‘Never Hacked’: The National Security and Accountability Failures in Flock Safety’s Nationwide Dynamic Surveillance Network

How four reported security failures and one undisclosed 335,701-record export turned a vendor’s ‘never hacked’ assurance into a national-security question.

Joshua Michael
Email: josh@nexanet.ai

September 2, 2026

Contents

Executive Summary

On December 14, 2025, I retrieved 335,701 device and deployment records from Flock Safety's production environment using credentials that Flock's own service issued without authentication. I had reported that failure a month earlier. This was the second exposed credential mechanism I had identified. The first concerned a geospatial environment serving Flock's nationwide customer network, which Flock reports generates more than 20 billion vehicle reads each month.

I reported that path, along with another vulnerability, on November 13 and heard nothing back. I followed up on November 14 and again on November 19. The only replies arrived after the second follow-up and read, in full, "Thank you for the findings. We are internally triaging them and will reach back out with next steps soon." Flock did not contact me again or provide a closure notice for either vulnerability. When I retested in December, the reported exposures remained accessible. I then retrieved the 335,701 production records without separately notifying Flock of that retrieval.[1]

Flock's response followed the same pattern across most of my disclosures: delayed or absent replies and no confirmed remediation for three of the four vulnerabilities. Flock confirmed remediation only for Vulnerability 1, the most severe, after I said I would publish if it remained unresolved. That vulnerability was the production credential to the mapping system behind FlockOS, associated with the environment serving Flock's reported customer network of roughly 5,000 police departments, 6,000 private communities, and 1,000 businesses.

What I did not do matters as much as what I did. The credential I used was the less powerful of two I had found and reported to Flock.

What I did	What I deliberately did not do
Obtained 335,701 production device and deployment records through a pre-login path I had already reported but Flock had not remediated	Access live investigative data from the roughly 5,000 departments on the platform
Took the inventory with the *less powerful* of the two exposed credentials	Run a plate search, follow a vehicle, or track a single American through the system
Validated the credential's scope and preserved the complete unredacted record	Open any of the 50 private ArcGIS items the earlier key reached

Those boundaries were self-imposed. I stopped because I chose to, not because the system prevented further access.

By the end of my research in December, the findings no longer looked like isolated software defects. In less than six months, the platform had failed four times: twice through pre-login credential paths and twice through application blueprints delivered before authentication. For a company holding movement data concerning service members, their families, and public officials, that pattern indicates systemic weakness rather than bad luck. It is consistent with the concerns raised in Senator Wyden's letter to Flock. The four defects amplified one another inside the largest dynamic surveillance network in the United States.

Twenty-three days after the export, Flock published its first statement that it had never been hacked. Its January 6 blog post said the cloud infrastructure had never been compromised, that customer data had never been accessed or exfiltrated by an attacker, and that the company had never had a data breach. The page has since been revised, but those categorical statements survived.[2] On March 27, chief information security officer (CISO) Chris Castaldo repeated the position, called the claims against Flock "false and/or misleading," and said the company would "continue to lead the industry in cybersecurity."[3] On June 10, 2026, Flock again said that its cloud platform "has not been hacked," distinguishing "a broad customer data breach" from "an isolated issue involving an undeployed device" and stating that conversations "are strongest when they're grounded in facts, context, and transparency rather than assumptions."[4] Throughout those public statements, I retained the 335,701 records obtained through credentials Flock's service had issued on request. Flock neither contacted me about the export nor publicly accounted for it.

Flock's statements leave two material possibilities. Either the company detected the export and excluded it from its public assurances, or it did not detect the export at all. The first would be a transparency failure. The second would be a detection failure with national-security implications.[5]

Flock may argue that device and deployment records are not customer data. Its public assurance, however, was broader. The company said its cloud infrastructure had never been compromised. The 335,701 records left production through a credential Flock's own service issued on a path inside Flock's own cloud. Regardless of how Flock categorizes the records, the evidence does not support an assurance that broad.

Section 2 describes all four vulnerabilities. The broadest static blast radius came from Vulnerability 1, a hardcoded production ArcGIS Default API key in Flock's geospatial control plane, part of what Flock's own patent calls a dynamic surveillance network. The key was associated with the live mapping environment serving Flock's reported

customer network of roughly 5,000 police departments, 6,000 private communities, and 1,000 businesses. It carried 50 private item grants and 13 premium capabilities, including services used for movement analysis. My research found the same key in 53 public files.[6]

Consider the two credential failures together. If Flock cannot account for a known 335,701-record retrieval, it cannot credibly assure the public that other use of its exposed production credentials would have been detected.

The thesis is straightforward. **Flock cannot demonstrate that it accounted for the use of its exposed production credentials. The inventory obtained through one of those credentials also reveals camera coverage around 22 sensitive military, intelligence, federal, and defense sites. Together, those facts make the platform a national-security concern.** Using the device inventory retrieved through Vulnerability 3, I conducted a modeled route-coverage study around those sites. The study asks how often ordinary public-road trips from off-installation residential areas to reviewed 24/7 gates would pass recorded Flock cameras. Across the 22 sites, the median 20-mile robust confirmed share is 66.0%. The results vary widely: 93.9% at Eglin Air Force Base and 89.4% at Joint Expeditionary Base Little Creek, compared with 18.5% at Northrop Grumman and 15.6% at Lockheed Martin. The study frames collectively represent roughly 8 million households before accounting for overlap among the dense Washington-area frames. Among confirmed modeled round trips, the median site-level mean is 3.17 distinct cameras per trip, equivalent to about 792 encounters a year at 250 commutes.[7] These results show why the exposure is a national-security question. Section 5 reports the complete results for all 22 military, intelligence, federal, and defense-contractor sites.

Flock's network can serve legitimate investigations. But failures in credential security, authorization, data retention, or auditing can expose the movements of service members, government personnel, and others whose safety is a national-security concern. This report documents that those controls have failed. A company may pursue growth, but its quarterly performance cannot take priority over the security of the nation whose roads, agencies, and people make that growth possible.

The table below ranks the sites from most to least covered. **Confirmed** is the occupied-housing-weighted share of modeled round trips that pass at least one camera, and **passes no camera** is the share that passes none. These are the strict **robust** figures.

Confirmation requires every plausible access route to agree. The columns show two of four outcome classes and therefore do not sum to 100%; the remainder is *might pass a camera* or *couldn't determine*.

Table 1. Robust results, 20-mile.

Site	Confirmed to pass a camera	Passes no camera
Eglin AFB	93.9%	3.4%
Joint Expeditionary Base Little Creek	89.4%	2.1%
Fort Lee	89.2%	0.0%
Jet Propulsion Laboratory	87.9%	1.6%
Hurlburt Field	87.0%	10.5%
Fort Cavazos (Hood)	85.7%	4.5%
Naval Amphibious Base Coronado	84.9%	0.6%
Buckley Space Force Base	81.1%	4.9%
Naval Station Norfolk	75.4%	18.5%
Joint Base Andrews	68.8%	9.1%
Naval Base San Diego	67.0%	2.2%
FBI Headquarters	65.0%	0.0%
CIA Headquarters	62.1%	0.7%
Anduril Industries Headquarters	61.7%	0.9%
Pentagon	57.2%	0.5%
Fort Benning	56.9%	12.9%
RTX Corporation Headquarters	55.9%	4.0%
MacDill AFB	54.9%	27.1%
Camp Pendleton	54.8%	4.8%
Fort George G. Meade	50.3%	34.8%
Northrop Grumman Headquarters	18.5%	17.0%
Lockheed Martin Headquarters	15.6%	11.0%

1. The System Behind the Cameras

Flock Safety is often described as a license-plate-reader company. That description is no longer adequate. The system represented in the evidence is a connected surveillance and investigation environment: cameras and audio sensors collect observations; FlockOS places detections, alerts, incidents, and response assets on a common map; FlockNova joins those observations to identity, location, account, signal, and agency-record data.

These are not products operated by unrelated companies. Flock Safety markets FlockOS and FlockNova inside the same platform and describes them as complementary layers: FlockOS supplies visibility into physical detections, while Nova supplies the data context behind each event. Flock's own phrase is **"Search Once. See Everything."** The same vendor therefore spans collection, mapping, alerting, search, identity expansion, and the security boundaries examined in this report.[8]

The three product layers do different jobs:

Flock Safety sensors and applications collect observations and create searchable events. This layer includes fixed and mobile license-plate reader (LPR), video-capable cameras, third-party camera gateways, Raven audio, trailers, drones, Search, Hotlist, device administration, and mobile clients.

FlockOS supplies the common operational map and response workspace. It combines camera and device layers with vehicle and people alerts, computer-aided dispatch (CAD) and patrol context, Raven events, drones, body-camera references, Flock911 events, custom layers, and real-time notification streams.

FlockNova supplies identity and data fusion. It organizes person, address, email, phone, vehicle, plate, device, signal, IP, online-account, dark-data, records-management system (RMS), CAD, arrest, BWC, LPR, and relationship-pivot records.

The evidence shows an end-to-end intelligence workflow. A device produces an observation. Search or Hotlist converts that observation into a query, alert, saved search, or watchlist event. FlockOS places the event on a map with location, source, camera, incident, and response context. Nova supplies the next set of pivots: who or what may be associated with the vehicle, address, account, device, case, or signal. The system's sensitivity comes from that sequence, not from any one database column.[9]

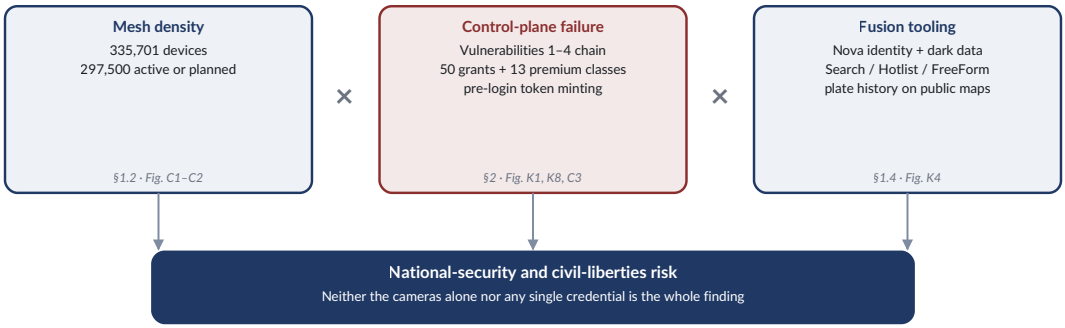


Figure 1. The national-security risk appears where a dense sensor network, exposed control and data planes, and identity/ movement fusion intersect.

1.1 A Dynamic Surveillance Network

Flock's own patent calls the architecture a **dynamic surveillance network**. It describes a system that can ingest video from unrelated neighborhood, residential, business, traffic, and portable cameras and search footage by what appears in the image rather than only by time and location. The patent discusses vehicle attributes, clothing and appearance attributes, and face-related feature or similarity matching.[10]

The product architecture follows that model. Wing Gateway-class devices can bring ordinary third-party IP cameras into Flock's detection plane. Business Network options place private commercial cameras within investigative search scope. FreeForm accepts an English description of a person or vehicle rather than requiring a complete plate. A query can therefore rely on a color, body type, trailer, equipment, logo, sticker, damage pattern, clothing description, or another visible combination. The system can remain useful when a plate is unreadable or absent.[11]

This does not require every camera to carry Flock branding. A camera at a neighborhood entrance, shopping center, gas station, hotel, warehouse, or private business can become a node in the same search environment. That expansion model matters around installations because public roads, private commercial property, residential communities, and government facilities overlap in the same commuting area.

1.2 Scale and Concentration

Flock's public materials state more than 20 billion vehicle reads per month across 49 states; my own January 2026 publication records more than 30 billion monthly vehicle detections, a broader measure that includes non-plate detections. My disclosure and published-research record places the operating context at roughly 5,000 police departments, 6,000 private communities, and 1,000 private businesses.[12] Those

customer figures are context, not counts derived from the December export. The December export supplies a separate, directly counted measurement of deployed and planned devices, set out in Section 3.

Concentration changes the security problem. A disconnected set of municipal camera systems would need its own access, search logic, and history for each city. A shared commercial platform centralizes credentials, application components, data models, and administrative controls under one vendor. A defect in a common control can therefore cross boundaries that would otherwise separate cities, agencies, private communities, and businesses.

The same concentration makes cybersecurity part of force protection. Camera positions mark where observation happens and where it is set to expand. Search and hotlist schemas expose how investigators define people, vehicles, places, time windows, and alert rules. The premium geospatial services go further, turning the inventory into routes, service areas, closest facilities, and origin-destination relationships that Nova can then tie back to a larger identity graph.

1.3 Retention and the Value of Time

Flock's current public policy describes an approximately 30-day default for certain evidence, subject to customer, legal, and contractual differences. The product catalog preserved in this repository also sells one-, three-, and five-year retention extensions priced per law-enforcement-grade camera.[13] A short window can expose a current shift pattern, recurring commute, protest attendance, or recent association. A multi-year history can support seasonal baselines, deployment comparisons, household changes, and repeated co-movement analysis.

Movement records do not become harmless because each trip is unclassified. What retention really buys is a baseline. With a long enough history, a break from someone's routine becomes visible as a break. Section 6.1 sets out what that supports around a specific installation.

That is why this report treats the Flock environment as movement-intelligence infrastructure. The cameras are the collection layer. The map, alerts, histories, and data-fusion applications determine what the observations can reveal.

1.4 From a Routine Observation to an Intelligence Product

Consider what happens when an ordinary vehicle passes a camera on an ordinary road. The initial record can be modest: a plate or vehicle description, time, camera, direction, confidence value, and location. That record becomes more valuable at each stage of the platform.

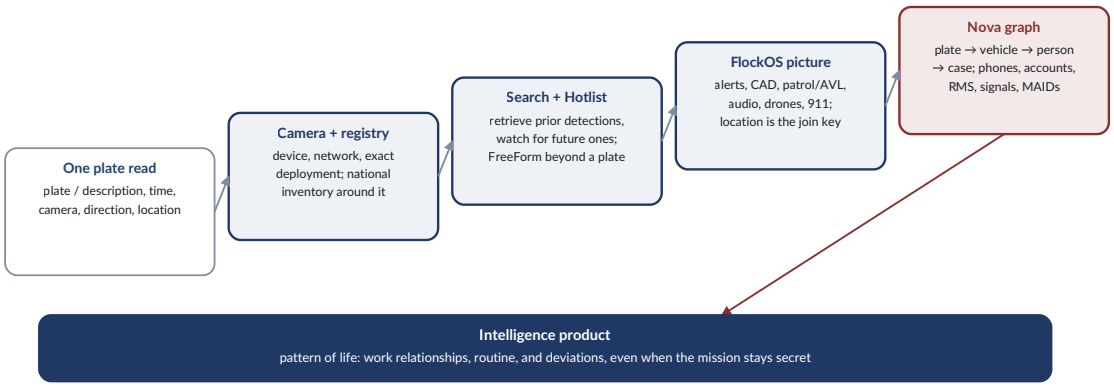


Figure 2. One plate read gains value at each stage: camera and registry context, Search and Hotlist continuity, the FlockOS operational picture, and Nova's relationship graph, until a routine observation becomes an intelligence product.

First, the camera and registry layers supply context. They identify the collecting device, its organization or network, its exact deployment point, its operational state, and sometimes its direction and health. The December export adds the national inventory around that observation, including nearby deployed and planned devices. An analyst is no longer looking at one sighting. The analyst can understand the collection geometry that produced it and the corridors likely to produce the next one.

Second, Search and Hotlist turn observations into continuity. A plate, vehicle description, time range, geographic area, camera group, saved filter, or alert reason becomes a way to retrieve prior detections or watch for future ones. FreeForm expands the target beyond a readable plate: a white work truck with a ladder rack, a vehicle with specific damage, or a person with described clothing can remain searchable. Regions of interest and selected camera groups turn an investigative question into a defined geographic collection plan.

Third, FlockOS places the target inside an operational picture. The map can combine camera and device layers with alerts, CAD incidents, patrol or automatic vehicle location (AVL) context, Raven audio events, drones, body-camera references, Flock911

events, and agency-defined custom layers. That common view matters because location is the join key. Events generated by different products become comparable when they appear at the same place and time.

