# Four Disclosed Flock Safety and FlockNova Vulnerabilities

Controlled supporting memorandum: the four-finding disclosure chronology, in submission order

**Joshua Michael**
Email: josh@nexanet.ai



September 2, 2026

# Contents

## Opening: An Undisclosed Production Export, and a Public Denial

On December 14, 2025, I used an authentication failure I had already reported to Flock Safety to obtain a production export of 335,701 device and deployment records. The path issued fresh ArcGIS credentials before login. I had reported that failure on November 13, 2025, followed up on November 14 and November 19, and then waited another month with no closure. I did not separately tell Flock that I had acquired the dataset.[1]

What made that export consequential was established by the first finding I ever reported. The credential at the center of this chain was not a cosmetic basemap token; it was tied to Flock Safety's production ArcGIS mapping plane. The original validation showed an active ArcGIS Location Platform organization subscription holding roughly 995,002.8 available credits, carrying the full network-analysis capability family a system uses to route units across a map.[L8] That mapping plane sits over an operational system of real consequence. The associated research record describes an environment covering roughly 5,000 police departments, 6,000 private communities, and 1,000 private businesses.[L2, L20, P1] The December 14 export itself contains 335,701 device records, including camera and audio-device records tied to nearly continuous public-road, community, business, and law-enforcement detection coverage. [L14, L15] Flock publicly claims roughly 20 billion monthly license-plate reads, and its own product catalog sells data-retention extensions for one-, three-, and five-year periods.[E2, L26] These were the keys to the geospatial control plane of a national surveillance network, not a stray demo secret.

Two points of precision belong here before the rest of this record is read. First, the device dataset came through the pre-login credential-minting path (Finding 3), not through the static ArcGIS Default API key (Finding 1). These are two separate credential-plane failures, and keeping them apart matters.

Finding 1 was, in plain terms, the keys to the kingdom. It was an authentication key to Flock's dynamic surveillance network, a system woven into the heartbeat of movement across America, and Flock leaked it across public assets 53 times.[L5, L20] With that key I did not pull police locations, query people or vehicle reads, access 911 call transcripts, or make changes to any of the private map layers. That restraint was a deliberate ethical boundary, not a technical limit: the access was there, and I chose not to use it. The significance is the point. The reason this never became one of the largest

national-security breaches of its kind was not Flock's security; it was my decision to disclose the vulnerability rather than exploit it. Disclosing a flaw for the public's safety, rather than using it, is the reason cybersecurity research exists.

The dataset itself came from the third vulnerability, the pre-login path that returned device-location records. That one I did use, and only after watching the same class of failure repeat and out of a genuine concern for the national-security exposure the data represents. Finding 1 is set out here as the context that gives the export its meaning; the acquisition belongs to Finding 3.

Twenty-three days later, on January 6, 2026, Flock published a security page stating that the company had never been hacked. The same page stated that its cloud infrastructure had never been compromised, that customer data had never been accessed or exfiltrated by an attacker, and that Flock had never had a data breach.[2]

On March 27, 2026, Flock reiterated its January 6 position. In a post from Chief Information Security Officer Chris Castaldo, the company again stated that it had never had a data breach and characterized the claims against it as "false and/or misleading," closing under a heading declaring that Flock would "continue to lead the industry in cybersecurity."[3]

Flock has repeated that denial since. As recently as June 10, 2026, a further Flock security page stated again that "Flock's cloud platform has not been hacked," attributing the reported activity to a single undeployed camera never connected to Flock's cloud. That page stresses a distinction it calls important, that "a broad customer data breach and an isolated issue involving an undeployed device are very different events," and closes that "security conversations are strongest when they're grounded in facts, context, and transparency rather than assumptions."[4]

Those statements matter because I never disclosed to Flock that I had pulled hundreds of thousands of device records out of its production mapping plane. That leaves only two possibilities, and both are damaging. Either Flock knew that I had taken those records from its network (I did not "hack" anything; I used a credential path Flock itself left exposed) and it has chosen clean marketing over an honest accounting to the Americans whose data it holds. Or Flock did not know: it publicly asserted three separate times, after being told it had been "hacked," that its platform had never been breached, and it characterized the researchers reporting the exposure as trading in "false and/or misleading" claims, all while its own security was too poor to register a national-scale export of production data as it happened. The legal label that attaches to responsible research does not resolve the operational question underneath it: if Flock

cannot account for the use of its own production credentials by someone who never announced the acquisition, would it know if a hostile foreign government had done the same? Flock's own June statement sets the standard, that security conversations "are strongest when they're grounded in facts, context, and transparency." The December export is such a fact, and it is neither an assumption nor the isolated undeployed-device issue Flock describes. On the evidence preserved here, a public posture that customer data was never accessed or exfiltrated, and that the company leads the industry in cybersecurity, is difficult to reconcile with a documented, undisclosed, unauthenticated pull of 335,701 production records from the very mapping plane the first finding had already shown to be exposed.

