude the foregoing. Without being obligated or taking any responsibility for the foregoing, Flock may pay and invoice related costs to Agency if Agency did not address them prior to the execution of this Agreement or a third party requires Flock to pay. Agency represents and warrants that it has all necessary right title and authority and

hereby authorizes Flock to install the Hardware at the Designated Locations and to make any necessary inspections or tests in connection with such installation. Flock is not responsible for installation of Agency Hardware.

2.7.3 Flock's Obligations. Installation of any Flock Hardware shall be installed in a workmanlike manner in accordance with Flock's standard installation procedures, and the installation will be completed within a reasonable time from the time that the Designated Locations are confirmed. Following the initial installation of the Hardware and any subsequent Reinstalls or maintenance operations, Flock's obligation to perform installation work shall cease; however, for the sole purpose of validating installation, Flock will continue to monitor the performance of the Units for the length of the Term and will receive access to the Footage for a period of three (3) business days after the initial installation in order to monitor performance and provide any necessary maintenance solely as a measure of quality control. Agency understands and agrees that the Flock Services will not function without the Hardware. Labor may be provided by Flock or a third party. Flock is not obligated to install, reinstall, or provide physical maintenance to Agency Hardware.

2.7.4 Security Interest. Flock Hardware shall remain the personal property of Flock and will be removed upon the natural expiration of this Agreement at no additional cost to Agency. Agency shall not perform any acts which would interfere with the retention of title of the Hardware by Flock. Should Agency default on any payment of the Flock Services, Flock may remove Hardware at Flock's discretion. Such removal, if made by Flock, shall not be deemed a waiver of Flock's rights to any damages Flock may sustain as a result of Agency's default and Flock shall have the right to enforce any other legal remedy or right.

2.8 Hazardous Conditions. Unless otherwise stated in the Agreement, Flock's price for its services under this Agreement does not contemplate work in any areas that contain hazardous materials, or other hazardous conditions, including, without limit, asbestos, lead, toxic or flammable substances. In the event any such hazardous materials are discovered in the designated locations in which Flock is to perform services under this Agreement, Flock shall have the right to cease work immediately in the area affected until such materials are removed or rendered harmless.

2.9 Support Services. Subject to the payment of fees, Flock shall monitor the performance and functionality of Flock Services and may, from time to time, advise Agency on changes to the Flock Services, Installation Services, or the Designated Locations which may improve the performance or functionality of the Services or may improve the quality of the Footage. The work, its timing, and the fees payable relating to such work shall be agreed by the Parties prior to any alterations to or changes of the Services or the Designated Locations ("*Monitoring Services*"). Subject to the terms hereof, Flock will provide Agency with reasonable technical and on-site support and maintenance services ("*On-Site Services*") in-person or by email at support@flocksafety.com. Flock will use commercially reasonable efforts to respond to requests for support.

2.10 Special Terms. From time to time, Flock may offer certain "Special Terms" related to guarantees, service and support which are indicated in the proposal and on the order form and will become part of this Agreement, upon

Agency's consent. To the extent that any terms of this agreement are inconsistent or conflict with the Special Terms, the Special Terms shall control.

2.10 Changes to Platform. Flock may, in its sole discretion, make any changes to any system or platform that it deems necessary or useful to (i) maintain or enhance (a) the quality or delivery of Flock's products or services to its Agency s, (b) the competitive strength of, or market for, Flock's products or services, (c) such platform or system's cost efficiency or performance, or (ii) to comply with applicable law.

3. RESTRICTIONS AND RESPONSIBILITIES

3.1 Agency Obligations. Flock will assist Agency end-users in the creation of a User ID. Agency agrees to provide Flock with accurate, complete, and updated registration information. Agency may not select as its User ID a name that Agency does not have the right to use, or another person's name with the intent to impersonate that person. Agency may not transfer its account to anyone else without prior written permission of Flock. Agency will not share its account or password with anyone, and must protect the security of its account and password. Agency is responsible for any activity associated with its account. Agency shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Services. Agency will, at its own expense, provide assistance to Flock, including, but not limited to, by means of access to, and use of, Agency facilities, as well as by means of assistance from Agency personnel, to the limited extent any of the foregoing may be reasonably necessary to enable Flock to perform its obligations hereunder, including, without limitation, any obligations with respect to Support Services or any Installation Services.