Fourth, Nova converts the event into a relationship problem. A plate can lead to a vehicle, address, person, case, or scan history. A person can lead to phones, emails, online accounts, associates, RMS records, arrests, body-worn-camera events, or other organization data. Signals, registration identifiers, advertising identifiers, IP addresses, and location searches create additional ways to connect a digital device to a physical pattern. Each source may have its own entitlement, but Nova's product design is to place the results into one pivotable graph.[14]

The intelligence value lives in the joins. Any single observation, on its own, is ordinary. One plate resolved against a residence, a contractor facility, and an airport is a different object than the same plate seen once, and Nova's pivot graph is what performs that resolution.

This progression also explains why the four vulnerabilities cannot be evaluated as isolated web defects. The public bundles described the collection, search, map, and fusion workflows; the exposed credentials reached the geospatial control plane; and the production export supplied the deployment inventory. Together, the four vulnerabilities exposed and reached the machinery that turns commonplace road observations into intelligence.

2. Four Vulnerabilities, One Security Failure Chain

The four vulnerabilities remain numbered by submission order. That order should not be mistaken for severity. Vulnerability 1, the hardcoded Default API key, created the largest static blast radius. Vulnerability 3, the pre-login credential factory, created a separate way to obtain new production-scoped credentials. Vulnerabilities 2 and 4 exposed the application logic that made both credential failures more useful.

Vulnerability	First reported	Failure	Function in the chain
1	June 11, 2025	Production ArcGIS Default API key in public development/ demo assets	Exposed private geospatial scope and premium movement-analysis privileges

Vulnerability	First reported	Failure	Function in the chain
2	November 13, 2025	FlockSafety/FlockOS bundles delivered before the intended authentication boundary	Exposed search, alert, map, device, and emergency-response logic
3	November 13, 2025	Planner/Beefeater issued mapping credentials before login	Created the production credential path later used for the December export
4	December 5, 2025	FlockNova bundles delivered before the intended authentication boundary	Exposed identity, signal, records, LPR, dark-data, and pivot logic

I followed up on Vulnerabilities 2 and 3 on November 14 and 19. Flock reported Vulnerability 1 ameliorated on July 1, 2025. Flock provided no closure details for Vulnerabilities 2 or 3 and no reply or remediation details for Vulnerability 4 [L2].

I first found a credential in public files. I later found the FlockSafety application blueprint and a service that would issue new mapping credentials to an anonymous caller. Finally, I found the Nova data-fusion blueprint. Each discovery made the previous one more consequential.

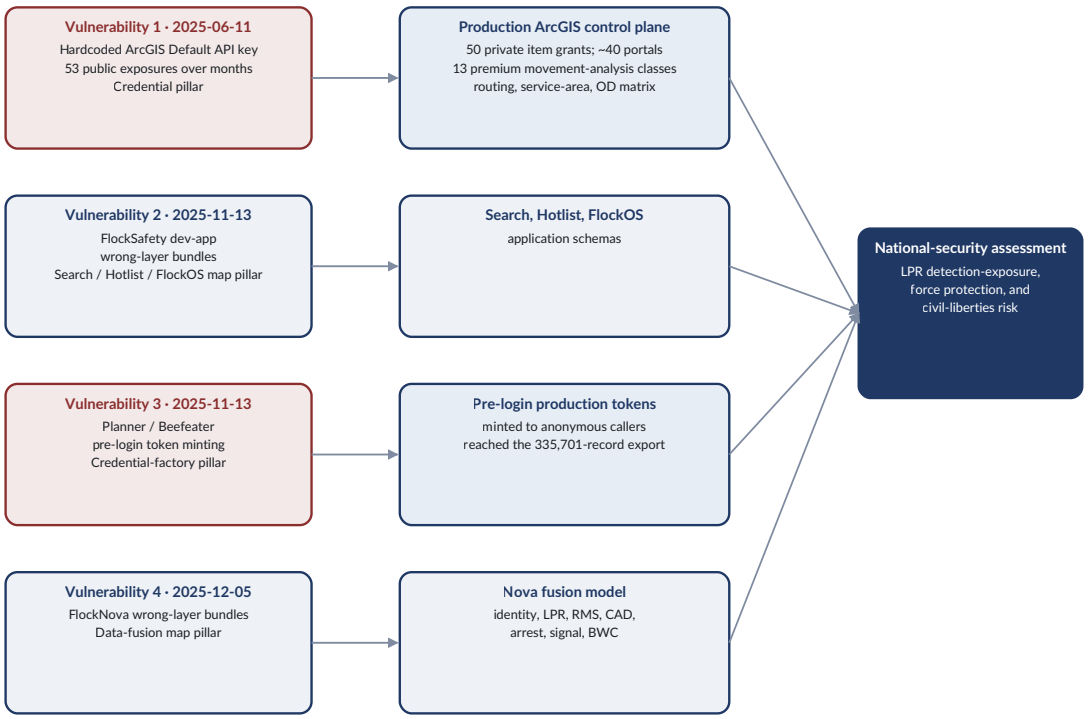


Figure 3. The public application maps and the two credential failures converge on the same production surveillance environment.

2.1 Vulnerability 1: A Production Geospatial Key Published 53 Times

Across the United States, license plate readers, drones, and audio sensors quietly record the movements of millions of people every day. Flock Safety operates one of the largest and fastest-growing of these networks. It comprises hundreds of thousands of cameras at the monthly-detection scale set out in Section 1.2, together with an undisclosed volume of people detections.[15]

At the center of this infrastructure is FlockOS, which Flock has marketed under the headline **“One map. Smarter Response.”** A Flock proposal describes its Esri-based interface as a map that “consolidates all data streams and the locations of each connected asset, enabling greater situational awareness and a common operating picture.”[16]

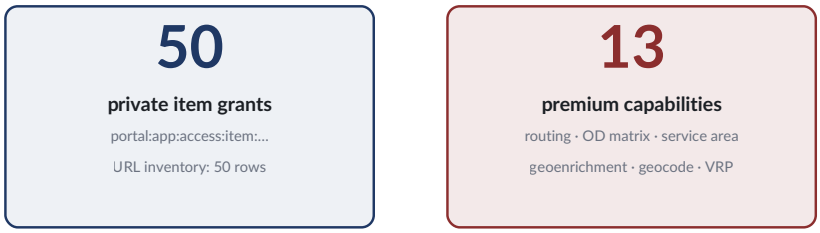
That “one map” is not a metaphor. It is an ArcGIS stack, and the exposed key unlocked the private geospatial scope assigned to it.

Vulnerability 1 began in a public development/demo environment. The assets contained what ArcGIS identified as a Default API key belonging to Flock's production organization. My published research documented 53 public instances.[17]

The repetition matters because it was not a harmless client identifier. The validation artifact records:

- **50 private ArcGIS item grants**;
- **13 premium ArcGIS capability classes**, which include basemap access, geocoding, geoenrichment, and the network-analysis services enumerated in Appendix C.1; and
- a direct role in the common FlockOS ArcGIS map component.[18]

Seven of the thirteen are movement-analysis functions: closest-facility analysis, location allocation, optimized routing, origin-destination cost matrices, routing, service-area generation, and vehicle routing. Appendix C.1 enumerates all thirteen. Those privileges are designed to answer movement questions. They can determine what is closest to a location, which routes connect two sets of points, what area is reachable within a threshold, or how many stops can be optimized into a route. Combined with private geospatial items and a national camera inventory, these are intelligence functions rather than cosmetic map features.



Vulnerability 1 damage model: not a cosmetic basemap token: a geospatial control-plane credential.
Published research documents 53 public exposures of this key class across development assets [P1, L20].

Figure 4. The direct credential facts are 50 private item grants and 13 premium capability classes.

Vulnerability 1 evidence plate F1-A. The unredacted repository view identifies the FlockSafety owner, the "Default API Key" title, active Location Platform context, the item-scoped privileges, and the premium capability list. The structured L8 artifact supplies the reconciled counts.

The client integration explains why the credential was so broadly important. The unified FlockOS component received the Esri key alongside base, dynamic, feature, marker, non-clustered-marker, clustered-marker, heatmap, focused-marker, selected-

layer, and custom-layer inputs. That component was the mapping substrate through which FlockOS assembled camera and device layers, agency layers, search results, alerts, incidents, and response assets.[19]

The ethical boundary and the OSINT reconstruction

I validated the grant count and service scope, but I did not open any of the 50 private items or collect police-department records behind them. Proving that the credential reached private content did not require me to acquire private third-party investigative records or personally identifiable information from those items. I stopped at that boundary.

I then used open-source intelligence to answer the blast-radius question without crossing it. I searched public ArcGIS portals and applications published by municipalities, police departments, and Flock itself; preserved the exposed schemas and screens; and compared them with FlockOS code, the December production export, and the key's privileges. A police-department employee responsible for ArcGIS separately confirmed that the department shared layers with Flock so the application could consume them.[20]

This method did not depend on guessing from product marketing. It found Flock camera inventories, mobile police-camera categories, detections, movement histories, camera-registry data, device-health records, future deployments, and municipal operational layers in ArcGIS form. The same FlockOS code accepted organization-specific ArcGIS item IDs or service URLs and rendered them in the common map. Together, those records provide a grounded reconstruction of the data classes likely represented among the private grants.

The blast-radius assessment rests on five connected evidence classes:

1. the key's validated private grants and premium services;
2. the FlockOS and application code showing how ArcGIS was integrated;
3. the production device export obtained through Vulnerability 3;
4. Flock-related ArcGIS layers published by agencies and Flock, which corroborate the data classes; and
5. the participating police department's confirmation of the layer-sharing architecture.

Taken together, the evidence supports the assessment that the key likely reached the private ArcGIS-backed data used by the common FlockOS mapping plane across Flock's full reported customer environment (Section 1.2). The key was not a complete FlockOS user session; it was a production geospatial credential with extensive private-

item and movement-analysis authority. Separate Flock APIs handled some live events and media, but the exposed credential still held the private item grants and movement-analysis authority that made the operational map valuable.

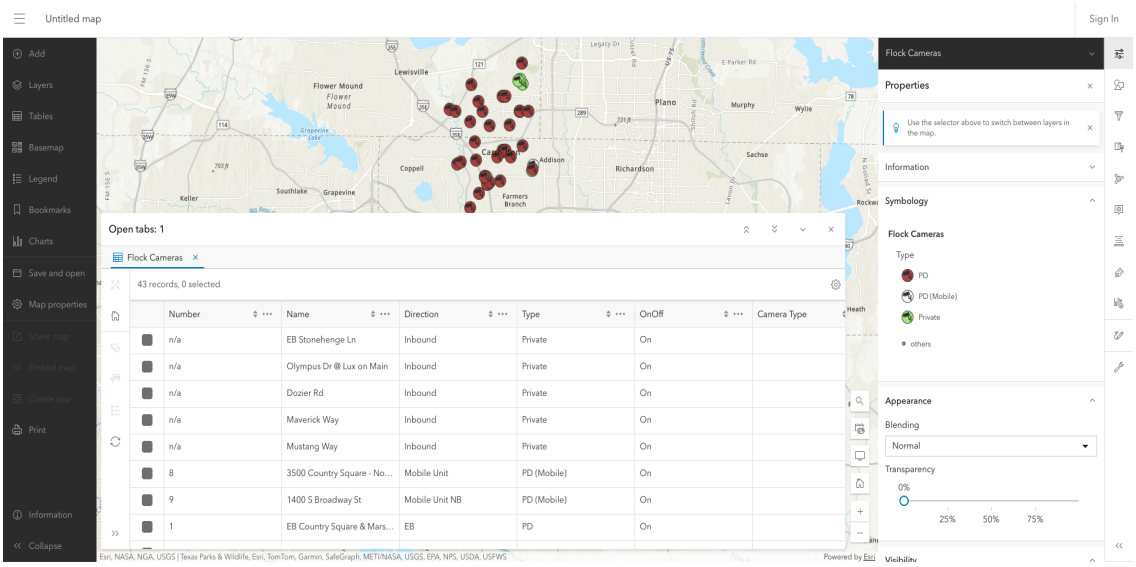
What the map plane represented

The public ArcGIS applications, FlockOS code, and production export show that the environment represented substantially more than camera dots:

Information family	Data represented in the connected evidence	Principal support
Surveillance infrastructure	Camera deployments operated by police departments, communities, and private businesses; third-party devices connected through Wing Gateways; Raven gunshot-detection sensors; trailers; and drone assets with live state.	[L10, L13-L15, L25, P1]
Law-enforcement location and response	Live and historical patrol-car and AVL positions; mobile police-camera categories; Axon body-worn-camera locations; officer mobile-app objects for phones and watches; trailers and auxiliary GPS trackers; CAD event geography; patrol history; and response context.	[L10, L13, L25, E80, P1]
People, vehicle, and audio intelligence	People-detection alerts with camera IDs, time windows, confidence, expiration, and map location; people searches rendered as tracked map objects; plate and vehicle alerts; persisted vehicle searches; visual alerts; and Raven audio classifications such as single versus multiple shots.	[L11-L13, L21, L23, P1]
Hotlists and investigative geography	Topic names, alert reasons, filter and deduplicated-detection IDs, plates, timestamps, locations, case and note fields, hit history, saved-search filters, camera groups, and the polygons or radii investigators drew around an area of interest.	[L11-L13, L21, L23, P1]

Information family	Data represented in the connected evidence	Principal support
Personally identifiable registry data	Camera-registrant names, email addresses, phone numbers, postal addresses, law-enforcement/non-law-enforcement/private location types, interior and exterior camera counts, and associated camera-location arrays.	[L10, L22, P1]
Camera registry and asset health	Physical deployment points, device serial numbers, uptime percentages, operating state, Flock support and service metadata, direction, network and organization identifiers, device capabilities, and planned deployment records.	[L14, L15, L24, L25, P1]
Flock911 emergency data	Live incident locations, call IDs, transcript and audio access-token classes, per-word transcript timing, audio scrub and playback state, duration, incident classification, and active/selected incident identifiers.	[L12, L13, P1]
Drone telemetry	Drone/video device records, livestream capability, network and organization context, and rendered states including `Docked`, `Buffering`, `Recording`, `Inactive`, `Offline`, `Off`, `ON`, `ONLINE`, `ACTIVE`, `Charging`, and `Uploading`.	[L13, L35, P1]

The following plates are the original visual exhibits from my January 2026 publication. Their source URLs, exact hashes, and uncombined originals are recorded in `Supporting Tools and Docs/master_report/figures/finding1/README.md`.[21]

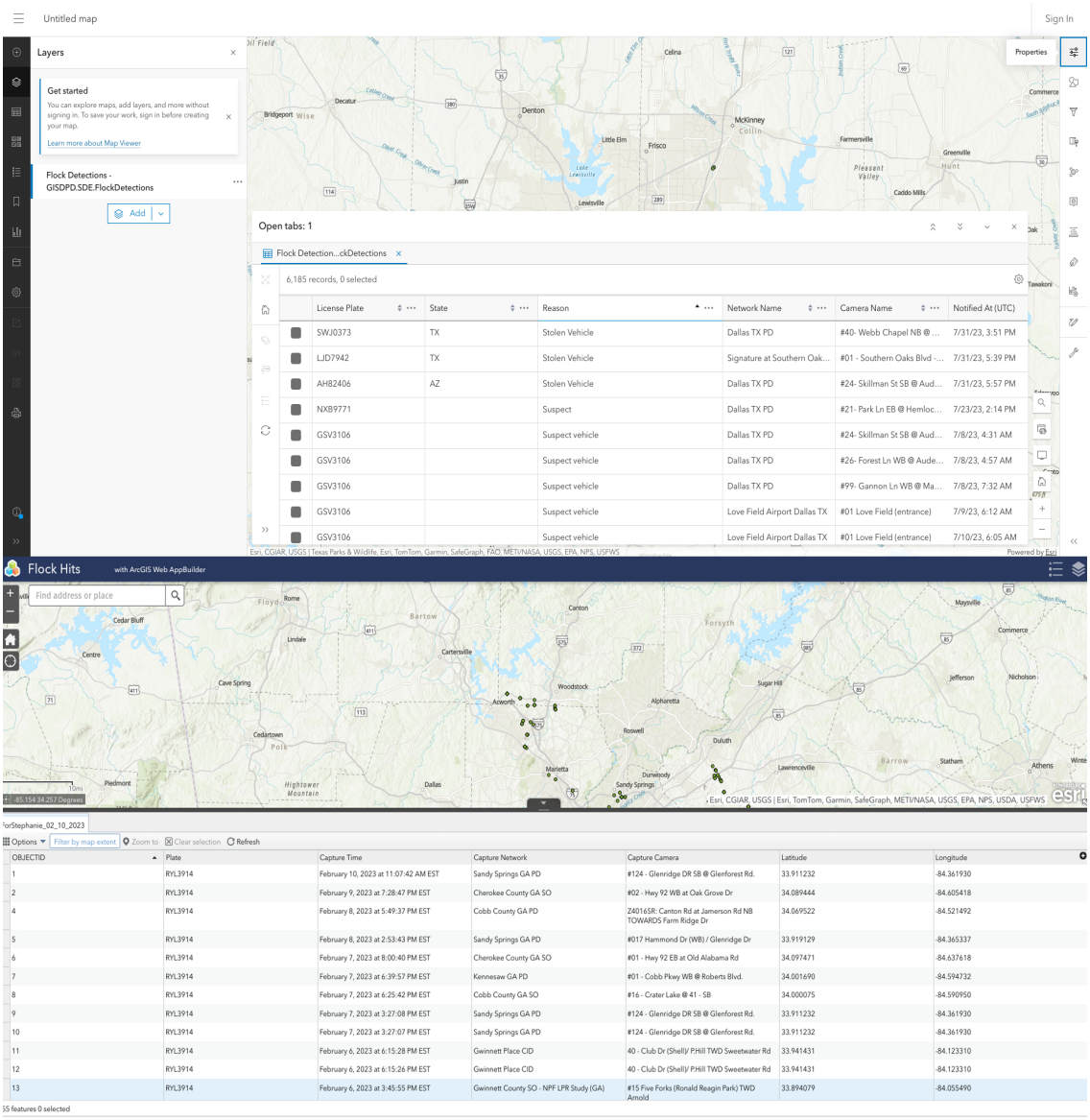


Vulnerability 1 evidence plate F1-B. A publicly exposed ArcGIS map placed fixed police cameras, mobile police units, and private cameras in one layer and displayed their locations, directions, on/off state, and camera category.