## Executive Summary

The four reported issues are best understood as one exposure chain rather than four unrelated bugs. First, a hardcoded ArcGIS Default API key exposed a production geospatial credential. Second, FlockSafety development bundles were served before the correct authentication boundary, revealing the application map for Search, Hotlist, and FlockOS-style workflows. Third, a Planner/Beefeater path minted ArcGIS and Google mapping credentials before login, creating a credential factory. Fourth, FlockNova bundles were served before the correct authentication boundary, revealing the data-fusion application model around identity, vehicles, device signals, LPR, RMS, CAD, arrest, and body-worn-camera workflows.

The combined effect was sufficient to reveal architecture, credential scope, camera inventory, and operationally significant movement-exposure patterns around sensitive sites. This memorandum does not claim that every visible frontend endpoint was anonymously readable. It states that exposed application logic and geospatial credential failures made enough of the system visible to support a defensive exposure assessment.

## Submission Timeline

1. **Finding 1**
   Reported 2025-06-11. Hardcoded active ArcGIS Default API key in a public development demo. Remediation reported 2025-07-01.
2. **Finding 2**
   Reported 2025-11-13, with follow-ups on 2025-11-14 and 2025-11-19. FlockSafety development application bundles were served before the correct authentication boundary. No closure or remediation detail was returned in the disclosure record.

3. **Finding 3**
   Reported 2025-11-13, with follow-ups on 2025-11-14 and 2025-11-19. Planner/Beefeater issued ArcGIS and Google mapping credentials before login. No closure or remediation detail was returned in the disclosure record.
4. **Finding 4**
   Reported 2025-12-05. FlockNova application bundles were served before the correct authentication boundary. No reply or remediation detail was returned in the disclosure record.

## Finding 1: Hardcoded ArcGIS Default API Key

Reported: 2025-06-11
Disclosure role: credential pillar

The first submitted finding involved a hardcoded active ArcGIS Default API key in a public Storybook/Ladle-style development demo served from `dev-search-component-demo.flocksafety.com`. The exposed demo allowed enumeration of internal component pages and corresponding source, including component props and internal logic. Follow-on research documented the same credential material appearing repeatedly across development assets; my published research documents 53 exposed instances on development subdomains.[L5, L20, P1] The package preserves the associated ArcGIS scope validation without reproducing the secret.

The significance was not that a cosmetic basemap token appeared in a webpage. The key was tied to Flock Safety's production ArcGIS mapping plane. The original validation showed an active ArcGIS Location Platform organization subscription holding roughly 995,002.8 available credits, exposed through the application titled `Default API Key` (appId qNvllGlOMKItMs4k, orgId 1KuIkn1ysFhZtjPD, itemId 030ff0e7721d43c9ab719e3df947ce5f, owner FlockSafety). My published research documents the exposed environment as Flock's production ArcGIS environment and roughly 40 private portals; the repository validation artifact records 63 granted privileges in total - 50 private ArcGIS item grants and 13 premium user capabilities. The 13 premium capabilities are basemaps, three geocoding privileges (geocode, stored, and temporary), GeoEnrichment, and an eight-privilege network-analysis family: the parent networkanalysis grant plus closest facility, service area, routing, optimized routing, location-allocation, origin-destination cost matrix, and vehicle routing. Those are movement-analysis and geospatial-control capabilities.[L6, L8]

The network-analysis family is operationally specific rather than decorative. Closest-facility, service-area, routing, optimized-routing, origin-destination cost-matrix, and vehicle-routing analysis are the capability class that a computer-aided-dispatch (CAD) and automatic-vehicle-location (AVL) system uses to route responders to incidents by nearest available unit and drive time. For a license-plate-reader network, that is the capability class for routing police units to camera alerts and hotlist hits. FlockOS's own mapped surfaces include CAD and AVL integration[L13], so a public production key carrying the full network-analysis family is consistent with, and sufficient for, alert-to-unit dispatch routing. This is an interpretation of the exposed capability set; it is not a claim that this key was used to dispatch any specific unit or that Flock operated it for that purpose.