3.2 Agency Representations and Warranties. Agency represents, covenants, and warrants that Agency will use the Services only in compliance with this Agreement and all applicable laws and regulations, including but not limited to any laws relating to the recording or sharing of video, photo, or audio content. Although Flock has no obligation to monitor Agency's use of the Services, Flock may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of the foregoing.

4. CONFIDENTIALITY; AGENCY DATA

4.1 Confidentiality. To the extent allowable by applicable FOIA and state-specific Public Records Acts, each Party (the "*Receiving Party*") understands that the other Party (the "*Disclosing Party*") has disclosed or may disclose business, technical or financial information relating to the Disclosing Party's business (hereinafter referred to as "*Proprietary Information*" of the Disclosing Party). Proprietary Information of Flock includes non-public information regarding features, functionality and performance of the Services. Proprietary Information of Agency includes non-public data provided by Agency to Flock or collected by Flock via the Unit, including the Footage, to enable the provision of the Services, which includes but is not limited to geolocation information and environmental data collected by sensors built into the Units ("*Agency Data*"). The Receiving Party agrees: (i) to take the same security precautions to protect against disclosure or unauthorized use of such Proprietary Information that the party takes with its own proprietary information, but in no event will a party apply less than reasonable precautions to protect such Proprietary Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information. Flock's use of the Proprietary

Information may include processing the Proprietary Information to send Agency alerts, such as when a car exits Agency's neighborhood, or to analyze the data collected to identify motion or other events. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Proprietary Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Proprietary Information pursuant to any judicial or governmental order, provided that the Receiving Party gives the Disclosing Party reasonable prior notice of such disclosure to contest such order. For clarity, Flock may access, use, preserve and/or disclose the Footage to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if Flock has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to: (a) comply with a legal process or request; (b) enforce this Agreement, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Flock, its users, a third party, or the public as required or permitted by law, including respond to an emergency situation. Agency hereby expressly grants Flock a non-exclusive, worldwide, perpetual, royalty-free right and license (during and after the term hereof) to disclose the Agency Data (inclusive of any Footage) to enable law enforcement monitoring against law enforcement hotlists as well as provide Footage search access to law enforcement for investigative purposes only. Flock may store deleted Footage in order to comply with certain legal obligations but such retained Footage will not be retrievable without a valid court order.

4.2 Agency Data. As between Flock and Agency, all right, title and interest in the Agency Data, belong to and are retained solely by Agency. Agency hereby grants to Flock a limited, non-exclusive, royalty-free, worldwide license to use the Agency Data and perform all acts with respect to the Agency Data as may be necessary for Flock to provide the Flock Services to Agency, including without limitation the Support Services set forth in Section 2.9 above, and a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid license to use, reproduce, modify and distribute the Agency Data as a part of the Aggregated Data (as defined in Section 4.4 below). As between Agency and Non-Agency End Users that have prescribed access of Footage to Agency, each of Agency and Non-Agency End Users will share all right, title and interest in the Non-Agency End User Data. This Agreement does not by itself make any Non-Agency End User Data the sole property or the Proprietary Information of Agency. Flock will automatically delete Footage older than thirty (30) days. Agency has a thirty (30) day window to view, save and/or transmit Footage to the relevant government agency prior to its deletion.

4.3 Feedback. If Agency provides any suggestions, ideas, enhancement requests, feedback, recommendations or other information relating to the subject matter hereunder, Agency hereby assigns (and will cause its agents and representatives to assign) to Flock all right, title and interest (including intellectual property rights) with respect to or resulting from any of the foregoing.