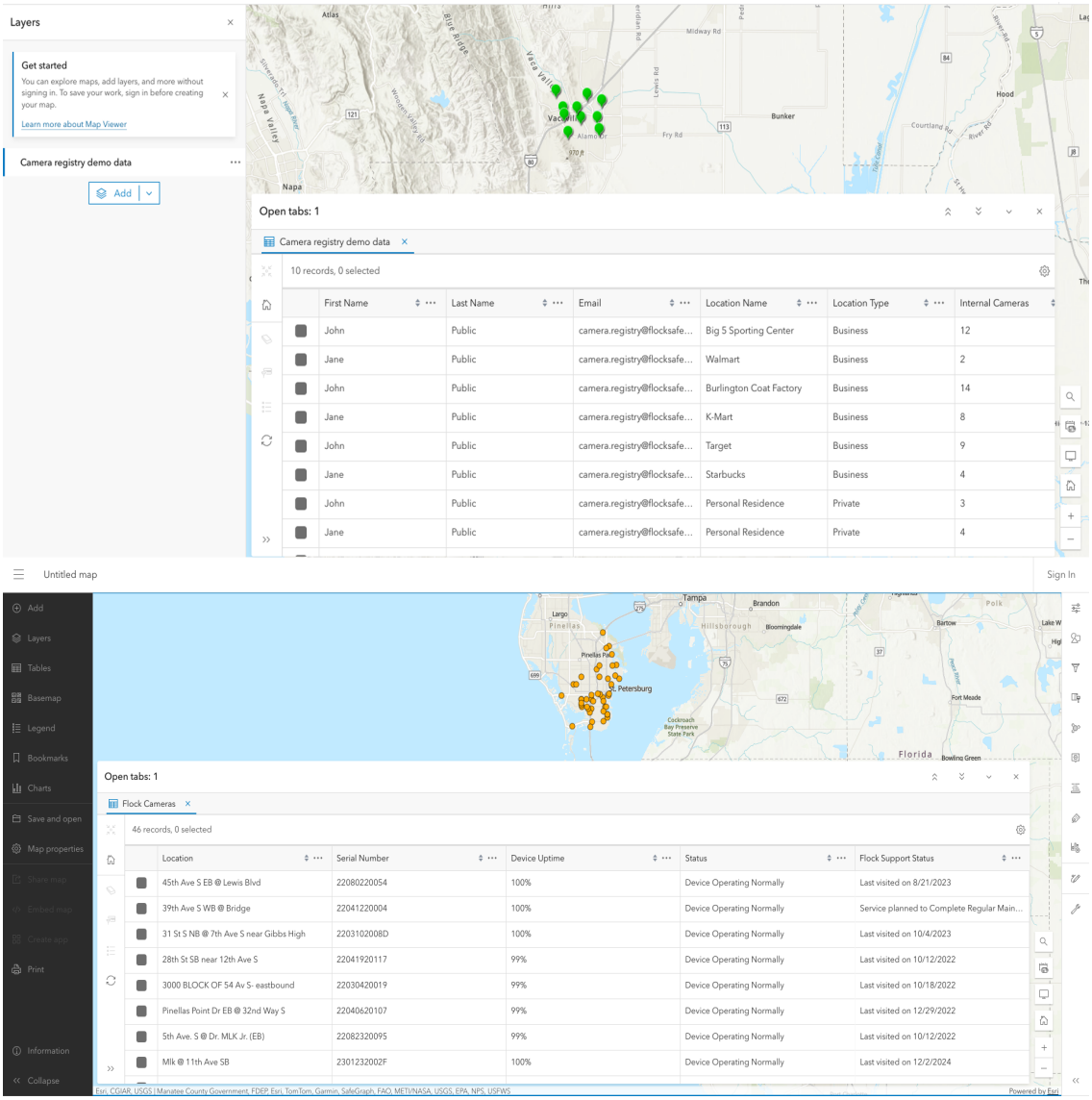
```
xF = {
  installationType: sE.InstallationType.wing,
  direction: 0,
  externalId: "46531e04-46bd-4848-bfff-3f7d12f8c4b6",
  id: 166343,
  name: "C#006 E McKellips @ N Miller (PTZ)",
  networkExternalId: "4bb91cf0-f80f-11ee-871c-5319aa54f1ae",
  networkId: 18928,
  organizationId: "535c3095-ed00-40be-923e-1b9d2c890669",
  rotationAngle: 0,
  lat: 33.45114346019635,
  long: -111.91804697648517,
  networkName: "Scottsdale AZ PD Cameras",
  type: "public",
  features: [sk.livestream],
},
```

```
return {
  type: "RealTime",
  localization: { lat: e.lat, lng: e.lng, address: e.address },
  aboutSection: [
    { label: "Source", value: "Person Detection Alert" },
    { label: "Alert Name", value: e.policyName },
    { label: "Reason", value: e.reason },
    { label: "Description", value: o_(e) },
    {
      label: e.address ? "Location" : null,
      value: e.address || null,
    },
    ...i,
  ],
  detailsSection: [
    { label: "Device", value: e.cameraName },
    { label: "Location", value: a },
    { label: "Network", value: e.networkName },
  ],
  resultsSection: [
    { label: "Audience", value: "Custom" },
    { label: "Roles", value: "SELECTED ROLES" },
    { label: "Users", value: "SELECTED USERS" },
    { label: "Confidence", value: "Confidence if we have it" },
  ],
  scheduleSection: [],
```

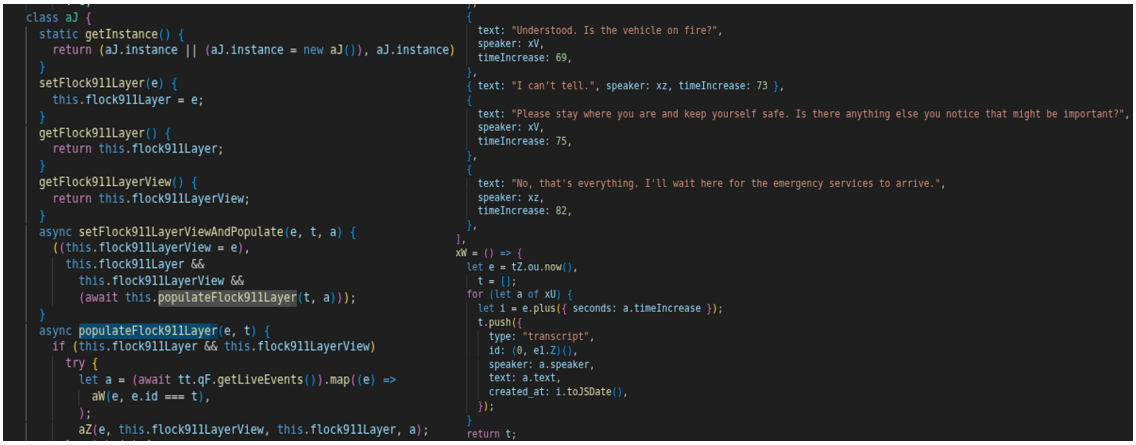
Vulnerability 1 evidence plate F1-C. Left: a Flock device object includes a Wing installation type, police-camera network, exact coordinates, and livestream capability. Right: the people-detection alert model includes source, policy, reason, description, address, camera, network, audience, roles, users, and confidence.



Vulnerability 1 evidence plate F1-D. Top: a public Dallas ArcGIS layer exposed Flock detection records with plates, reasons, networks, cameras, and timestamps. Bottom: a separate Flock Hits application plotted one plate's observations across agencies, cameras, times, and coordinates.



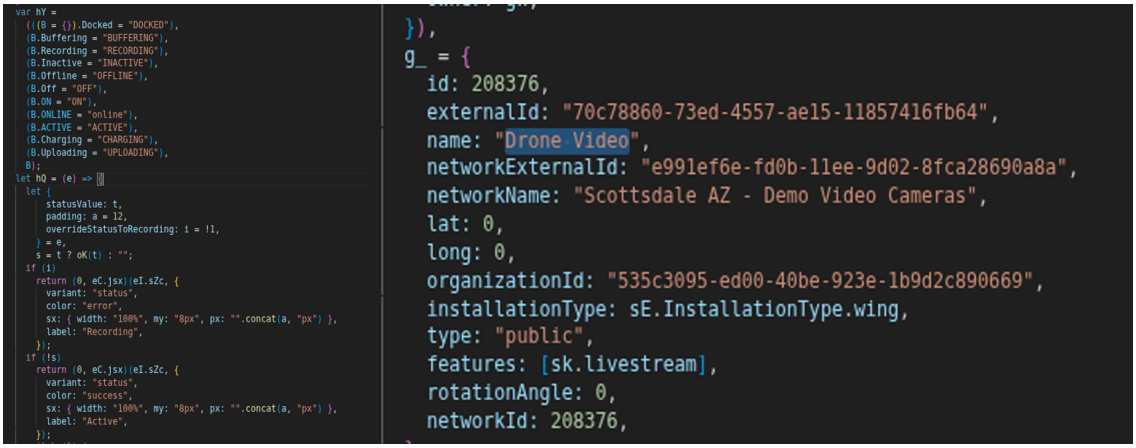
Vulnerability 1 evidence plate F1-E. Top: a camera-registry ArcGIS layer exposed registrant, email, location, location-type, and camera-count fields. Bottom: a municipal camera layer exposed deployment locations, serial numbers, uptime, operational state, and Flock support history.



```
class aJ {
  static getInstance() {
    return (aJ.instance || (aJ.instance = new aJ()), aJ.instance)
  }
  setFlock911Layer(e) {
    this.flock911Layer = e;
  }
  getFlock911Layer() {
    return this.flock911Layer;
  }
  getFlock911LayerView() {
    return this.flock911LayerView;
  }
  async setFlock911LayerViewAndPopulate(e, t, a) {
    ((this.flock911LayerView = e),
      this.flock911Layer &&
        this.flock911LayerView &&
        (await this.populateFlock911Layer(t, a)));
  }
  async populateFlock911Layer(e, t) {
    if (this.flock911Layer && this.flock911LayerView)
      try {
        let a = (await tt.qF.getLiveEvents()).map((e) =>
          aW(e, e.id === t),
        );
        aZ(e, this.flock911LayerView, this.flock911Layer, a);
```

```
{
  text: "Understood. Is the vehicle on fire?",
  speaker: xV,
  timeIncrease: 69,
},
{ text: "I can't tell.", speaker: xz, timeIncrease: 73 },
{
  text: "Please stay where you are and keep yourself safe. Is there anything else you notice that might be important?",
  speaker: xV,
  timeIncrease: 75,
},
{
  text: "No, that's everything. I'll wait here for the emergency services to arrive.",
  speaker: xz,
  timeIncrease: 82,
},
],
xW = () => {
  let e = tZ.ou.now(),
    t = [];
  for (let a of xU) {
    let i = e.plus({ seconds: a.timeIncrease });
    t.push({
      type: "transcript",
      id: (0, e1.Z)(),
      speaker: a.speaker,
      text: a.text,
      created_at: i.toJSDate(),
    });
  }
  return t;
```

Vulnerability 1 evidence plate F1-F. FlockOS code populated live Flock911 events into a dedicated ArcGIS layer and represented transcript entries with speaker, text, creation time, and relative timing.



```
var hY =
  ((B = {}).Docked = "DOCKED"),
  (B.Buffering = "BUFFERING"),
  (B.Recording = "RECORDING"),
  (B.Inactive = "INACTIVE"),
  (B.Offline = "OFFLINE"),
  (B.Off = "OFF"),
  (B.ON = "ON"),
  (B.ONLINE = "online"),
  (B.ACTIVE = "ACTIVE"),
  (B.Charging = "CHARGING"),
  (B.Uploading = "UPLOADING"),
  B);
let hQ = (e) => {
  let {
      statusValue: t,
      padding: a = 12,
      overrideStatusToRecording: i = !1,
    } = e,
    s = t ? oK(t) : "";
  if (i)
    return (0, eC.jsx)(eI.sZc, {
      variant: "status",
      color: "error",
      sx: { width: "100%", my: "8px", px: "".concat(a, "px") },
      label: "Recording",
    });
  if (!s)
    return (0, eC.jsx)(eI.sZc, {
      variant: "status",
      color: "success",
      sx: { width: "100%", my: "8px", px: "".concat(a, "px") },
      label: "Active",
    });
```

```
}),
g_ = {
  id: 208376,
  externalId: "70c78860-73ed-4557-ae15-11857416fb64",
  name: "Drone Video",
  networkExternalId: "e991ef6e-fd0b-11ee-9d02-8fca28690a8a",
  networkName: "Scottsdale AZ - Demo Video Cameras",
  lat: 0,
  long: 0,
  organizationId: "535c3095-ed00-40be-923e-1b9d2c890669",
  installationType: sE.InstallationType.wing,
  type: "public",
  features: [sk.livestream],
  rotationAngle: 0,
  networkId: 208376,
```

Vulnerability 1 evidence plate F1-G. FlockOS rendered operational drone/device states and included a livestream-capable Drone Video record in the shared device model.

Integrity was also at issue

One production camera FeatureServer advertised Create, Update, Delete, attachment, and query capabilities while separately permitting anonymous query.[22] ArcGIS capability metadata describes operations the service supports for an authorized editor; I did not attempt a write. Defenders still had to verify the authorization boundary. If a leaked or under-scoped credential could exercise those operations, an actor could move, relabel, forge, or delete camera records and attachments on a map agencies use as coverage ground truth.

The result is a confidentiality and integrity problem. An exposed geospatial credential can disclose where collection exists and where it is planned. An improperly scoped editor can corrupt the same picture used to make operational decisions.

2.2 Vulnerability 2: The FlockSafety Application Blueprint Before Login

Vulnerability 2 concerned where authentication was enforced. The visible web route could present a login screen while the static asset server and module-federation loader still served the application's JavaScript before authorization. Anyone who could fetch the assets could read the endpoint names, request shapes, feature flags, permission vocabulary, map construction, storage conventions, and data models.

The October 2025 host snapshot contains 370 scoped `flocksafety.com` hosts. Within the wider research corpus were development, staging, preview, API, government, authentication, observability, device, camera, streaming, and internal-service families. A strict development/preview/staging subset contained 213 names.[23] This was not one abandoned test page. The environment exposed a broad collection of application families and PR-preview surfaces.