The exposure was also significant because of the operational context of the underlying system. The associated research record describes Flock's environment as covering data from roughly 5,000 police departments, 6,000 private communities, and 1,000 private businesses.[L2, L20, P1] The December 14, 2025 ArcGIS export analyzed in the broader research contains 335,701 device records, including camera and audio-device records used for nearly continuous public-road, community, business, and law-enforcement detection coverage.[L14, L15] Flock publicly claims roughly 20 billion monthly license-plate reads, and separate product catalog evidence shows data-retention extension products for one-, three-, and five-year periods.[E2, L26]

The exposed component source also included enumeration-useful values such as device-layer and organization-identifier props. Remediation was reported on 2025-07-01. This public memorandum does not publish the key, token values, item IDs as a bulk list, or query examples.

## Finding 2: FlockSafety Development Bundles Served at the Wrong Layer

Reported: 2025-11-13, with follow-ups on 2025-11-14 and 2025-11-19
Disclosure role: FlockSafety application-map pillar

The second submitted finding involved FlockSafety development application bundles served before the correct authentication boundary. The reported example was `dev-app.flocksafety.com`, but the disclosure record states that the issue applied to the broader development-subdomain pattern rather than only that host. The observed pattern was that the browser-facing login gate did not prevent static application artifacts and module-federation bundles from being downloaded and inspected.

Those exposed artifacts mattered because they revealed how the application was assembled and what data classes it modeled. The FlockSafety bundle evidence included `dev-search-2` and `dev-hotlist` bundle artifacts and shows Search/Monaco, Hotlist, and FlockOS-style map workflows, including plate and vehicle search, camera selection, case/reason metadata, geofence and map selection behavior, people-search paths, hit history, hotlist alerts, owner or enrichment concepts, CAD, Prepared911/Flock911-style event handling, drone-dispatch concepts, people-detection alerting, ROI/geofence workflows, custom map layers, CAD/AVL, Raven/audio sensors, GoLive-style surfaces, and organization-scoped feature flags or permission concepts.[L5, L11, L12, L13]

The root issue was authentication at the UI routing layer while the asset server and module-federation loader remained reachable. This finding did not prove that every backend endpoint returned production data to every caller. It proved that application logic, route names, API shapes, feature flags, hardcoded organization-configuration concepts, role-conditional UI paths, module-federation metadata, data-model boundaries, and permission vocabulary were exposed at the wrong layer. That information is operationally meaningful because it shows where credentials and application requests would be meaningful if a credential or token boundary failed.

After follow-ups on 2025-11-14 and 2025-11-19, Flock replied that the findings were being internally triaged and that next steps would follow. No closure or remediation detail was returned in the disclosure record.

## Finding 3: Pre-Login ArcGIS and Google Mapping Credential Issuance

Reported: 2025-11-13, with follow-ups on 2025-11-14 and 2025-11-19
Disclosure role: credential-factory pillar

The third submitted finding involved Planner and Beefeater production and development subdomains issuing ArcGIS and Google mapping credentials before login. The reported class was not merely that a mapping-token endpoint existed. The boundary failure was that authentication order and environment separation were wrong for services that mediated access to production mapping capabilities.

The disclosure record describes unauthenticated issuance of ArcGIS and Google mapping credentials, including development infrastructure able to mint production-scope geospatial credentials. Both production and development Planner/Beefeater paths minted credentials scoped to the same production ArcGIS mapping environment, rather than maintaining a meaningful dev/prod privilege boundary. The token responses also

carried production application metadata in both environments. Wire evidence preserved in the research archive shows anonymous requests returning successful responses with tokens;[L37] this public memorandum does not reproduce those tokens or provide a request recipe.

This credential-factory path is also the provenance for the bulk ArcGIS map-point/device export used in the broader research. The camera and device map points used for the installation reachability analysis came from the production ArcGIS mapping plane reached through this Finding 3 credential path, not from the static Default API key alone.

On December 14, 2025, after reporting Finding 3 and sending the November follow-ups, I used this path to obtain the 335,701-record device/deployment[L14, L15] export. I did not send Flock a separate notice that I had acquired the dataset. The preserved export and verification artifacts establish the date and record count; the notice statement records my first-person disclosure history.

The same disclosure also described unauthenticated exposure of a working Google Maps JavaScript API key.[L37] The key is not reproduced here. The security issue is that it was returned to unauthenticated callers before login and could create cost or abuse risk if referrer controls, redirects, or related web-trust boundaries were misconfigured.

This finding is critical because it is a second credential-plane failure separate from the static ArcGIS key in Finding 1. The static key showed that a broadly scoped production geospatial credential had been embedded in public development assets. The Planner/Beefeater issue showed that production-scope mapping credentials could be minted on demand before login. It also put premium and potentially billable GIS capabilities, deployment data, and Google mapping credentials in scope for unauthenticated exposure. Together, they support the conclusion that the problem was systemic credential governance and environment-boundary failure, not a one-off leaked secret.

