



October 9, 2026

Transmitted via email

Chairman Chris Phillips
Delegate Tristan Leavitt
Delegate Ryan Browning
Delegate Patrick Lucas
West Virginia House of Delegates Building 1
Room 231E 1900 Kanawha Blvd.
East Charleston, WV 25305-0470

Dear Chairman Phillips, Delegate Leavitt, Delegate Browning, and Delegate Lucas,

Flock has worked in good faith to answer your questions. Before attempting another pass, I'd like to address a point of apparent confusion.

We have seen public statements suggesting that Flock requested an "off the record" meeting, or one held "behind closed doors." That was not our intent. We did not make any such request or set any such condition.

To be explicitly clear: we are proud of our record in West Virginia. We are proud of our products, our safeguards, and our ongoing efforts to continuously improve on each of those fronts. We extended offers to meet, in any setting, with members of the legislature to answer questions, provide a demonstration, and discuss in depth how Flock protects customer data in an effort to further dialogue and understanding. That offer stands. We are committed to continuing to voluntarily answer these questions and are available to meet at your convenience. While we believe that the 10-page response we provided in response to the August 14, 2026 letter was thorough and responsive, please see the below answers to each of your specific questions:

I. Security Incidents & Unauthorized Access

1. For each year since Flock Safety's founding and for each Flock Safety product line, how many incidents is Flock Safety aware of where raw video footage has been accessed by unauthorized users?

Response: Flock's central cloud database housing customer data has never been breached or accessed by an unauthorized external party. In a distinct, previously disclosed incident, a vendor configuration error temporarily exposed a limited number of video (not ALPR) camera streams to the public internet. Access to these streams required specific IP knowledge. To be clear, what was viewable during that brief period, for a small number of cameras, was live streams of public places, no different from what thousands of communities (including some in West Virginia) make available online deliberately, as a public service (see, e.g., this [public feed aggregation site](#)). That was not the intended function of the impacted cameras, however, and we have addressed the issue with our vendor.



While attempted attacks occur continuously across the industry, Flock maintains strict logging, layered security, and continuous monitoring to detect and prevent unauthorized access. Please see the following publicly available blog post from our CISO, Chris Castaldo, which discusses claims of unauthorized access:

<https://www.flocksafety.com/blog/flock-safety-cybersecurity-how-we-protect-customer-community-data>

2. What investigations did Flock Safety conduct of each instance of unauthorized access?

Response: When security events or customer-level credential compromises of any kind occur, Flock leverages comprehensive customer audit logs and backend infrastructure logs capturing IP addresses, authentication attempts, user IDs, and API activity. Our dedicated incident response team, supported by an active partnership with Google Mandiant, conducts thorough forensic investigations to evaluate scope and root causes.

Additionally, independent partners such as the Miami-Dade Sheriff's Office Cyber Crimes Bureau and the cybersecurity firm Bishop Fox have conducted rigorous adversarial testing on field-deployed hardware and software to verify system security and confirm remediation. For more information on the Bishop Fox testing, please visit:

<https://www.flocksafety.com/blog/flock-security-testing-2026-what-the-bishop-fox-penetration-test-found>

3. For each instance of unauthorized access, what was the cause of the security breach?

Response: As noted above, the specific incident referenced was caused by an error by our SIM card vendor. More broadly, system-wide investigations of other security incidents that did not result in the exposure of raw video footage indicate that isolated security risks typically stem from customer-side issues, such as compromised credentials, or improper credential sharing, rather than a breach of Flock's cloud architecture. Flock differentiates customer-side credential issues from infrastructure vulnerabilities and applies learned security lessons platform-wide.

4. What remedial steps has Flock Safety taken after each security breach to prevent recurrence?

Response: Any time an incident or vulnerability is reported, Flock immediately engages its PSIRT (Product Security Incident Response Team). PSIRT triages the report and works with appropriate stakeholders to remediate any issues. We also engage third-party firms such as Bishop Fox to validate those remediations.

In response to the above incident, the team built a series of alerts should a camera inadvertently be made public. Other vulnerability findings have led to the rollout of Secure Boot and strong device authentication, as well as the mandatory enforcement of MFA for all customers.

Flock operates a Coordinated Vulnerability Disclosure (CVD) program as a CISA CVE Numbering Authority to



receive and coordinate any vulnerabilities affecting Flock products. If a vulnerability is discovered, Flock will issue a CVE and make customers aware of the finding. Furthermore, we undergo annual SOC 2 Type II, ISO, and CJIS-aligned audits alongside independent penetration testing to ensure long-term resilience.

II. Surveillance Scope & Data Sharing

5. Please reconcile Mr. Kane's March 4, 2026 claim with the August 25, 2025 blog post regarding pilot programs with CBP and HSI.