The downloaded bundles described:

- Search/Monaco plate, vehicle, people, FreeForm, camera-selection, geofence, case, and reason workflows;
- Hotlist/Strawberry-Soju watchlists, hit history, alerts, people-detection filters, schedules, regions of interest, drone and CAD flags, and emergency-response integrations;
- the FlockOS notification and map plane, including CAD, patrol assets, Raven audio, people and vehicle alerts, drones, body-camera references, and Flock911 events;
- camera, device, sharing, planning, stream, and administrative surfaces; and
- module-federation relationships tying those functions into one browser shell.[24]

Source exposure is not the same as universal backend access. The security failure is that Flock delivered a detailed operational map of the product before the intended authentication boundary. The separate key validation and Beefeater captures establish the production-access paths. Together, the vulnerabilities gave an outside researcher both the blueprint and credentials connected to the geospatial plane.

2.3 Vulnerability 3: A Credential Factory Before Authentication

Vulnerability 3 was more than another leaked string. Four hosts formed one token path:

Host family	Function
`planner.flocksafety.com`	Production planning frontend requesting mapping credentials before login
`dev-planner.flocksafety.com`	Development frontend with the same request pattern
`beefeater.flocksafety.com`	Service issuing ArcGIS and Google mapping credentials
`dev-beefeater.flocksafety.com`	Development service that still issued production-scope ArcGIS credentials

The preserved HTTP captures show anonymous requests returning HTTP 200 and usable credentials without a cookie or Authorization header.[25] The evidence therefore rests on response behavior, not an endpoint name discovered in JavaScript.

Three control failures were present. Credentials were issued before authentication. Development infrastructure could mint production-scope authority. The request lacked an authenticated person or tenant against which issuance could be authorized and audited. A public map may need a narrowly scoped browser token; it does not need an anonymous service that can mint credentials reaching a national production deployment inventory.

Vulnerability 1 and Vulnerability 3 are independent. Rotating the hardcoded Default API key would close one static exposure. It would not repair an unauthenticated service capable of issuing fresh credentials. That distinction is why both vulnerabilities remain critical.

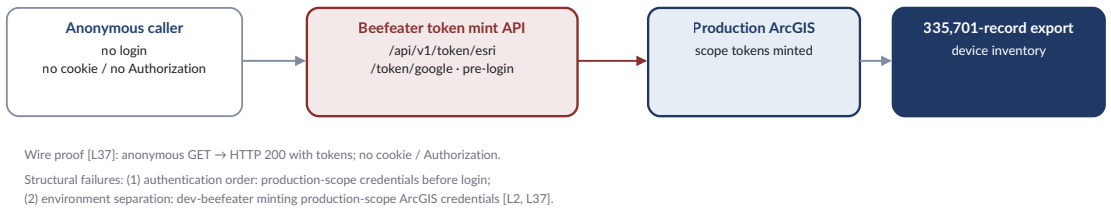


Figure 5. The development and production Planner clients reached Beefeater token endpoints before authentication; development infrastructure also crossed into production scope.

2.4 Vulnerability 4: The Nova Data-Fusion Blueprint Before Login

Vulnerability 4 applied the same wrong-layer problem to FlockNova. The exposed bundles contained 148 JavaScript files from the preserved Nova application tree. They described how the product established sessions, refreshed tokens, interpreted claims, selected organizations, required case information, classified freeform inputs, fanned searches out to data sources, and organized returned records into a pivot graph.[26]

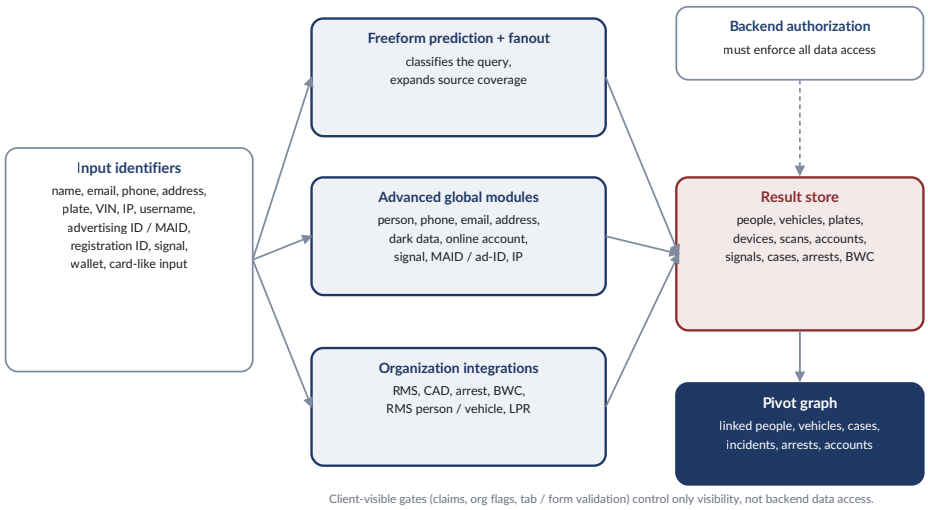


Figure 6. FlockNova resolves entered identifiers into one pivotable graph, fanning a query across advanced modules and organization integrations into a shared result store; client-visible gates control only visibility, not backend data access.

The visible source taxonomy included:

- names, emails, phones, addresses, Social Security numbers, plates, VINs, IP addresses, usernames, businesses, keywords, cryptocurrency addresses, and payment-card-like values;
- person, address, online-account, signal, advertising-ID, device-registration, location, and dark-document modules;
- RMS cases and persons, CAD events, arrests, body-worn-camera events, vehicles, LPR results, warrants, inmates, guns, property, traffic events, ballistics, trafficking, and Internet Crimes Against Children (ICAC) categories; and
- relationship helpers that connected people, vehicles, plates, addresses, accounts, devices, cases, incidents, arrests, and other records.[27]

The client exposed several access concepts: decoded claims, organization feature flags, tab visibility, search-reason and case fields, and form validation. Those controls did not all serve the same purpose. Case and reason fields were usage and audit metadata. Tabs and form checks controlled presentation. Backend authorization still had to enforce

every source, tenant, field, pivot, and export. In the freeform path, missing claims could visibly suppress some network calls; the advanced and organization modules relied more heavily on the backend once a visible form was submitted.

The shared-build evidence also weakened a simple “demo only” explanation. The route wrapper treated `nova.flockdemo.com`, `app.flocknova.com`, and `stage.flocknova.com` as one application family, alongside connected Lucidus, CodeFour, and Healthcare Safely domains.[28] The exposed code was a product blueprint, not a decorative mock-up.

2.5 Why the Chain Is Systemic

Any company can make one deployment mistake. The pattern here crossed distinct controls:

- a broadly scoped production credential was embedded repeatedly in public assets;
- development and preview environments exposed production-relevant application logic;
- development infrastructure could issue production-scope credentials;
- two major application families enforced authentication at the wrong delivery layer;
- client-side entitlement and presentation logic exposed how sensitive sources were organized;
- a bulk production export could be obtained through the anonymous credential path; and
- live-video, edge, mobile, and government-tier surfaces widened the same trust boundary.

The defects amplified each other. The bundles revealed what to ask for and how the products joined data, the key and token factory supplied the geospatial authority, and the export showed the national deployment scale. FlockOS and Nova showed how deployment data, detections, incidents, identities, signals, and agency records could be combined. The security conclusion depends on the whole chain, not on any single frontend file being a complete compromise.

3. The December Export and Flock's Accounting Problem

Vulnerability 3 created a test that the earlier vulnerabilities could not. A hardcoded key meant a credential had escaped. The anonymous token response meant a service was handing out credentials at the wrong boundary. The December export went further, reaching consequential production data.

I obtained the export on December 14, 2025, 31 days after the initial Vulnerability 3 report. It contained 335,701 rows representing devices and planned or historical deployments. The records included names, identifiers, device types, operational status, organization and network relationships, parent/child relationships, capabilities, geometry, and other deployment metadata. Exact coordinates and the row-level fields remain in the evidence package, with one exception: five identifier fields (`externalId`, `networkExternalId`, `organizationId`, `networkId`, `parentExternalId`) were emptied in the published copy, and the complete record is retained offline.[29]

Source status	Records	Meaning in this report
`inService`	214,073	Source-labeled operational device records
`inPlanning`	83,427	Intended or planned deployment records
`decommissioned`	38,190	Excluded from the reachability camera filter
Unknown	11	Retained in the source count but excluded from the primary filter
Total	**335,701**	Complete December 14 export

These were not aggregate counts. The rows carried geometry and operational metadata that made the inventory usable: physical deployment coordinates, device and external identifiers, names, types, capabilities, status, organization or network relationships, and parent-child references. Creator and editor fields recorded ArcGIS ownership or edit identities for the feature records; they did not establish that every named account was a Flock employee. `parentExternalId` linked a component or child record to a parent asset

in Flock's device model. Taken together, those fields allow a reviewer to distinguish a detection-capable camera from a co-located component, associate devices within a deployment, and reconstruct how the mapped inventory was organized.[30]

That structure is why the export has national-security value even without historical plate-read data. It identifies current and intended collection positions, reveals concentrations and gaps, distinguishes device families, and shows relationships among assets and organizations. Planned coordinates can expose where coverage is expected before hardware becomes operational. Parent-child and capability fields can reveal which records belong to a larger sensor package and which functions a deployment may support. A national inventory also makes local anomalies easier to find. An analyst can compare one installation's approaches with the vendor's wider deployment pattern instead of studying isolated public camera sightings.

The installation study used only the fields needed for its declared camera filter and geospatial model. The full export supports a broader asset and control-plane assessment preserved in Appendix G. The route results are only one analysis drawn from the inventory, not the limit of what it reveals.

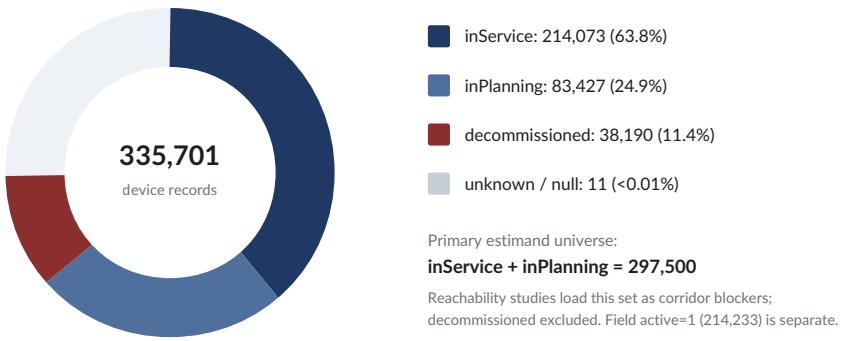


Figure 7. The primary study filter uses the 297,500 records whose source status is inService or inPlanning.

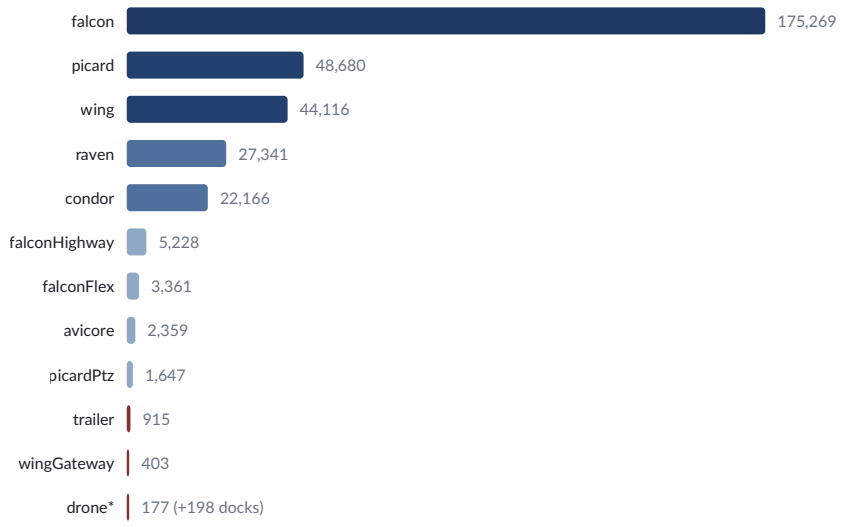


Figure 8. The largest device families in the 335,701-record export; mobile, trailer, and gateway conversion classes point to growth beyond fixed license-plate poles.

The integer field `active` is not interchangeable with `status`. The export contains 214,233 rows with `active=1`, 160 more than the 214,073 rows marked `status=inService`. The study therefore uses the declared `status` values rather than treating the separate integer as a substitute.[31]

Planned deployments are security-relevant even before installation. They reveal where a vendor and its customers intend to add collection, which corridors are being prioritized, and how coverage may develop. The export inventory in this section keeps the original `inPlanning` label and does not relabel those rows as active. In contrast, the installation study in Sections 4 and 5 treats a device planned in the December 2025 snapshot as operational because the studies ran eight months later. Section 4.3 states this dated assumption and provides a reproducible `inService`-only floor.

3.1 The Event Flock Was Not Separately Told About

I reported the token path before obtaining the export. I also sent two follow-ups. I did not send a separate message saying that I had used the still-available path to acquire the production inventory. That decision created a clean question for access accounting. Would Flock identify a bulk retrieval without relying on the researcher to describe it afterward?

Flock's January security page offered categorical assurances rather than an answer. In three formulations, it said the company had never been hacked or suffered a leak, that its cloud infrastructure had never been compromised or customer data accessed or exfiltrated, and that it had never had a data breach or customer data compromised. Its March cybersecurity post reinforced the denial, labeled the January claims false or misleading, attacked a November video featuring this report's author, and declared that Flock would continue to lead the industry in cybersecurity.[32]

Two interpretations remain:

1. **Flock accounted for the access.** If the company knew or later determined that the export occurred, its public language excludes the event from several broad security terms without telling readers what was excluded or why.
2. **Flock did not account for the access.** If the company did not identify the retrieval, the anonymous credential path supported bulk production-data access without effective detection, attribution, or escalation.

Neither answer supports categorical confidence in the platform's monitoring. In the first case, the public assurance is incomplete. In the second, the assurance rests on controls that failed a known real-world test. The responsible nature of my work changes the actor's intent; it does not change what the path allowed or what the company's telemetry should have recorded.

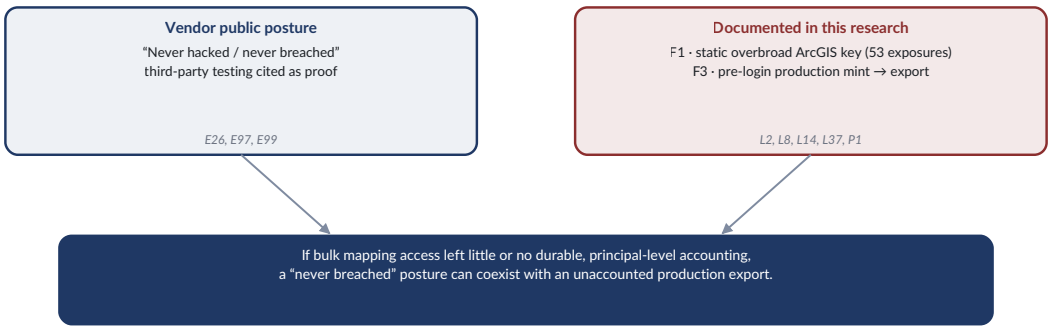


Figure 9. The documented access event turns Flock's public posture into a testable accounting question.

Vulnerability 1 raises the stakes. Flock had already published a private-item-capable Default API key 53 times. Vulnerability 3 then supplied fresh credentials before login. Without reconstructable logs, reviewers cannot determine who else used those paths or how long similar access could persist undetected.

Independent reporting about open camera feeds, Flock's acknowledged Condor configuration issue, and published edge-device research concern different technical events. They do not prove use of the ArcGIS paths. They do show why a national surveillance vendor should support its security claims with auditable access records rather than categorical marketing language.[33]

4. How the Installation Study Worked

The export answered where Flock devices were recorded. The reachability study asks **what share of modeled ordinary public-road round trips from the off-installation residential market to reviewed 24/7 gates would have no recorded operational camera observation?**

The V7 cohort covers 22 sites spanning military installations, federal headquarters, and defense-contractor and federal-laboratory headquarters; Section 5 lists the set and its classes.