4.4 Aggregated Data. Notwithstanding anything in this Agreement to the contrary, Flock shall have the right to collect and analyze data that does not refer to or identify Agency or any individuals or de-identifies such data and other information relating to the provision, use and performance of various aspects of the Services and related

systems and technologies (including, without limitation, information concerning Agency Data and data derived therefrom). For the sake of clarity, Aggregated Data is compiled anonymous data which has been stripped of any personal identifying information. Agency acknowledges that Flock will be compiling anonymized and/or aggregated data based on Agency Data input into the Services (the “*Aggregated Data*”). Agency hereby grants Flock a non-exclusive, worldwide, perpetual, royalty-free right and license (during and after the Service Term hereof) to (i) use and distribute such Aggregated Data to improve and enhance the Services and for other development, diagnostic and corrective purposes, other Flock offerings, and crime prevention efforts, and (ii) disclose the Agency Data (both inclusive of any Footage) to enable law enforcement monitoring against law enforcement hotlists as well as provide Footage search access to law enforcement for investigative purposes only. No rights or licenses are granted except as expressly set forth herein. Flock shall not sell Agency Data or Aggregated Data.

5. PAYMENT OF FEES

5.1a Wing Fees. For Wing products, the Agency will pay Flock the first Usage Fee and the Implementation Fee (as described on the Order Form attached hereto, together the “*Initial Fees*”) as set forth on the Order Form on or before the 30th day following the Effective Date of this Agreement. Flock shall have no liability resulting from any delay by the Agency in installing the Embedded Software on the Agency Hardware. If applicable, Agency shall pay the ongoing Usage Fees set forth on the Order Form with such Usage Fees due and payable thirty (30) days in advance of each payment period. All payments will be made by either ACH, check, or credit card.

5.1b Falcon Fees. For Falcon products during the Initial Term, Agency will pay Flock fifty percent (50%) of the first Usage Fee, the Implementation Fee and any fee for Hardware (as described on the Order Form attached hereto, together the “*Initial Fees*”) as set forth on the Order Form on or before the 30th day following receipt of initial invoice after Effective Date. Upon commencement of installation, Flock will issue an invoice for twenty-five percent (25%) of the Initial Fees, and Agency shall pay on or before 30th day following receipt of invoice. Upon completion of installation, Flock will issue an invoice for the remaining balance and Agency shall pay on or before 30th day following receipt of final invoice. Flock is not obligated to commence the Installation Services unless and until the first payment has been made and shall have no liability resulting from any delay related thereto. For a Renewal Term, as defined below, Agency shall pay the entire invoice on or before the 30th day following receipt of invoice.

5.2 Changes to Fees. Flock reserves the right to change the fees or applicable charges and to institute new charges and fees at the end of the Initial Term or any Renewal Term, upon sixty (60) days’ notice prior to the end of such Initial Term or Renewal Term (as applicable) to Agency (which may be sent by email). If Agency believes that Flock has billed Agency incorrectly, Agency must contact Flock no later than sixty (60) days after the closing date on the first billing statement in which the error or problem appeared, in order to receive an adjustment or credit. Inquiries should be directed to Flock’s Agency support department. Agency acknowledges and agrees that a failure to contact Flock within this sixty (60) day period will serve as a waiver of any claim Agency may have had as a result of such billing error.

5.3 Invoicing, Late Fees, Taxes. Flock may choose to bill through an invoice, in which case, full payment for invoices issued in any given month must be received by Flock thirty (30) days after the mailing date of the invoice.

If Agency is a non-tax exempt entity, Agency shall be responsible for all taxes associated with Services other than U.S. taxes based on Flock's net income.