Response: The two statements reflect distinct operational models: limited, temporary pilot evaluations of the Flock platform and sharing experience are fundamentally different from contractual, ongoing data-sharing arrangements. In 2025, Flock conducted time-bound, non-contractual pilots with HSI (March–May) and CBP (May–August). Flock publicly announced in August 2025 that it would no longer conduct federal pilot projects, and Mr. Kane's testimony accurately reflected the absence of contractual federal data-funneling relationships.

6. Were the CBP and HSI pilots requested by those agencies, or by Flock Safety?

Response: Our customer relationships result from numerous conversations over a span of time. We are unable to determine whether these particular pilots were prompted by an incoming request or a proactive offer. These temporary pilots were enabled to allow agencies to test platform capabilities within opt-in networks. Following the conclusion of those pilots, Flock ended all federal pilot programs in August 2025.

7. Which Flock Safety product lines feed the National Lookup Tool available for license plate data?

Response: The Nationwide Network (often referenced as the national lookup capability) only includes images and associated metadata from Flock's automated license plate readers (ALPRs). It is an opt-in search feature designed solely for license plate investigations, enabling authorized users with a full plate number to query participating law enforcement networks.

8. What percentage of Flock Safety automated license plate reader users are currently opted into the National Lookup Tool?

Response: Participation in the optional Nationwide Network is governed entirely by individual customer choice, and agencies may join or opt out at any time. In jurisdictions where state law restricts this type of sharing, such as California, Flock has disabled the feature altogether. Federal agencies are completely excluded from Nationwide and Statewide networks and may only connect through explicit, one-to-one local sharing with individual agencies. Participation in networks can change at the customer's discretion, so the specific answer to your question varies as agencies opt in and out. Approximately 50% of customers in eligible jurisdictions are



opted into the nationwide network as of October 2026.

9. Is there an equivalent of the National Lookup Tool for Flock Safety Condor cameras?

Response: No.

10. Will Flock Safety's Condor camera return FreeForm natural language search results for such bodily characteristics as height, hair color, wearing glasses, or a scar on one's face?

Response: Flock's FreeForm search allows investigators to search observable attributes in video footage—such as clothing—to help locate relevant scene footage. Neither Condor nor any other Flock product employs facial recognition technology. The system does not identify individuals, and does not build, reference, or otherwise categorize biometric characteristics or a biometric database. Guardrails deliberately built into the system strictly prohibit certain types of searches, including searches based on race or ethnicity.

III. Accuracy & False Positive Rates

11. For each year since Flock Safety's founding, how many false "Hot List" positives have been generated by: a. Flock Safety's Falcon license plate reader; and b. Flock Safety's Sparrow license plate reader.

Response: Flock offers "Hot List" alerts, which notify law enforcement when a known suspect's vehicle is detected. These real-time notifications work by connecting Flock cameras with data originating from the National Crime Information Center, state databases, and local law enforcement agencies. When a listed vehicle passes a camera, officers receive a notification enabling them to respond accordingly.

Flock's ALPR system uses machine learning to assign a confidence level to plate reads and automatically filters out low-confidence reads before comparing records against hot-lists. Hot-list hits serve as investigative leads rather than final conclusions, and non-enforcement outcomes often result from stale database records, lawful status changes, or unlocated vehicles rather than camera read errors. Flock's ALPR hot-list alerting system generates only approximately nine reported inaccuracies for every one million alerts.

12. Based on the aforementioned false positive data, what was the accuracy rate of the Falcon license plate reader for all license plate "Hot List" hits in 2025?

Response: Inaccurate reads or unverified alerts are rare, but they do happen, and we understand they can have serious consequences. Accuracy is engineered, measured, and continuously improved. Flock's ALPR technology performs multiple checks before a hot-list alert is generated. The camera first captures an image and uses machine-learning models to interpret the license plate. Each read is assigned a confidence score, and low-confidence reads are filtered out rather than sent to officers as alerts. The system then compares both the



interpreted plate and the issuing state against the applicable hot-list record. Only after those steps does the system generate an alert. A hot-list alert is a lead—not a conclusion. A properly-trained officer will independently verify the vehicle and circumstances before taking action.

Flock separately evaluates plate-read accuracy and hot-list alert performance. Plate-read accuracy asks whether the camera correctly identified the characters appearing on the plate. Our latest findings from July 2026 found the following capture and OCR rates:

Test	Results
Clear Weather ALPR Capture Rate* ¹	>99% ALPR capture rate on a two-lane roadway with optimal camera placement and installation.
Rain ALPR Capture Rate*	>99% ALPR capture rate on a two-lane roadway with optimal camera placement and installation.
Dawn/Dusk ALPR Capture Rate*	>98% ALPR capture rate on a two-lane roadway with optimal camera placement and installation.
Optical Character Recognition (OCR) Accuracy	>96% ALPR OCR accuracy on a two-lane roadway with optimal camera placement and installation.
License Plate State Accuracy	>97% ALPR plate state read accuracy on a two-lane roadway with optimal camera placement and installation.