4.1 Why Five and Twenty Miles

Each study run creates two nested views from a single frozen 20-mile frame:

- **5 public-road miles per directional leg** isolates the near-base corridor, where traffic converges toward a small set of gates.
- **20 public-road miles per directional leg** is the primary standardized commuting-area result. DoD housing guidance permits a housing-market boundary based on 20 miles or one hour of peak-traffic travel, with local adjustment.[34]

The engine draws 1,000 occupied-housing-weighted observations from the 0-5-mile stratum and another 1,000 from the greater-than-5-to-20-mile stratum. The 5-mile artifact contains the near stratum. The 20-mile artifact contains those exact 1,000 draws, routes, gates, and camera observations unchanged, then adds the 1,000 outer-stratum draws. The primary 20-mile estimate weights both strata by their represented occupied housing; it is not a simple average of the two samples.

This design makes the difference interpretable. The two views share one source frame and one near-base sample, so a change reflects the measured difference between the near and outer residential markets rather than two unrelated town-balanced samples.

4.2 Why Only 24/7 Gates

The route model includes only gates manually reviewed as continuously available to authorized traffic. A part-time, visitor-only, commercial-only, or schedule-limited gate cannot be treated as a dependable commute route. Including one would create modeled trips that disappear when the gate closes.

Gate selection is installation-specific and remains reviewable in the complete record. For each origin-access hypothesis, the engine routes every saved gate within the stratum's directional road-mile limit and selects the gate with the lowest actual round-trip travel time whose route legally crosses the protected boundary at the saved gate and returns legally. Selection is made from full point-to-point routing rather than a distance-matrix approximation, so a gate on a divided road is not penalized by edge-snapping. A hypothesis with no legal ordinary round trip fails closed; if no hypothesis produces a resolved outcome, the draw becomes `excluded_unroutable`, remains in the full weighted denominator, and is counted in the unresolved-rate QA check. Study generation never moves or deletes gates, blockers, boundaries, or cantonments.

4.3 Origins, Roads, and Camera Eligibility

The origin frame uses 2020 Census occupied housing at block geography. Frozen OpenStreetMap residential buildings and address nodes provide residential access points inside each occupied block; each carries a human-readable `origin_address` from the OSM `addr:*` tags, and a block's representative point is used only where the block has no mapped residential point. A maximum of four points represents one block, and the block's occupied-housing weight is divided across those points. Origins are public residential sampling points. No occupant, identity, or affiliation is determined or claimed, and no sampled home is treated as a military household.

Candidates inside the protected target polygon are excluded, then Valhalla tests public-road reachability to every saved gate in both directions. The minimum across gates of the larger outbound or return distance assigns each candidate to exactly one distance stratum. Sampling is deterministic from the recorded seed and proportional to occupied housing within each stratum. Town names are descriptive labels assigned after sampling; towns do not determine the weights.

A residential point can be plausibly accessible from more than one nearby road. The model searches vehicle-routable corridors within 150 meters, deduplicates them into at most three bounded hypotheses, pins each hypothesis to its selected physical way with a 2-meter route radius, and nudges a shared intersection endpoint up to 8 meters into that

way when needed to escape Valhalla's 5-meter node snap. Each H0/H1/H2 hypothesis is routed independently. The model asserts `unobserved` or `confirmed_exposure` only when every complete supported hypothesis agrees; disagreement or incomplete access evidence remains `possible_exposure` and expands the origin-access uncertainty bound.

Routing uses a pinned Valhalla 3.6.3 container and a hashed, frozen OpenStreetMap extract. Valhalla's `auto` costing supplies ordinary travel-time routes using mapped road hierarchy, access rules, one-way restrictions, turn restrictions, and ramp transitions. Manual blockers remain active as analyst-declared road restrictions. Camera locations are absent from route and gate selection, so a camera cannot cause a highway exit, frontage-road bypass, gate change, or other evasive behavior. For every retained access hypothesis, Valhalla generates a camera-blind outbound route to the fastest in-scope 24/7 gate and an **independent legal return route**. Exposure is scored on both actual directed legs. A missing, illegal, or untraceable return is not replaced with a reversed outbound geometry; it fails that hypothesis closed.

Detection eligibility is centralized in the study code. A record is eligible when its `status` is `inService` or `inPlanning` and it is a retained detection device. Every retained detection device supports Flock's FreeForm vehicle search, so all such records are treated as vehicle-detecting and no capability sub-filter is applied; the device `type` field is not used to gate detection, because it is unreliable (a device tagged `Condor Trailer`, for example, can in fact be a pole PTZ with a Picard pack). Both statuses are treated as **operational**. The camera snapshot was pulled in December 2025 and the studies were run in August 2026, so a device sited as planned at snapshot time is treated as deployed roughly eight months later. This is a stated, dated assumption; each counted planned record keeps its `inPlanning` label on the observation, and the conservative `inService`-only floor is reproducible from the same code (`COUNT_PLANNED_AS_OPERATIONAL = False`). Decommissioned rows and support-only devices such as talkdown speakers and backhaul boxes are excluded. Co-located components are treated as part of the associated device rather than independent coverage.

4.4 The Vehicle-Fingerprint Camera Model

The camera model is a **vehicle-fingerprint field-of-view overlay** applied only after the route geometry is fixed. It replaces the earlier strict directional plate-read overlay, which counted a trip as exposed only when the route traversed a camera's assigned directed edge, in the camera's travel direction, within 75 feet. That earlier rule modeled a directional license-plate read and understated the device's observation capability. A Flock camera can make the wider scene searchable. This includes make, model, color,

occupants, and FreeForm person and vehicle queries, extending well beyond the plate window. A camera therefore observes a vehicle on a route leg when **both conditions** are met:

- **Range.** The route passes within the camera's capture range. The overlay records every camera out to a maximum 250 feet; the headline status uses a primary **150-foot** field of view. The 75/150/250-foot exposure curve (Section 5) reports all three so no single range has to be defended, and the 75-foot point is the closest analogue to the retired plate rate.
- **Direction and corridor.** The vehicle is traveling in the camera's monitored direction within 35° and the route has positive same-corridor evidence. Crossing, parallel-frontage, grade-separated, and oncoming traffic are not counted as confirmed exposure. Nearby ambiguous encounters remain in the spatial-sensitivity record.

Direction is derived from the road, not from the device's `rotationAngle`. Validated against 72,971 in-service imaging cameras that also carry an NB/SB/EB/WB name, `rotationAngle` aligns to the road axis only about 10% of the time (median error 90°); it encodes housing orientation, not travel. For a named-direction camera the monitored bearing is therefore the true road bearing at the camera, with the compass name used only to pick which of the two travel senses. A directionless, intersection-named camera takes its road axis from `rotationAngle ± 90°`; because that is noisy, such a camera is retained only as a *possible* observation and only when the vehicle travels along that axis, which drops the cross-street and parallel-road cameras that bare proximity would over-count.

The complete artifact records every weighted draw, Census block identifier, exact synthetic origin and address, bounded access hypothesis, selected gate, rejected gate options, independent outbound and return geometry, camera observation, direction/corridor/assignment evidence, source and implementation hash, uncertainty field, and run parameter.[35]

4.5 Reading the Outcome Classes

Each independently routed access hypothesis receives one status under the range, direction, and same-corridor test. The all-hypotheses lattice then gives every draw one of four mutually exclusive primary statuses:

- **Confirmed exposure:** every complete supported access hypothesis encounters at least one direction-confirmed same-corridor camera within the primary field of view.

- **Possible exposure:** the hypotheses disagree, a direction is unresolved, or the access set is incomplete, truncated, or weakly supported.
- **Unobserved:** every complete supported hypothesis encounters no operational camera on either independently routed leg.
- **Excluded unroutable:** no legal, traceable route outcome can be established. Its weight remains in the denominator and is reported as unresolved.

The public map presents these same four classes under plain-English labels for a general reader: *confirmed exposure* appears as **passes a camera**, *unobserved* as **avoids all cameras**, *possible exposure* as **might pass a camera**, and the *excluded unroutable* remainder as **couldn't determine**. These labels are presentation aliases for the formal terms used throughout the rest of this report.

The plain-English labels compress two important cautions. First, *confirmed* means that camera geometry, direction, and same-corridor alignment are all confirmed. In the robust all-hypotheses view, every plausible access route must satisfy that test. In the primary single-hypothesis view reported alongside it, only the modeled first-access route must satisfy the test. The robust confirmed share therefore cannot exceed the primary share.

Second, *possible exposure* does not require competing roads. A single modeled route is classified as *might pass a camera* when a camera sits on it but the camera's direction or same-corridor edge cannot be resolved, or when the access evidence is incomplete. Disagreement among plausible roads is an additional source of uncertainty that exists only in the robust view. A large *might pass a camera* share in the primary single-route view therefore reflects unresolved camera geometry on the modeled route, not a choice between roads.

Because a standard commute is modeled as recurring travel on the same ordinary route, a confirmed camera on every supported access scenario represents repeated exposure rather than a one-time event. For each site, the audit output gives the occupied-housing-weighted all-hypotheses confirmed share, the mean number of distinct cameras per round trip among confirmed draws, and annualized encounters at 250 commutes a year. The point estimate for the unobserved rate is reported alongside a sampling interval, an origin-access bound, direction and spatial intervals, a 25–60-degree direction-tolerance sweep, single-camera influence, and the full-denominator unresolved rate. These terms describe the route-camera model; they are not empirical traffic counts or optical-recognition probabilities.

The unit of analysis is a modeled round trip, not a person. The study measures the *opportunity* to observe traffic in a residential commuting environment; it does not track any individual, uses no Flock detection record, and makes no claim that a particular service member, employee, or vehicle passed a particular camera. Every rate in Section 5 is a property of this route-and-camera model applied to a residence-weighted sample, and should be read as the camera exposure of the road environment around a site rather than as surveillance of the people who work there.

Occupied housing is the weighting frame because no authoritative, public, installation-specific distribution of where personnel live exists, and constructing one would require exactly the personnel-location data whose sensitivity this report examines. The 2020 Census occupied-housing frame provides a reproducible, neutral proxy for the civilian residential market around each site. Section 6 documents that roughly two-thirds of service members live off base, but the study does not assume that any sampled household contains military or federal personnel. By weighting all occupied housing equally, the frame avoids deliberately concentrating the sample on presumed personnel commuting corridors. The results should therefore be read as estimates of the residential road environment, not as personnel-specific estimates or as inherently conservative estimates. Raw draw counts, represented-housing totals, and sampling intervals are retained for every site so a reviewer can assess sensitivity to this choice.

The 95% sampling interval is a Wilson score interval computed at the smaller of the design-effect-adjusted Kish effective sample size and distinct-candidate count, because draws are made with replacement and the raw draw count would overstate precision; Wilson also stays valid near 0% and 100%. It must not be confused with the origin-access bound, which asks how the result can change across plausible residential road access. The QA checks flag a record for a wide origin-access span, direction-threshold sweep, elevated unresolved rate, or single-camera influence without an exact source-hash-bound review, as well as for incomplete route/camera semantics or other contract failures; where a flag applies, the corresponding uncertainty range is reported alongside the estimate rather than hidden.

Appendix L contains the exact input rules, pseudocode, reason categories, and reproducibility checks. Appendix H records the per-site counts for every run; the artifacts are in the staging path recorded in the snapshot at L41.

5. Results of the 22 Sensitive Sites

> **About these numbers.** The results below come from cohort `reachability-v7-audit-92bd2e6a45c3a7c6`, the V7 run. They are **modeled** coverage estimates from a routing simulation over public camera locations, reported with explicit uncertainty ranges (origin-access, direction, spatial, and capture-range). They describe where cameras sit relative to the routes a resident would drive; they are not observations of any real vehicle or person being tracked.

Every site below was generated under the V7 vehicle-fingerprint route-exposure protocol described in Section 4 and Appendix L. The values are modeled route-coverage estimates, reported with uncertainty ranges, not empirical plate-read observations.

The set covers 22 sites in three classes: 15 military installations, 2 federal headquarters (CIA, FBI), and 5 defense-contractor and federal-laboratory headquarters (Lockheed Martin, Northrop Grumman, RTX, Anduril, and the Jet Propulsion Laboratory). The purpose is not a national average but a test of how one national device inventory intersects with different local road networks and sensitive missions.

Each row reports two forms of uncertainty: sampling uncertainty around the point estimate and the origin-access bound, which measures how much the classification can change across plausible residential access roads. The fixed-gate U20 bound in the last column captures the latter, the modeled result's main sensitivity.[36]

The table below gives the headline result for each site. It shows the share of modeled round trips confirmed to pass at least one camera, the share that passes none, and how far the no-camera share could move depending on the residential access road. All figures are the strict (robust) 20-mile estimates, weighted by the occupied housing represented by each sampled origin. The complete technical record for every site, both channels, both trip distances, and the full unobserved/confirmed/possible/unresolved split, is in Appendix H.

Site	Confirmed to pass a camera (20-mi)	Passes no camera (20-mi)	No-camera range if the road differs
Eglin AFB	93.9%	3.4%	3.4–6.1
Joint Expeditionary Base Little Creek	89.4%	2.1%	2.1–8.8

Site	Confirmed to pass a camera (20-mi)	Passes no camera (20-mi)	No-camera range if the road differs
Fort Lee	89.2%	0.0%	0.0–10.8
Jet Propulsion Laboratory	87.9%	1.6%	1.6–8.2
Hurlburt Field	87.0%	10.5%	10.5–13.0
Fort Cavazos (Hood)	85.7%	4.5%	4.5–13.9
Naval Amphibious Base Coronado	84.9%	0.6%	0.6–14.5
Buckley Space Force Base	81.1%	4.9%	4.9–16.5
Naval Station Norfolk	75.4%	18.5%	18.5–24.1
Joint Base Andrews	68.8%	9.1%	9.1–23.0
Naval Base San Diego	67.0%	2.2%	2.2–17.7
FBI Headquarters	65.0%	0.0%	0.0–13.4
CIA Headquarters	62.1%	0.7%	0.7–17.0
Anduril Industries Headquarters	61.7%	0.9%	0.9–12.2
Pentagon	57.2%	0.5%	0.5–20.7
Fort Benning	56.9%	12.9%	12.9–25.8
RTX Corporation Headquarters	55.9%	4.0%	4.0–16.9
MacDill AFB	54.9%	27.1%	27.1–33.0
Camp Pendleton	54.8%	4.8%	4.8–14.9
Fort George G. Meade	50.3%	34.8%	34.8–45.3
Northrop Grumman Headquarters	18.5%	17.0%	17.0–31.3
Lockheed Martin Headquarters	15.6%	11.0%	11.0–23.3

Values are occupied-housing-weighted shares over the full sampled denominator. “Confirmed” on the robust channel requires every complete supported access hypothesis to encounter a direction-confirmed camera; “possible” applies under some but not all hypotheses; and unresolved-route weight remains in the denominator. Weighted `unobserved/confirmed/possible/unresolved` percentages for both radii appear

in Appendix H. The raw per-origin counts remain in the L41 snapshot and the offline per-origin records. Among confirmed modeled round trips, the median site-level mean is **3.17 distinct cameras per trip**, equivalent to about **792 encounters a year** at 250 commutes.

Across the 22 sites, the median 20-mile robust confirmed share is **66.0%**. Eglin AFB (93.9%) is the only site above 90% confirmed on the robust channel; several additional sites exceed 90% on the single-policy primary channel.

Eleven of the 22 sites sit at or below 4% unobserved at the 20-mile scope. The largest unobserved shares are Fort George G. Meade (34.8%), MacDill AFB (27.1%), Naval Station Norfolk (18.5%), and Northrop Grumman (17.0%). A point estimate is not the whole picture. The fixed-gate access bound beside each site shows how far the 20-mile unobserved share can move depending on which entry gate a driver uses. At Meade, for example, the range extends from 34.8% to 45.3%, which is why the bound appears next to every site rather than in a footnote.

The model also reports the 75/150/250-foot capture-range curve. Across the cohort, on the primary single-policy channel, the median 20-mile unobserved rate is 8.16% at 75 feet, 4.65% at the 150-foot primary field of view, and 3.54% at 250 feet. The robust channel behind the Section 5 “passes no camera” column is slightly lower, with a 4.25% unobserved rate at 150 feet. The curve isolates capture-range sensitivity; it does not replace the separate origin-access, direction, spatial/grade, camera-influence, or sampling uncertainty measures in each summary.