6. TERM AND TERMINATION

6.1a Wing Term. Subject to earlier termination as provided below, the initial term of this Agreement shall be for the period of time set forth on the Order Form (the "*Initial Term*"). The Term shall commence upon execution of this Agreement. *Following the Initial Term, unless otherwise indicated on the Order Form, this Agreement will automatically renew for successive renewal terms of the greater of one year or the length set forth on the Order Form (each, a "Renewal Term", and together with the Initial Term, the "Service Term") unless either party gives the other party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.*

6.1b Falcon Term. Subject to earlier termination as provided below, the initial term of this Agreement shall be for the period of time set forth on the Order Form (the "*Initial Term*"). The Term shall commence upon first installation and validation of a Unit. *Following the Initial Term, unless otherwise indicated on the Order Form, this Agreement will automatically renew for successive renewal terms for the length set forth on the Order Form (each, a "Renewal Term", and together with the Initial Term, the "Service Term") unless either party gives the other party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.*

6.2 Termination for Convenience. At any time during the agreed upon Term, an Agency not fully satisfied with the service may self-elect to terminate this Agreement for convenience. Termination for convenience will result in a one-time fee of \$500 per Flock Hardware. Upon termination for convenience, a refund will be provided for Falcon Cameras, prorated for any fees for the remaining Term length set forth previously. Agency will remain liable to pay the full outstanding fees for any Wing product on the effective date of termination of that Order Form. Flock will invoice, and Agency will pay, any unbilled fees and any unpaid fees covering the remainder of the term of that Order Form had it not been terminated. Termination for convenience of the Agreement by the Agency will be effective immediately. Flock will provide advanced written notice and remove all Flock Hardware at Flock's own convenience, within a commercially reasonable period of time upon termination.

6.3 Termination. Notwithstanding the termination provisions in Section 2.4(b), in the event of any material breach of this Agreement, the non-breaching party may terminate this Agreement prior to the end of the Service Term by giving thirty (30) days prior written notice to the breaching party; provided, however, that this Agreement will not terminate if the breaching party has cured the breach prior to the expiration of such thirty (30) day period. Either party may terminate this Agreement, without notice, (i) upon the institution by or against the other party of insolvency, receivership or bankruptcy proceedings, (ii) upon the other party's making an assignment for the benefit of creditors, or (iii) upon the other party's dissolution or ceasing to do business. Upon termination for Flock's material breach, Flock will refund to Agency a pro-rata portion of the pre-paid fees for Services not received due to such termination.

6.5 No-Fee Term. For the Term of this Agreement, Flock will provide Agency with complimentary access to 'hot-list' alerts, which may include 'hot tags', stolen vehicles, Amber Alerts, etc. ("*No-Fee Term*"). In the event a Non-Agency End User grants Agency access to Footage and/or Notifications from a Non-Agency End User Unit, Agency will have access to Non-Agency End User Footage and/or Notifications until deletion, subject to the thirty (30) day

retention policy. Non-Agency End Users and Flock may, in their sole discretion, leave access open. The No-Fee Term will survive the Term of this Agreement. Flock, in its sole discretion, can determine not to provide additional No-Fee Terms or can impose a price per No-Fee Term upon thirty (30) days' notice. Agency may terminate any No-Fee Term or access to future No-Fee Terms upon thirty (30) days' notice.

6.6 Survival. The following Sections will survive termination: 2.4, 2.5, 3, 4, 5 (with respect to any accrued rights to payment), 5.4, 6.5, 7.4, 8.1, 8.2, 8.3, 8.4, 9.1 and 10.5.