After follow-ups on 2025-11-14 and 2025-11-19, Flock replied that the findings were being internally triaged and that next steps would follow. No closure or remediation detail was returned in the disclosure record.

## Finding 4: FlockNova Bundles Served at the Wrong Layer

Reported: 2025-12-05
Disclosure role: FlockNova data-fusion application-map pillar

The fourth submitted finding involved FlockNova application bundles served before the correct authentication boundary on `nova.flockdemo.com` and `nova-api.flockdemo.com`. [L2, L38] The disclosure record also stated that the environment was not locked behind a VPN or equivalent private-access boundary. FlockNova should be treated as a data-fusion application, not merely a plate-search interface. Flock publicly markets Nova with the phrase “Search Once. See Everything.” It adds data context to FlockOS sensor visibility.

The exposed Nova frontend models freeform search, advanced search, and pivot workflows across public-records identity data, dark-data documents, online accounts, device signals, addresses, IP intelligence, LPR results, RMS records, CAD events, arrests, and body-worn-camera events. The code also models email-to-location signals, hashed-email device lookup, registration-ID lookup, advertising-ID/MAID-style location lookup, IP-to-signal lookup, location/radius signal search, and bulk-signal loading with a 500,000-row client-side load limit.[L4, L27, L36]

The client-side access-control model visible in the frontend is also relevant. The strongest visible client-side enforcement is in the freeform pipeline. Other advanced-search modals and RMS/CAD/BWC screens rely largely on tab visibility and form validation, meaning final enforcement must depend on backend authorization, tenant scope, logging, and abuse controls. This memorandum does not claim that every Nova backend endpoint lacked authorization. It states that the exposed frontend made the application’s search taxonomy, pivot model, data sources, and access-control assumptions visible. It also made connected-service provenance inspectable, including that Nova inherited or incorporated service lineage from CodeFour.ai and Healthcare Safely.[L38]

No reply or remediation detail was returned in the disclosure record.

## Combined Exposure Chain

The findings combine into a single chain:

1. Exposed FlockSafety and FlockNova application logic identified the mapping, search, alerting, data-fusion, and investigation surfaces.
2. A hardcoded production-scoped ArcGIS Default API key and a separate pre-login token-minting path exposed or minted geospatial credentials.

3. The resulting application and credential evidence made it possible to assess camera inventory, geospatial scope, and movement-detection exposure around sensitive sites.

This chain supports a defensive security conclusion: Flock's application, credential, and geospatial data planes were not isolated strongly enough for a system that aggregates law-enforcement, private-community, business, and public-road surveillance data at national scale.

## Published Research by Joshua Michael

- 53 Times Flock Safety Hardcoded the Password for America's Surveillance Infrastructure.
- Misconfigured Demo Exposed Flock Safety's 83,000-Camera Nationwide Tracking System.
- License Plate Reader Company Flock Said It Does Not Use Dark Web Data. My Analysis of Their Code Tells a Different Story.

---

1. Production ArcGIS export of 335,701 device and deployment records obtained December 14, 2025 through the pre-login credential-minting path documented in this memorandum as Finding 3. The date and record count are preserved in the research export and verification artifacts; I did not send Flock a separate notice that the dataset had been acquired.↩
2. Flock Safety, "Has Flock Been Hacked?" (https://www.flocksafety.com/blog/has-flock-been-hacked), published January 6, 2026 and last updated July 24, 2026: the company had never been hacked, its cloud infrastructure had never been compromised, customer data had never been accessed or exfiltrated by an attacker, and it had never had a data breach ("No, Flock's cloud platform has not been hacked… There has never been an incident in which customer data was accessed or exfiltrated by an attacker").↩
3. Flock Safety Chief Information Security Officer Chris Castaldo, "Flock Safety Cybersecurity: How We Protect Customer & Community Data" (https://www.flocksafety.com/blog/flock-safety-cybersecurity-how-we-protect-customer-community-data), March 27, 2026: reiterated that the company had never had a data

breach and characterized the claims against it as “false and/or misleading,” ending under a heading stating that Flock would “continue to lead the industry in cybersecurity.”↩

4. Flock Safety, “What Makes a Public Safety Platform Secure” (https://www.flocksafety.com/blog/what-makes-a-public-safety-platform-secure), June 10, 2026: “No, Flock’s cloud platform has not been hacked,” attributing the reported activity to “a single camera that had never been deployed to a customer… and had never been connected to Flock’s cloud environment”.↩