Each site’s frame represents tens of thousands to more than a million 2020-Census occupied housing units; the figures are not summed across sites because the dense Washington-area frames overlap. Raw outcome counts, represented-housing totals, camera and gate counts, source-file hashes, the locked per-site random seed, access scenarios, and exact nested-sample validation for both scopes are recorded per site in Appendix H and the SHA-256-bound snapshot.[37]

6. Why Movement Data Becomes Military Intelligence

The installation results matter because much of the military and federal workforce lives and travels outside a protected perimeter. The Government Accountability Office reports that about two-thirds of U.S. service members live off base in local communities. The Congressional Research Service reports that about 58% receive

Basic Allowance for Housing and obtain housing through the civilian market.[38] Contractors, civilian employees, visitors, and many intelligence personnel also use ordinary roads.

Commercial camera placement follows traffic. Devices are installed at intersections, arterials, neighborhood entrances, retail corridors, parking facilities, and other places where many vehicles pass. Personnel assigned to sensitive missions are not separate from that traffic. Their daily movement becomes part of the same searchable record as school trips, deliveries, shopping, medical appointments, and every other ordinary journey.

That fact creates three escalating levels of intelligence value:

1. **Inventory and coverage** reveal where observation exists, which approaches are dense, where gaps remain, and where deployment is planned.
2. **Historical observations and alerts** reveal when particular vehicles appeared, where they traveled, which cameras saw them, and which vehicles moved or disappeared together.
3. **Identity and data fusion** connect vehicles and locations to people, households, accounts, devices, employers, cases, associates, and other records.

These map onto the escalation set out in Section 1.4: the first level is present in the December export and the ArcGIS evidence, the second in Search, Hotlist, FlockOS, and exposed agency FeatureLayers, and the third is the organizing purpose of Nova.

6.1 Readiness, Training, and Aviation Patterns

Hurlburt Field runs special-operations aviation and specialized intelligence, surveillance, and reconnaissance. Eglin handles test and evaluation, and Fort Cavazos (Hood) is home to III Armored Corps, heavy-force training, and mobilization. Buckley covers missile warning, space surveillance, communications, intelligence, cyber, and resident air operations. Joint Base Andrews manages National Capital Region response and senior-leader airlift.[39]

No individual commute reveals a classified mission. Repeated group behavior can. A stable set of vehicles arriving on a regular cadence creates a baseline. A sudden shift in arrival time, weekend activity, vehicle volume, or co-movement can indicate a change in readiness. Several recurring vehicles disappearing for the same period and returning together can suggest a deployment, exercise, test event, or shared duty cycle.

Longer histories improve confidence. A 30-day window can show current rhythm. One-, three-, or five-year retention can compare recurring seasonal events, rotations, exercises, personnel changes, or unusual departures against prior baselines. Nova's named convoy/caravan permission and its person, vehicle, address, device, signal, and records pivots show that multi-object correlation and identity enrichment are product concepts, not capabilities invented for this report.[40]

An intelligence service would not need to identify every employee. A probable cluster associated with one sensitive function can be enough to monitor whether that function appears active, absent, expanding, or interacting with another organization.

6.2 Fleet and Amphibious Cycles

Naval Station Norfolk hosts fleet command functions and carrier strike groups. Naval Base San Diego supports the Pacific Fleet surface force, homeported ships, tenant commands, regional headquarters, medical functions, and fleet readiness. Coronado supports amphibious and special-warfare activity.[41]

Naval operations produce patterns both at the installation and at home. Crew vehicles may disappear from normal commute routes during an underway period. Household vehicles may remain and continue school, work, shopping, or childcare routines. Maintenance, training, qualification, and deployment activity can change traffic at different times and in different combinations.

Historical movement records can therefore reveal more than whether one plate entered a city. They can distinguish a recurring installation-associated population, observe synchronized absence, and compare the timing of return. When several public and private camera networks feed one platform, the useful observation point may be far from the gate. A neighborhood entrance, commercial corridor, or highway interchange can contribute to the same pattern.

The route studies are designed to measure the modeled opportunity for those observations, not actual fleet schedules. The naval figures reported in Section 5 measure that modeled opportunity; they are not schedule observations and no operational tempo is inferred from them here.

6.3 Intelligence, Command, and Contractor Relationships

Fort Meade, CIA Headquarters, the Pentagon, FBI Headquarters, and Joint Base Andrews represent the intelligence, command, defense, law-enforcement, and airlift functions concentrated in and around the National Capital Region.[42]

Movement and association are especially valuable in that environment. Repeated co-location at a government site and a contractor facility hints at a working relationship, and recurring travel among headquarters, airports, secure facilities, and industry locations can expose liaison or acquisition activity. When the set of vehicles arriving together changes, it may mark a new team or project before anything is announced.

FlockNova's data model increases that risk because it is built around pivots. The pivots chain outward. An address surfaces people and associates, a plate surfaces vehicles and scans, and an email, registration ID, advertising identifier, IP address, or signal ties back to location records. Agency integrations add cases, CAD events, arrests, RMS entities, body-worn-camera events, and LPR observations. The security burden lies in keeping each source, tenant, field, and search purpose properly authorized and audited.

6.4 Families and Protected Persons

Families extend the observation surface beyond the duty station. A spouse or dependent may never enter a secure gate but can still connect a household to schools, medical providers, religious institutions, shopping locations, and recurring absences. A secondary vehicle can maintain the household pattern while the service member or employee is away. Those relationships can be inferred from repetition before any investigator knows a person's name.

The same architecture creates a structural risk for witnesses, victims, undercover personnel, and others whose safety depends on breaking prior identity and location links. The federal Witness Security Program publicly describes relocation and new-identity support for endangered witnesses and authorized family members.[43] A long-lived commercial plate history or identity graph can preserve links that a protection program is trying to sever. The answer cannot be a queryable "protected person" list, which would create its own target set. It requires strict purpose limitation, anomaly detection, rapid notification, controlled retention, and independent oversight.

6.5 Threat Paths Do Not Require a Spy at the Gate

The risk is not limited to an outsider who discovers the exact vulnerabilities described in this report. Several access paths can produce the same operational consequence.

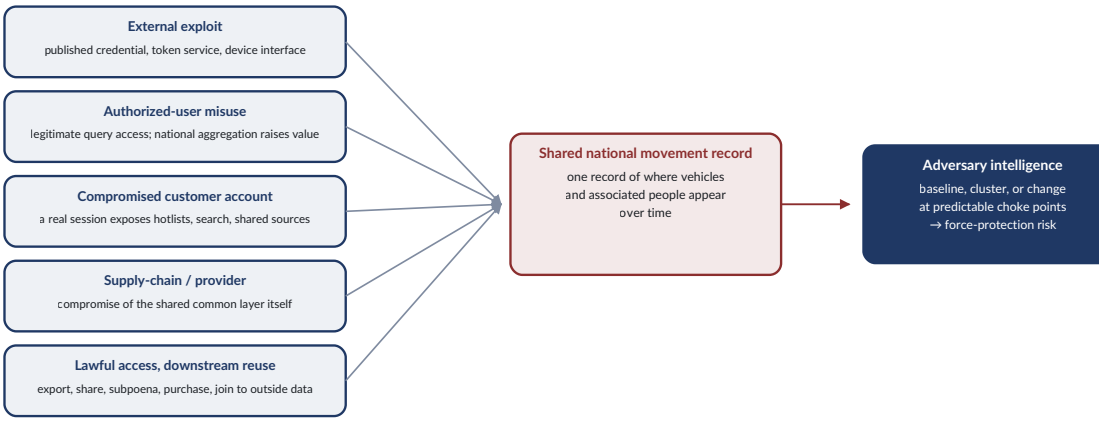


Figure 10. Five distinct access paths, from external exploit to lawful downstream reuse, converge on the same shared national movement record and the same force-protection risk.

An external actor can exploit a published credential, an unauthenticated token service, an exposed device interface, or another internet-facing defect. That is the clearest cybersecurity path, and Vulnerabilities 1 and 3 show why credential discovery and bulk-access monitoring have to work even when the actor does not announce every action.

An authorized user can misuse legitimate search access. A local officer, contractor, vendor employee, or partner-agency user may already have permission to query part of the system. Least privilege, purpose limits, case review, and immutable auditing determine whether that access remains tied to a legitimate investigation. National aggregation increases insider value because one account or sharing relationship can reach beyond the actor’s own street or jurisdiction.

A compromised customer account can turn ordinary application functions into an intelligence-collection tool. The attacker does not need to defeat every platform boundary if a real user’s session already exposes hotlists, search history, shared cameras, exports, or Nova sources. Strong authentication matters, but so do per-source authorization, session controls, anomalous-query detection, and rapid customer notification.

A supply-chain or service-provider compromise can target the common layer itself. Flock's concentration of devices, application logic, integrations, and geospatial services makes the platform more efficient for customers and more valuable to an adversary. The same applies to third-party data and application partners connected to Nova, emergency-response integrations, mobile applications, and edge devices.

Finally, lawful access can create downstream exposure. Data returned for one approved purpose can be exported, retained, shared, subpoenaed, purchased through another source, or joined to outside datasets. Policy and contract controls matter because not every national-security risk begins with a technically unauthorized query.

These paths require different safeguards, but they all draw on a common record of where vehicles and associated people appear over time. An adversary does not need perfect coverage. It needs enough observations to establish a baseline, identify a cluster, or detect a change. Repeated observations at predictable choke points can be more valuable than continuous tracking everywhere.

6.6 The Force-Protection Conclusion

Traditional installation security concentrates on the perimeter: gates, barriers, guards, access cards, and restricted areas. Commercial surveillance moves the observation point outward. The relevant question becomes whether off-base travel can be collected, searched, retained, fused, and accessed by people who should not have that authority.

The vulnerabilities in this report make that a cybersecurity question. Credential scope, development isolation, backend authorization, bulk-access logging, device security, and incident reporting can determine whether ordinary public-road observations become adversary intelligence. A secure gate does not protect a recurring movement pattern already assembled outside it.

7. Privacy, the Fourth Amendment, and Corporate Accountability

The national-security problem and the civil-liberties problem arise from the same architecture. A plate observation on a public road may appear modest when viewed alone. A national, searchable history of observations linked to addresses, people, devices, cases, and relationships is different in kind.

The Supreme Court's decision in *Carpenter v. United States* concerned historical cell-site location information, not Flock's specific system. What makes it relevant here is aggregation. Repeated records can reveal a detailed chronicle of a person's movements even when each underlying observation involves travel outside the home.[44] Commercial automated license-plate reader (ALPR) networks raise the same unresolved question of when scattered public observation becomes persistent location surveillance.

Flock's public messaging often draws narrow product boundaries. A fixed LPR camera may be described as collecting vehicle data rather than personal information, and Flock says it does not offer facial recognition. Those statements do not resolve the system-level privacy issue. A license plate is routinely linkable to a registered owner or household. Natural-language visual search can locate a person or vehicle using appearance rather than a plate. Flock's patent describes face-related feature and similarity matching that can support re-identification even if a production feature does not return a legal name from a face.[45]

Private placement further complicates accountability. Police cameras, neighborhood cameras, business cameras, and third-party IP cameras connected through gateways can participate in one search plane. A person may pass through several nominally separate property and government contexts while generating observations available through a common vendor. Ordinary notice at one location says little about how the combined network will be searched later.

Legitimate investigations do not eliminate this concern. They increase the need for enforceable purpose limits, strong backend authorization, search justification, immutable audit logs, retention controls, misuse detection, and public rules for cross-agency sharing. The same platform that helps find a dangerous suspect can expose a protester, a victim, a protected witness, a service member, or an intelligence employee when controls fail or permissible uses expand.

This is also a corporate-governance issue. Flock's growth depends on adding devices, customers, integrations, data sources, and retention. Every expansion increases the value of the system and the damage a common control failure can cause. Security cannot be treated as a cost center that follows deployment. A company's quarterly performance cannot take priority over the national security of the United States or the constitutional interests of the people whose movements make the product valuable.

Public agencies and private customers therefore share responsibility. Procurement decisions create the network. Contracts determine retention, audit access, incident notice, sharing, and independent testing. Policymakers decide whether a national movement database can emerge through thousands of local purchases without national-level security and privacy review.

8. Counterarguments and Limits

The strongest objections change how individual facts should be described. They do not dissolve the combined record.

Objection or limitation	Evidence-based answer
Public JavaScript does not prove every backend endpoint was open.	Correct. Vulnerabilities 2 and 4 establish exposed application logic, schemas, permissions, and client controls. Vulnerability 1's validation, Vulnerability 3's wire responses, and the December export separately establish production authority and data access.
ArcGIS may not contain Flock's master historical detection database.	It does not need to. The validated key held 50 private grants and 13 premium capabilities, and the connected evidence shows deployment, layer, search-result, detection, registry, and device-health classes. Separate Flock APIs and stores can remain distinct while the geospatial exposure stays material.
The content of every private grant was not resolved.	Correct. The report identifies grant scope as direct evidence and uses separate code, export, and FeatureLayer evidence for the represented data classes. It does not assign every runtime object to every grant.
The production FeatureServer's Create/Update/Delete flags do not prove anonymous write access.	Correct. They establish an integrity-relevant capability configuration. I did not test writes. The required defensive action is to verify that anonymous and under-scoped credentials cannot edit the layer.

Objection or limitation	Evidence-based answer
Planned devices may never become operational.	The source labels remain unchanged in the artifacts, and planned records are counted as operational in the headline on a stated, dated assumption: the snapshot is December 2025 and the studies ran in August 2026. The assumption inflates coverage if a planned site was cancelled or relocated, and the conservative `inService`-only floor is reproducible from the same artifacts.
The route model is not a commuter census or optical-capture test.	Correct. It is a residence-weighted route-exposure model. Outputs depend on the declared gates, frozen OpenStreetMap topology, Census occupied-housing frame, retained device snapshot, bounded residential-access hypotheses, route model, and directed same-corridor camera rules.
Occupied housing is not the same as the installation workforce.	Correct. Occupied housing supplies a reproducible residential weighting frame where no complete installation-specific workforce-residence distribution is available. Raw counts, represented housing, and sampling intervals remain visible so reviewers can assess that choice.
Five and 20 miles describe different residential strata.	Correct. The 5-mile draws are retained unchanged in the 20-mile artifact, which adds the outer stratum. The 20-mile result weights both strata by represented occupied housing; the two headline rates are reported separately and never averaged.
The Section 5 percentages are modeled, not empirical.	Correct, and stated plainly. They are a routing simulation over public camera locations that shows where cameras sit relative to the routes a resident would drive. They are not observations of any real vehicle. Every site is reported with its access and direction uncertainty ranges so the modeled estimate is never mistaken for a plate-read measurement.
Flock has legitimate public-safety uses.	That strengthens the need for least privilege, isolation, logging, and oversight. The more consequential the authorized use, the higher the required security assurance.
Flock publicly describes an approximately 30-day default retention period.	The report uses that default where applicable and separately documents priced one-, three-, and five-year extensions. Short-window pattern analysis remains possible under the default.

Objection or limitation	Evidence-based answer
Responsible research is not necessarily a legally defined breach.	The paper does not need that legal conclusion. The December retrieval tests whether Flock could account for production credential use and bulk access without a separate notice from the actor.
No evidence proves that Flock intentionally targeted military personnel.	Intentional targeting is not the thesis. Cameras placed on high-traffic corridors record vehicles used by military personnel and employees of sensitive facilities as part of ordinary traffic.

The export is a December 14, 2025 snapshot. Device locations and statuses may have changed. Public mission descriptions establish why the selected sites are sensitive; they do not reveal classified activity or individual assignments. Intelligence scenarios describe plausible value from documented capabilities and movement patterns, not completed hostile operations.

9. What Must Change

The immediate fixes follow directly from the four vulnerabilities. The broader response has to address the system that allowed them to amplify one another.

Priority	Required controls	Evidence customers should receive
Production credential governance	Eliminate default organization-wide keys from public clients; use per-application and per-environment credentials; remove unnecessary private grants and premium capabilities; rotate exposed keys; scan every build and preview deployment for secrets.	Current item-grant inventories, rotation records, negative public-asset scans, and anomalous-use alerts.
Token issuance and environment isolation	Require authentication and tenant authorization before minting; prevent development services from issuing production credentials; use short lifetimes and narrow audiences; record principal, tenant, environment, scope, IP, and volume for every mint.	Negative anonymous tests, dev-to-prod isolation tests, and complete issuance logs.