7. REMEDY; WARRANTY AND DISCLAIMER

7.1 Remedy. Upon a malfunction or failure of Flock Hardware or Embedded Software (a "*Defect*"), Agency must notify Flock's technical support as described in Section 2.9 above. If Flock is unable to correct the Defect, Flock shall, or shall instruct one of its contractors to repair or replace the Flock Hardware or Embedded Software suffering from the Defect. Flock reserves the right in their sole discretion to refuse or delay replacement or its choice of remedy for a Defect until after it has inspected and tested the affected Unit provided that such inspection and test shall occur within seventy-two (72) hours after Agency notifies the Flock of a known Defect. In the event of a Defect, Flock will repair or replace the defective Unit at no additional cost. In the event that a Unit is lost, stolen, or damaged, Agency may request that Flock replace the Unit at a fee according to the then-current Reinstall Policy (<https://www.flocksafety.com/reinstall-fee-schedule>). Agency shall not be required to replace subsequently lost, damaged or stolen Units, however, Agency understands and agrees that functionality, including Footage, will be materially affected due to such subsequently lost, damaged or stolen Units and that Flock will have no liability to Agency regarding such affected functionality nor shall the Usage Fee or Implementation Fees owed be impacted. Flock is under no obligation to replace or repair Hardware.

7.2 Exclusions. Flock will not provide the remedy described in Section 7.1 if Agency is found to have misused the Flock Hardware, Agency Hardware or Embedded Software in any manner.

7.3 Warranty. Flock shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Installation Services in a professional and workmanlike manner. Upon completion of any installation or repair, Flock shall clean and leave the area in good condition. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Flock or by third-party providers, or because of other causes beyond Flock's reasonable control, but Flock shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

7.4 Disclaimer. THE REMEDY DESCRIBED IN SECTION 7.1 ABOVE IS AGENCY 'S SOLE REMEDY, AND FLOCK'S SOLE LIABILITY, WITH RESPECT TO DEFECTIVE EMBEDDED SOFTWARE. THE FLOCK DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED "AS IS" AND FLOCK DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE AND NON-INFRINGEMENT. THIS DISCLAIMER OF SECTION 7.4 ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 10.6, OR IF NO STATE IS MENTIONED IN SECTION 10.6, BY THE LAW OF THE STATE OF GEORGIA.

7.5 Insurance. Flock will maintain commercial general liability policies with policy limits reasonably commensurate with the magnitude of Flock's business risk. Certificates of Insurance can be provided upon request.

7.6 Force Majeure. Flock is not responsible nor liable for any delays or failures in performance from any cause beyond its control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, acts or omissions of third-party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, weather conditions or acts of hackers, internet service providers or any other third party or acts or omissions of Agency or any Authorized End User.

8. LIMITATION OF LIABILITY; NO FEE TERM; INDEMNITY

8.1 Limitation of Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY, FLOCK AND ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL HARDWARE AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCT LIABILITY, OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY, INCOMPLETENESS OR CORRUPTION OF DATA OR FOOTAGE OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY MATTER BEYOND FLOCK'S ACTUAL KNOWLEDGE OR REASONABLE CONTROL INCLUDING REPEAT CRIMINAL ACTIVITY OR INABILITY TO CAPTURE FOOTAGE OR IDENTIFY AND/OR CORRELATE A LICENSE PLATE WITH THE FBI DATABASE; (D) FOR ANY PUBLIC DISCLOSURE OF PROPRIETARY INFORMATION MADE IN GOOD FAITH; (E) FOR CRIME PREVENTION; OR (F) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID AND/OR PAYABLE BY AGENCY TO FLOCK FOR THE SERVICES UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS PRIOR TO THE ACT OR OMISSION THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN THE EVENT OF AN EMERGENCY, AGENCY SHOULD CONTACT 911 AND SHOULD NOT RELY ON THE SERVICES. THIS LIMITATION OF LIABILITY OF SECTION 8 ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 10.6, OR IF NO STATE IS MENTIONED IN SECTION 10.6, BY THE LAW OF THE STATE OF GEORGIA.

8.2 Additional No-Fee Term Requirements. IN NO EVENT SHALL FLOCK'S AGGREGATE LIABILITY, IF ANY, ARISING OUT OF OR IN ANY WAY RELATED TO THE COMPLIMENTARY NO-FEE TERM AS DESCRIBED IN SECTION 6.5 EXCEED \$100, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE. Parties

acknowledge and agree that the essential purpose of this Section 8.2 is to allocate the risks under the No-Fee Term described in Section 6.5 and limit potential liability given the aforementioned complimentary service, which would have been substantially higher if Flock were to assume any further liability other than as set forth herein. Flock has relied on these limitations in determining whether to provide the complimentary No-Fee Term. The limitations set forth in this Section 8.2 shall not apply to claims or damages resulting from Flock's other obligations under this Agreement.