These high capture and OCR rates, combined with our verification process of filtering out low-confidence reads, has led to Flock’s ALPR hotlist alerting system generating approximately nine reported inaccuracies for every one million alerts.

A hot-list “hit” can fail to result in an enforcement action for a number of reasons that do not mean the ALPR inaccurately read the plate. For example, the underlying hot-list record may have changed, the vehicle may have lawfully changed status, the officer may be unable to locate the vehicle, the vehicle may no longer correspond to the circumstances reflected in the database, or the officer may determine through independent verification or assessment that the alert should not be acted upon. No system can protect entirely against human error. However, our high and continuously-improving rate of accuracy, combined with the safeguards described above, help to make those human errors rare and will continue to decrease error prevalence over time.

¹ Items marked with an asterisk reflect testing on our latest-generation ALPR cameras.

13. Based on the aforementioned false positive data, what was the accuracy rate of the Sparrow license plate reader for all license plate “Hot List” hits in 2025?

Response: The Sparrow ALPR is a deprecated name for our ALPR hardware. Our most up-to-date hotlist accuracy numbers in 2026 show that, LPR fleetwide, our alerting system generates only approximately nine reported inaccuracies for every one million alerts.

IV. Internal Oversight & Employee Access Controls

14. For each corporate division of Flock Safety, approximately how many employees have access to all customer data?

Response: No corporate division or employee possesses broad, unrestricted access to all customer data. System permissions follow strict least-privilege, role-based controls, separation of duties, and hardware-backed authentication, limiting elevated access to designated technical personnel for platform operation, support, or security triage.

15. How often does Flock Safety audit its employees’ access of customer data? What do the audits consist of? Do such audits comprehensively review every search, or only perform spot checks?

Response: Employee oversight is continuous rather than periodic: Security Operations teams conduct continuous monitoring in lieu of scheduled audits, periodic privilege reviews, and targeted forensic investigations whenever anomalous behavior is flagged.

16. Since Flock Safety’s founding, how many employees have ever been found to have improperly accessed customer data?

Response: Flock enforces a strict code of conduct, robust technical boundaries, and comprehensive audit logging to deter and identify internal policy violations. In any instance where an employee is found to have accessed data outside authorized technical duties, Flock executes formal incident response procedures, which include access revocation, personnel sanctions, and potential termination.

V. Data Governance & Infrastructure

17. What disaster recovery backup methods does Flock Safety use for customer data?

Response: Customer data is hosted in Amazon Web Services (AWS) East 1 in Virginia using encrypted S3 containers, encrypted databases, and encrypted snapshot backups utilizing AES-256 or better encryption. The architecture provides automated recovery, system-level failover, and multiple snapshot backups requiring multi-factor authentication for restoration.

18. How are metadata, derivative data, analytics, insights, intelligence, and extracted data from footage governed across Flock Safety’s platforms? Who owns the aforementioned?

Response: Customers retain full ownership and control over all customer data, which is defined in our Terms:

“Customer Data” means all (a) data and information captured by Flock Hardware on behalf of Customer through the Flock Services (e.g., images, audio, and/or video) and metadata associated therewith, (b) content input into the Web Interface by Customer or its Authorized End Users, and (c) data and information provided to Flock through the Flock Services by third parties at Customer’s direction.

19. How long are metadata, derivative data, analytics, insights, intelligence, and extracted data from customer products retained by Flock Safety for research purposes?

Response: Flock does not retain data “for research purposes.” Flock does not maintain a single blanket retention figure, as schedules vary based on data type, customer agreements, and legal or security log requirements. Customer image retention is dictated by agency contract, while system audit logs are retained separately for accountability and compliance needs. Flock may use a very small fraction of images captured by Flock license plate reader cameras to improve model accuracy. Before an image is used for model training, Flock strips the customer-identifying metadata. The purpose is to improve recognition accuracy for new vehicle types and license plates. Customers may choose to opt out of this training, and customers in states with a statutory license plate reader data retention period are not included in this training.

20. Please list all contracts Flock Safety has ever had with entities outside of the United States to conduct third-party review of Flock Safety data, metadata, derivative data, analytics, insights, intelligence, or extracted data.

Response: Flock utilizes non-U.S. vendors exclusively for machine-learning data annotation to improve model accuracy across varying weather and lighting conditions. These vendors do not receive independent review access to customer accounts, search histories, or operational data. Annotators work solely on isolated, decontextualized images stripped of customer identifying metadata.

21. Please provide your most recent SOC 2 Type II compliance audit.

Response: Flock undergoes annual independent SOC 2 Type II and ISO compliance audits. Authorized agency partners and officials can securely review and download our latest SOC 2 Type II report directly through the Flock Security Center at [\[https://security.flocksafety.com/\]](https://security.flocksafety.com/)(<https://security.flocksafety.com/>).

We welcome the opportunity to provide an on the record briefing to the Committee, including appropriate technical personnel, to walk through any of these matters in detail.

Sincerely,



Dan Haley

Chief Legal Officer, Flock