Priority	Required controls	Evidence customers should receive
Application and backend authorization	Protect sensitive bundles and module manifests where exposure itself is harmful; enforce every search, source, field, organization, pivot, and export on the server; normalize claim names; treat case and reason fields as audit metadata rather than authorization.	Authorization matrices, denied-source tests, tenant-isolation tests, and immutable search/export logs.
Bulk-access detection and incident accounting	Alert on inventory-scale queries, unusual item enumeration, high-volume export, and repeated credential minting; retain logs long enough to reconstruct an event; notify affected customers under a clear contractual standard.	A documented answer to who accessed what, when, through which credential, and what alert or review followed.
Geospatial integrity	Remove anonymous or broad edit rights; separate read and edit credentials; audit changes to camera position, status, ownership, planning, and attachments; monitor destructive and mass-update behavior.	FeatureServer authorization tests and tamper-evident change history.
Device, video, mobile, and federal tiers	Require TLS and authentication for camera administration and streams; patch edge devices; remove internal credentials and backends from mobile clients; minimize session replay; isolate government and GovCloud environments from public development infrastructure.	Independent edge/mobile testing, patch evidence, network-isolation tests, and government-tier architecture review.

Military and federal customers should make these controls procurement requirements rather than accepting a general security statement. Contracts should guarantee access to relevant audit records, prompt notice of credential or bulk-data events, retention transparency, and independent testing scoped to development, preview, production, GIS, mobile, and device surfaces.

Installation security teams should receive the complete camera and route records for their own sites and verify the modeled 24/7 gates. They should assess whether recurring traffic associated with special operations, intelligence, test, fleet, command, or contractor functions can be inferred from commercial observation outside the perimeter. Where the answer is yes, OPSEC planning has to account for the civilian-road collection environment.

Agencies should enforce purpose-limited searches, case and reason review, least-privilege sharing, periodic audit inspection, bulk-search anomaly detection, and defensible deletion. Oversight should cover not only plate searches but FreeForm visual search, hotlists, identity and signal pivots, CAD/RMS/BWC integrations, third-party datasets, cross-agency queries, and exports.

Policymakers face a question the market cannot answer on its own. A national record of where Americans drive did not emerge from a single program debated by Congress. It accumulated through thousands of separate municipal, community, and commercial purchases. Each purchase may be defensible in isolation, but no review asks what those purchases create in aggregate.

No authority currently tests whether a private surveillance network of this scale meets a national-security or civil-liberties standard, because no law requires such a review. Congress and the relevant oversight bodies should decide, deliberately and publicly, whether a company holding movement data on service members, cleared personnel, and their families must meet security, retention, audit, and independent-testing obligations commensurate with that responsibility. Those obligations should reflect the company’s national role, not merely the terms a local procurement officer can negotiate in a single contract.

Finally, Flock should answer the December event directly. The required response is not another categorical assurance. It is an auditable account of whether the credential use was detected, which records show it, how the issue was remediated, whether any other use was found, and what customers were told.

10. Conclusion

On December 14, 2025, I used an unauthenticated production credential path, which I had reported a month earlier, to retrieve 335,701 device and deployment records from Flock Safety's cloud. I did not announce the retrieval. In the months that followed, Flock told the public three times that it had never been hacked, compromised, or breached.

Both possible explanations for that gap are damning. Either Flock detected a national-scale export of production data and excluded it from its public assurances, or it never detected the export at all. The company has not said whether this was a failure of transparency or a failure of detection. Either answer undermines the confidence those assurances asked the public to place in Flock.

The access event was not an isolated lapse. It was the visible result of a systemic failure. A production geospatial key appeared in 53 public files. Two application blueprints and a credential-minting service were accessible before login. The inventory exposed by those failures was not merely a collection of records. The V7 model found repeated modeled exposure around 22 military, federal, and defense-contractor sites, with a median 20-mile confirmed estimate of 66.0%. That estimate is reported alongside the access uncertainty for each site. The network has intelligence value, but the model must not claim greater precision than the evidence supports.

Flock's network can serve legitimate investigations. But failures in credential security, authorization, data retention, or auditing can expose the movements of service members, government personnel, and others whose safety is a national-security concern. This report documents that those controls have failed. A company may pursue growth, but its quarterly performance cannot take priority over the security of the nation whose roads, agencies, and people make that growth possible.

Flock has answered all of this by repeatedly asserting that it has never been hacked. The preserved evidence supports a narrower and far more troubling statement. Flock cannot show that it has not been. A surveillance vendor that cannot account for the use of its own production credentials has not earned the public's trust. The country whose service members, agency personnel, and families travel through this camera network is under no obligation to accept its assurances.

Technical Appendices

Appendix A. Evidence, Provenance, and Research Conduct

A.1 Source hierarchy

Artifact-specific claims in this report are controlled by the codebase and preserved evidence package. Public sources establish vendor statements, product positioning, disclosure norms, public mission context, housing policy, legal background, and independent corroboration. They do not override a conflicting captured response, bundle, validation record, or export.

The source prefixes are:

Prefix	Source class
L	Local repository evidence, generated study artifacts, source analyses, validation records, and package documentation
P	My previously published research
E	External public sources, including vendor material, government records, standards, court opinions, journalism, and third-party research

The canonical catalogs are Research_Paper_Citations.md and the evidence annex. The sources this report cites are appended to the primary PDF; the complete package-wide catalog is Research_Paper_Citations.md.

A.2 Research provenance

This is my research record. I discovered and reported the four vulnerabilities, collected the preserved application and network artifacts, validated the ArcGIS key scope, obtained the December export through Vulnerability 3, designed the reachability question, reviewed the study setup, and interpreted the resulting security and policy significance.

System and artifact facts remain distinct from my judgments. The evidence types answer different questions. A captured HTTP response records what the endpoint returned. A bundle captures the client's own model of the data, and a scope artifact fixes

the grants in place at validation time. The export is a snapshot of the records on its date, and a route summary is only what the declared model computed. The interpretation sections then explain what those facts mean for force protection, privacy, and accountability.

A.3 Disclosure chronology and collection

I reported the four vulnerabilities between June and December 2025. Flock said it ameliorated Vulnerability 1 on July 1, 2025. Flock provided no closure details for Vulnerabilities 2 or 3 and no reply or remediation details for Vulnerability 4 [L2].

I obtained the December 14 export after reporting Vulnerability 3 and sending two follow-ups. The acquisition used the same pre-login Planner/Beefeater path documented in the disclosure and wire evidence. For Vulnerability 1, I validated the 50 grants but did not open any private item or retrieve private police-department records behind them. Instead, I used public ArcGIS portals and applications published by municipalities, police departments, and Flock, then cross-checked those examples against FlockOS code and the production export. That ethical collection boundary preserved the evidence needed to assess likely scope without acquiring the unresolved private-item contents [L10, L20-L25, P1].

A.4 Complete unredacted record

The counsel and technical-review record is unredacted. The V7 artifacts retain:

- exact synthetic origin labels and coordinates;
- reviewed gate identifiers and coordinates;
- blocks;
- every bounded origin-access hypothesis and its independently routed outbound and return geometry;
- every gate attempt;
- blocked-camera names, coordinates, distances, and reasons;
- complete per-origin scenario outcomes, uncertainty evidence, and full four-class outcomes; and
- report, summary JSON, GeoJSON, and CSV representations.

The master paper does not reproduce millions of route coordinates or every camera row because doing so would make the document unusable. Appendix H identifies the staging record for each run. These are modeled estimates, not empirical plate-read observations. That distinction describes the evidence; it is not a redaction category.

A.5 Claim control and authorship

Appendix M is the claim-confidence matrix. Each material claim is listed with its principal support, a confidence classification, and an interpretation.

First-person statements identify my actions and judgments. Third-person statements describe files, systems, responses, data, and model output. No AI detector is used as an authorship or release gate. I remain responsible for checking and accepting the final text.

Appendix B. Vulnerability Timeline and Vulnerability Cards

B.1 Timeline

Figure 11. The disclosure chronology: three vulnerability reports and the December production export preceded three public "never hacked" denials.

Date	Event
2025-06-11	Vulnerability 1 reported: public Flock Safety development endpoint exposed a hardcoded production ArcGIS Default API key
2025-07-01	Flock reported Vulnerability 1 ameliorated
2025-11-13	Vulnerabilities 2 and 3 reported
2025-11-14	Follow-up sent for Vulnerabilities 2 and 3

Date	Event
2025-11-19	Second follow-up sent for Vulnerabilities 2 and 3
2025-12-05	Vulnerability 4 reported
2025-12-14	Production device/deployment export obtained through Vulnerability 3
2026-01-06	Flock security-posture page published
2026-03-27	Flock CISO cybersecurity post reiterated the no-breach position [E97]
2026-06-10	Flock security page again stated the cloud platform has not been hacked [E99]
2026-08-07	Canonical paired installation studies completed

B.2 Vulnerability 1 card

Field	Value
Title	Hardcoded ArcGIS Default API key
Approximate CWE	CWE-798 / overbroad geospatial credential
Severity	Critical
Preconditions	Public asset fetch; key present and valid; private grants or premium capabilities assigned
Direct evidence	53 published instances; 23 repository occurrences; 50 private grants; 13 premium capabilities; active Location Platform context and approximately 995,002.8 available organization credits
Remediation record	Reported ameliorated July 1, 2025
Residual risk	Rotation does not repair Vulnerability 3, public bundle delivery, or future re-embedding

The validated application was titled `Default API Key`, with app ID `qNvllGlOMKItMs4k`, organization ID `1KuIkn1ysFhZtjPD`, item ID `030ff0e7721d43c9ab719e3df947ce5f`, and owner `FlockSafety` [L8]. The credential carried 63 recorded privileges: 50 item grants and 13 premium capabilities.

Retest standard: no live production key in public or preview assets; public map keys have no private grants and only justified capabilities; old credentials fail after rotation; CI blocks production key patterns; ArcGIS monitoring detects anomalous item and routing activity.

Standalone card: Finding_01_Hardcoded_ArcGIS_Default_API_Key.md.

B.3 Vulnerability 2 card

Field	Value
Title	FlockSafety wrong-layer bundle exposure
Approximate CWE	Broken access control / missing authentication on static asset delivery
Severity	High
Preconditions	SPA or federated bundle reachable; asset path unauthenticated; bundle contains sensitive product logic
Direct evidence	Pre-auth bundle corpus; Search, Hotlist, FlockOS, device, map, and Flock911 schemas
Remediation record	Internally triaged; no closure detail returned
Residual risk	Route-only login, public source maps, production-shaped previews, telemetry and configuration leakage

The vulnerability establishes application-logic exposure. Server-side data access requires separate evidence, supplied elsewhere by the key validation, token responses, and export.

Retest standard: sensitive bundles, manifests, source maps, and environment files require authorization or are stripped of sensitive content; PR previews are private and expire; anonymous probes receive 401/403 or a non-sensitive stub.

Standalone card: Finding_02_FlockSafety_Wrong_Layer_Bundles.md.

B.4 Vulnerability 3 card

Field	Value
Title	Planner/Beefeater unauthenticated token minting
Approximate CWE	Missing authentication / broken credential-issuance boundary
Severity	Critical
Preconditions	Beefeater endpoint reachable; anonymous request accepted; usable token returned

Field	Value
Direct evidence	HTTP 200 ArcGIS and Google token responses without cookie or Authorization header; development-to-production scope collapse; December export
Remediation record	Internally triaged; no closure detail returned
Residual risk	Static rotation is insufficient; the accounting gap persists until Flock states whether the credential use was detected

This was a credential factory. The development service also issued production-scope ArcGIS authority, collapsing environment separation.

Retest standard: anonymous requests fail; every mint requires an authenticated and authorized principal; development cannot mint production scope; credentials have narrow audience and lifetime; every attempt records principal, tenant, environment, scope, IP, and outcome.

Standalone card: Finding_03_Planner_Beefeater_Token_Minting.md.

B.5 Vulnerability 4 card

Field	Value
Title	FlockNova wrong-layer bundle exposure
Approximate CWE	Broken access control / client-side authorization exposure
Severity	High
Preconditions	Shared Nova build reachable before authentication; bundles encode source, claim, request, and pivot logic
Direct evidence	148-file client corpus; freeform and advanced taxonomy; signals, dark documents, organization integrations, result graph, and shared-host logic
Remediation record	No reply or closure detail returned
Residual risk	UI-only gates, claim-name drift, token handling, and shared demo/stage/production architecture

Retest standard: sensitive application assets are protected or stripped; backend tests deny every source, field, tenant, export, and pivot without the required entitlement; claim names are normalized; searches and pivots are logged with subject and organization.

Standalone card: Finding_04_FlockNova_Wrong_Layer_Bundles.md.

Appendix C. ArcGIS Key Scope and Geospatial Damage Model

C.1 Direct credential scope

Scope class	Validated value
Private `portal:app:access:item:` grants	50
Unique premium user capabilities	13
Total recorded granted privileges	63
Available Location Platform credits at validation	approximately 995,002.8

The premium capability set included basemap access, geocoding, stored geocoding, temporary geocoding, geoenrichment, network analysis, closest facility, location allocation, optimized routing, origin-destination cost matrix, routing, service area, and vehicle routing [L8].

C.2 Damage questions

Question	Evidence-grounded answer
What could a holder learn directly?	Private item inventory and metadata within the granted scope, map and layer structure, and the capability set assigned to the key.
What could granted layers expose?	Item-specific camera/device, registry, deployment, detection, search-result, boundary, and status fields where the underlying item allowed query.
What could premium services calculate?	Routes, service areas, closest facilities, optimized routes, origin-destination costs, location allocation, geocoding, and enrichment over authorized or supplied inputs.

Question	Evidence-grounded answer
What could be inferred operationally?	Coverage density, planned corridors, service geography, potential detours, and relationships among cameras, alerts, roads, and sensitive locations.
What required separate Flock authorization?	API- or websocket-fed alerts, hotlist changes, historical detection stores, media, Flock911 audio/transcripts, and tenant administration not published through a granted ArcGIS item.
What remained unresolved?	The exact content of every private item and the post-remediation live scope.

C.3 Demonstrated map-plane data classes

Family	Specific represented information	Evidence status
Surveillance infrastructure	Device and camera coordinates, types, names, status, capabilities, organizations, networks, parent/child relationships, Wing gateways, Raven sensors, trailers, and drones	Direct export and application evidence [L10, L13-L15, L35]
Law-enforcement location	Mobile-unit categories, patrol/AVL concepts, officer mobile-app objects, CAD geography, body-camera references, trailers, and auxiliary trackers	Application evidence with selected ArcGIS field corroboration [L10, L13, L25]
People, vehicle, and audio	optical character recognition (OCR) and plate fields, vehicle attributes, people and visual alerts, confidence/time filters, Raven classifications, source, device, and location	Search/Hotlist/FlockOS code and FeatureLayers [L11-L13, L21, L23]
Investigative geography	Selected cameras, groups, map-drawn polygons, radii, saved searches, hotlist fields, reasons, cases, schedules, and hit history	Application evidence [L11-L13]
Registry PII	Registrant name, email, phone, address, location type, interior/exterior camera count, and associated locations	Published camera-registry FeatureLayer [L22]

Family	Specific represented information	Evidence status
Asset health	Serial number, uptime, support state, operational/planning status, direction, capabilities, and geometry	Export and FeatureLayer evidence [L14-L15, L24-L25]
Flock911 context	Incident and call IDs, map locations, audio and transcript token classes, per-word timing, event state, playback time, scrub position, duration, and classification	FlockOS/Hotlist application evidence [L12-L13]
Drone telemetry	Drone/video records, livestream capability, organization/network context, and docked, buffering, recording, inactive, offline, charging, and uploading states	FlockOS application and permission evidence [L13, L35, P1]

C.4 Shared-layer inference

The direct key fact is the grant set. I did not query any of the 50 private items. The broader map-plane assessment instead combines that scope with the common FlockOS integration, production export, application schemas, municipality/police/Flock ArcGIS applications found through OSINT, and a participating police department's confirmation that it shared ArcGIS layers with Flock. This supports a high-confidence inference that the key likely exposed private ArcGIS-backed data used by the common FlockOS plane across the reported customer context.

That statement should not be expanded into "every FlockOS record was in ArcGIS." FlockOS mixed ArcGIS layers, client graphics, browser storage, Flock APIs, and websocket streams. The key reached what was granted to the ArcGIS substrate; separate boundaries governed other services.