8.3 Responsibility. Each Party to this Agreement shall assume the responsibility and liability for the acts and omissions of its own employees, deputies, officers, or agents, in connection with the performance of their official duties under this Agreement. Each Party to this Agreement shall be liable (if at all) only for the torts of its own officers, agents, or employees that occur within the scope of their official duties. Agency will not pursue any claims or actions against Flock's suppliers.

8.4 Indemnity. Agency hereby agrees to indemnify and hold harmless Flock against any damages, losses, liabilities, settlements and expenses in connection with any claim or action that arises from an alleged violation of Section 3.2, a breach of this Agreement, Agency's Installation Obligations, Agency's sharing of any data in connection with the Flock system, Flock employees or agent or Non-Agency End Users, or otherwise from Agency's use of the Services, Flock Hardware, Agency Hardware and any Embedded Software, including any claim that such actions violate any applicable law or third party right. Although Flock has no obligation to monitor Agency's use of the Services, Flock may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of Section 3.2 or this Agreement.

9. RECORD RETENTION

9.1 Data Preservation. The Agency agrees to store Agency Data in compliance with all applicable local, state and federal laws, regulations, policies and ordinances and their associated record retention schedules. As part of Agency's consideration for paid access and no-fee access to the Flock System, to the extent that Flock is required by local, state or federal law to preserve the Agency Data, Flock will notify Agency of the requirement and applicable retention period, and Agency agrees to preserve and securely store this data on Flock's behalf so that should Flock be legally compelled by judicial or government order, Flock may retrieve the data from Agency upon demand.

10. MISCELLANEOUS

10.1 Severability. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

10.2 Assignment. This Agreement is not assignable, transferable or sublicensable by Agency except with Flock's prior written consent. Flock may transfer and assign any of its rights and obligations, in whole or in part, under this Agreement without consent.

10.3 Entire Agreement. This Agreement, together with the Order Form(s), the then-current Reinstall Policy (<https://www.flocksafety.com/reinstall-fee-schedule>), and Deployment Plan(s), are the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein. None of Agency's purchase orders, authorizations or similar documents will alter the terms of this Agreement, and any such conflicting terms are expressly rejected.

10.4 Relationship. No agency, partnership, joint venture, or employment is created as a result of this Agreement and Agency does not have any authority of any kind to bind Flock in any respect whatsoever.

10.5 Governing Law; Venue. This Agreement shall be governed by the laws of the State in which the Agency is located. The parties hereto agree that venue would be proper in the chosen courts of the State of which the Agency is located. The parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this Agreement.

10.6 Publicity. Upon prior consent from Agency, Flock has the right to reference and use Agency's name and trademarks and disclose the nature of the Services provided hereunder in each case in business and development and marketing efforts, including without limitation on Flock's website.

10.7 Export. Agency may not remove or export from the United States or allow the export or re-export of the Flock IP or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority. As defined in FAR section 2.101, the Services, the Hardware, the Embedded Software and Documentation are "commercial items" and according to DFAR section 252.2277014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with DFAR section 227.7202 and FAR section 12.212, any use, modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

10.8 Headings. The headings are merely for organization and should not be construed as adding meaning to the Agreement or interpreting the associated Sections.

10.09 Authority. Each of the below signers of this Agreement represent that they understand this Agreement and have the authority to sign on behalf of and bind the organizations and individuals they are representing.

10.10 Notices. All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested.

flock safety

EXHIBIT A

Statement of Work

Installation of Flock Camera on existing pole or Flock-supplied pole if required