C.5 FeatureServer integrity

The `flock_safety_production` FeatureServer metadata advertised Create, Update, Delete, query, and attachment operations [L29]. Anonymous query was separately permitted. I did not attempt a mutation. Required validation includes:

1. anonymous create/update/delete requests fail;
2. public or display credentials cannot edit;
3. editing is limited by tenant, layer, field, and operation;

4. high-volume and destructive changes alert;
5. changes to coordinates, status, ownership, planning, and attachments are attributable and tamper-evident.

The integrity risk is operational. A surveillance coverage map can be corrupted as well as stolen. Moving or deleting devices creates false gaps, and adding or relabeling records creates false coverage. Altered attachments can also corrupt the evidence behind a record.

Appendix D. FlockSafety and FlockOS Technical Inventory

D.1 One Vendor and One Operational Stack

As Section 1 establishes, Flock Safety places its collection hardware, FlockOS, Flock911, FreeForm, and FlockNova in one product catalog, and the four vulnerabilities exposed credentials and application logic inside different layers of that single Flock-operated stack rather than four unrelated vendors [E23]. This appendix inventories that stack; the per-module detail follows in D.2-D.7.

Flock currently markets FlockOS as providing **24/7 situational awareness** by connecting video, LPR, sensors, CAD, RMS, drones, 911, gunshot detection, FreeForm, cross-agency sharing, and geospatial mapping [E6]. The preserved clients show the same architecture in greater technical detail:

Collection hardware. Falcon, Sparrow, Highway, Flex, Condor, Wing, trailers, and mobile-device classes support fixed and mobile plate or vehicle collection, video-capable observation, third-party-camera ingestion, livestream and device-state functions, and deployment metadata [L13-L15, L35]. Raven adds gunshot and audio-event classification, source and location context, alert delivery, and map placement [L12-L13].

Search and alerts. Search / Monaco models full, partial, unknown, and absent-plate searches alongside vehicle attributes, cameras, geography, time, case, reason, export, and people-search workflows [L11]. Hotlist / Strawberry-Soju adds watchlists, future alerts, hit and image history, people and vehicle-description policies, camera groups, schedules, confidence thresholds, regions of interest, and notification audiences [L12].

AI visual search. FreeForm provides natural-language search across enabled video and LPR sources for people, vehicles, clothing, accessories, color, type, damage, and other visible characteristics, with alert handoff [E7, L11-L13].

Operational map and emergency response. FlockOS is the common map for devices, detections, CAD/AVL, patrol context, people and vehicle alerts, Raven events, drones, body-camera references, Flock911, custom ArcGIS layers, and real-time streams [L13, E6, E80]. Flock911 / Prepared911 adds live emergency-call context, incident location, audio and transcript token classes, per-word timing, playback state, event selection, and map integration [L12-L13].

Administration, sharing, mobile, and edge. Camera-registry and device-administration surfaces hold registrant and asset records, operational health, camera controls, interagency access, HTTP Live Streaming (HLS)/video functions, mobile workflows, and field-device control paths [L5, L10, L13, L30-L33].

Identity and data fusion. FlockNova adds federated identity, account, signal, location, LPR, public-record, agency-record, breach-oriented, and relationship-pivot search [L4, L27-L28, L35-L38].

The analytical capability extends beyond reading a plate. Flock's patent describes neural networks that classify people by male/female and race classes, clothing type, height, and weight, and classify vehicles by make/model, color, and plate information. It stores those outputs with time and location for historical analysis, search, and alerting [E37]. The preserved Search, Hotlist, and FlockOS clients add operational vehicle fields such as body type, plate visibility, back and top racks, bumper and window stickers, toolboxes, OCR, confidence, and camera position [L11-L13]. Current FreeForm material describes natural-language searches such as a person in specified clothing or a vehicle with visible damage across enabled video and LPR systems [E7].

The resulting system is an always-available surveillance and search environment with multiple collection modalities. Individual device types differ. An LPR, an AI video camera, a Raven audio sensor, a drone, and a third-party feed do not collect identical data. Their outputs become materially more sensitive because FlockOS, Search, Hotlist, FreeForm, and Nova can place them in shared operational and investigative workflows.

D.2 Host and bundle footprint

The canonical October 2025 snapshot contains 370 scoped `flocksafety.com` hosts. The wider local corpus contains 387 names, the strict development/preview/staging subset contains 213, and 80 hostnames appear inside downloaded bundle artifacts [L5]. The

scoped families include customer applications, development and staging, PR previews, backend codenames, government tiers, identity, observability, support, device administration, camera management, and streaming.

The preserved bundle groups include Search/Monaco, Hotlist/Strawberry-Soju, the dev-app FlockOS shell, device and camera-management modules, sharing, planning, and multiple preview builds. Their exposure revealed application composition as well as individual screens.

D.3 Search / Monaco

Capability	Client-visible model
Plate search	Full, partial, unknown, and no-plate modes; state and plate type
Vehicle search	Make, type, color, racks, stickers, toolbox and other appearance attributes; vehicle-fingerprint controls
FreeForm	English-language visual descriptions for people and vehicles; alert handoff paths
Geography	Drawn polygons, selected cameras, camera groups, organization extent, statewide/nationwide concepts, Business Network inclusion
Time and summaries	Date windows, histogramming, per-camera hit counts, raw counts, and export/download concepts
Compliance metadata	Search reason, case number, offense type, request identifiers, user and organization context
People-search eligibility	Wing/Condor-class hardware and capability gating
Contacts and scope	Agency contacts, network and organization identifiers, user-type and policy concepts

The request and result classes include OCR and plate fields, vehicle attributes, object identifiers, capture times, camera and network IDs, case/reason/offense fields, polygons, date windows, count summaries, camera geometry, capability metadata, and agency contact information [L11].

D.4 Hotlist / Strawberry-Soju

Hotlist models watchlist creation and administration, plate add/remove and bulk operations, expiry, reason, case and note fields, hit and image history, owner enrichment, and interagency notification. Its alert surface adds vehicle-description and people-detection filters, camera groups, schedules, distance and confidence thresholds, region-of-interest drawing, custom layers, GoLive/VMS concepts, CAD and Prepared911 integration, drone-dispatch flags, and talkdown/audience configuration [L12].

Its sensitive data classes include the reason a vehicle or person is watched, case labels, notes, hit history, images, owner details, camera/network IDs, alert schedules, geofences, emergency context, stream references, and organization-specific feature flags.

D.5 FlockOS map and event plane

Surface	Data and behavior represented in the client
Notification families	Audio, CAD, target, custom hotlist, vehicle-description, people-detection, Prepared911, FreeForm, third-party, and generic alerts
User categories	Vehicle, audio, people, 911, CAD, and other event filters
Vehicle enrichment	OCR, plate state/type, make, color, body type, accessories, vehicle vectors, plate crops, and visibility confidence
Device model	Falcon, Sparrow, Wing, Highway, Flex, Condor, Raven, Ubicquia, Avicore, parent/gateway, trailer, livestream, and LPR capability classes
CAD and dispatch	Coordinate and address incident context, response geography, source, classification, and timing
Subjects and assets	Vehicle, body camera, drone, batch, notification, FirstTwo, public-safety answering point (PSAP), Flock mobile app, and other subject-message types
Realtime transport	Websocket handlers for CAD, subject batches, hits, audio, realtime alerts, FirstTwo packets, Prepared911, and generic alerts

Surface	Data and behavior represented in the client
Browser storage	NotificationDB, EventMessageDB, Prepared911DB, derived OCR/hotlist/camera/address fields, unseen state, and expiry workers
Integrations	Axon, Fusus, Azure AD, Cradlepoint, Okta, Esri, FirstTwo, DroneSense, Aerodome, support, and telemetry hooks
Shell composition	Federated Search/Monaco, Hotlist/Strawberry-Soju, and other Flock modules

Map popups can draw from OCR, vehicle attributes, source, hotlist, camera and device labels, address, audio classification, reason, topic, case, policy, and saved-search information. The client combines ArcGIS layers, client graphics, websocket events, Flock API responses, and browser-persisted objects [L13].

D.6 Flock911 / Prepared911

Flock911 events are first-class objects in the same map as vehicle, people, audio, CAD, and hotlist events. The preserved code models:

- incident and call IDs;
- open, closed, selected, and playing state;
- event, incident, call-end, and update times;
- live-audio state;
- incident audio and transcript token retrieval;
- transcript entries with per-word `started_at` and `ended_at` timing;
- current playback time, scrub position, duration, pause, resume, and completion;
- address and classification context; and
- browser persistence and timed expiration in `Prepared911DB`.

Flock911 audio and transcript calls used separate service credentials. Their presence in the common map establishes operational convergence, not that the ArcGIS Default key independently authorized the media endpoints.

D.7 Client controls and security dependence

The FlockSafety clients expose authenticated session state, organization context, feature flags, user types, capability booleans, allowlists, websocket audiences, map-token refresh, request identifiers, case and reason fields, and policy constants. These controls mix three different functions:

1. presentation, such as hiding a tab;
2. compliance metadata, such as case number or search reason; and
3. entitlement, which must ultimately be enforced by the backend.

Wrong-layer delivery exposed the vocabulary and assumptions at all three levels. Separate testing is required to determine whether each server endpoint enforced the same tenant, source, field, and action boundaries.

Primary evidence paths: FlockSafety_Dev_Subdomain_Bundle_Enumeration.md, ArcGIS_Search_App_Data.md, ArcGIS_Hotlist_App_Data.md, and ArcGIS_Mapped_Attributes.md [L5, L11-L13].

Appendix E. FlockNova Technical Inventory

E.1 Why Nova Changes the Consequence

FlockNova is not a separate company's product sitting outside the surveillance network. Flock Safety markets it as the data-context layer paired with FlockOS, under the phrase **"Search Once. See Everything."** [E23]. The preserved source explains how this works. One starting identifier can be classified, sent to multiple configured sources, normalized into common result buckets, and expanded through a relationship graph [L4].

Name, address, phone, or email. Nova can fan these identifiers into person, address, public-record, account, and organization sources, producing relatives, associates, linked addresses, phones, emails, online accounts, vehicles, and agency records.

Plate, VIN, or vehicle. Vehicle, LPR, scan, RMS-vehicle, and integrated search paths can expand an observation into linked vehicles and people, addresses, cases, incidents, and organization records.

Email, hashed email, registration ID, advertising ID / mobile advertising ID (MAID), or IP address. Device and signal workflows include email-to-location, registration-ID and advertising-ID location queries, IP-to-signal, and geographic signal search. The result model holds timestamped device points, locations, registration identifiers, IPs, and movement-oriented signal records.

Social Security number, payment-card-like value, crypto address, username, IP, email, phone, or keyword. Dark-data search forms, `darkDocs` storage, and breach/leak components model records containing crawl date, network, leak name, leak host, download location, accounts, and linked identifiers.

RMS, CAD, arrest, BWC, jail, or other agency record. Organization-integrated modules and the common result store add cases, calls, arrests, body-camera events, inmates, warrants, property, guns, vehicles, people, attachments, and LPR observations.

What matters is the expansion ratio. A road camera may begin with one plate, vehicle description, time, and location. Nova's data model can turn that starting point into many people, addresses, devices, accounts, scans, cases, and associations when the configured sources return matches. The local client also contains a bulk-signal loader with a 500,000-row browser limit and summary fields for location points, registration IDs, IPs, and time range [L4].

The breach-data evidence is equally direct at the application layer. The preserved client accepts Social Security numbers, payment-card-number-like inputs, crypto addresses, Discord and Telegram identifiers, usernames, IP addresses, emails, phones, and keywords for dark-data searches. It renders `darkDocs` and a leak table with crawl date, network, leak name, leak host, and download-location fields [L27, L36]. Appendix E.7 sets that client capability against Flock's published statement that Nova would not supply dark-web data.

This is why the shared operator matters. The same company that runs the collection and operational-map layers also runs the product designed to turn a detection into identity, location, account, and association context. A weakness in a camera inventory, map credential, token service, application boundary, customer account, or tenant-control layer becomes more consequential when the surrounding platform is built to convert one observation into a much larger intelligence graph.

E.2 Session, organization, and access model

The preserved Nova source contains 148 JavaScript files. The client establishes and refreshes sessions, decodes claims, selects organizations, checks organization feature flags, requests case information, controls tab visibility, validates forms, calls source-specific endpoints, and stores returned records in a common result model [L4].

Visible controls include:

Control	Function
Decoded claims	Identify source or capability entitlements used by the client
Organization flags	Determine whether integrated RMS, CAD, BWC, LPR, or other modules appear
Case number	Usage and audit context for selected workflows
Search reason	Policy/audit metadata sent with selected searches
Tab visibility	Presentation control
Form validation	Input completeness control
Backend authorization	Required final control for tenant, source, field, record, pivot, and export access

The freeform path visibly skips selected calls when required claims are absent. Advanced and organization-integrated modules more often proceed once a visible form validates, leaving the backend responsible for the decisive authorization.

E.3 Freeform classification and source fanout

Nova freeform is an identifier classifier, not Flock FreeForm visual search. It recognizes or models:

- name, email, phone, address, Social Security number, plate, and VIN;
- IP address, username, business, and keyword;
- cryptocurrency and payment-card-like inputs; and
- source-specific variations for person, account, signal, dark-document, LPR, and organization data.

The classifier can fan a single input out to configured person, address, online-account, dark-data, vehicle, LPR, signal, and public-record sources. Claim checks can skip unavailable sources. Returned objects are normalized into shared result buckets for follow-on pivots.

Address and person models include relatives, associates, linked addresses, vehicles, phones, emails, accounts, and other relationship fields. Flock marketing separately states that Nova can return an associate's home address from recent food-delivery data [L28]. That vendor claim illustrates the identity-broker depth the client graph is designed to use.

E.4 Advanced search domains

Domain	Inputs or result concepts present in the client
Person and identity	Names, dates, addresses, phones, emails, Social Security numbers, relatives, associates, and linked records
Online accounts	Usernames, email/account links, platforms, and account-oriented result objects
Dark documents and breaches	SSN, payment-card-like values, crypto addresses, Discord/Telegram handles, username, IP, email, phone, keyword, `darkDocs`, and breach/leak table fields
Signals and devices	Email-to-location, hashed-email device lookup, registration ID, advertising ID/MAID, IP-to-signal, location/radius, timestamps, and device points
Bulk signals	Client-side load limit of 500,000 rows; total points, unique registration IDs, unique IPs, and time-range summaries
Ballistics and public-safety data	National Integrated Ballistic Information Network (NIBIN)-style classes, inmates, warrants, guns, property, accidents, citations, trafficking/IMB, and ICAC leads
Convoy and broker functions	Named `canCaravanSearch` permission and Lucidus redaction/opt-out workflow

The 500,000 figure is a client load limit, not evidence that a particular user exported that many rows. The point is architectural. The browser was built to ingest and summarize bulk location-signal data.

E.5 Organization-integrated modules

Nova models organization-specific search across RMS cases, RMS persons, RMS vehicles, CAD events, arrests, body-worn-camera events, and LPR results. Result classes include cases, people, vehicles, plates, scans, attachments, inmates, guns, property, accidents, citations, warrants, and evidence-adjacent objects.

These modules make Nova more than a commercial-record search tool. They connect identity and signal sources to agency incident, case, arrest, vehicle, person, video, and LPR systems. Organization flags decide which integrations are visible, while the backend must enforce whether a selected organization and user may query the data.

E.6 Result store and pivot graph

The common result model contains people, emails, phones, addresses, vehicles, plates, devices, scans, IPs, signals, dark documents, places, online accounts, sex-offender records, linked data, bulk signals, and ICAC leads. Agency-oriented result classes add RMS cases, CAD events, integrated LPR, RMS vehicles and persons, retail events, arrests, BWC events, attachments, inmates, guns, property, accidents, citations, and warrants [L4].

Link helpers traverse relationships among those objects with bounded depth. The exposure reveals investigative strategy, not just schemas. It shows which objects are first-class nodes, which identifiers can start a search, and which relationships lead to the next pivot.

E.7 Dark-data and shared-build evidence

Flock published “Correcting the Record: Flock Nova Will Not Supply Dark Web Data” on May 30, 2025 [E40]. The later preserved client models dark-document and breach enrichment as first-class sources, accepts high-sensitivity identifier types, and renders `darkDocs` and breach-oriented result fields [L4, L27, L36, P2]. Tenant availability and backend population remain separate questions; the code establishes the product model.

The route wrapper treats `nova.flockdemo.com`, `app.flocknova.com`, and `stage.flocknova.com` as one application family and includes Lucidus, CodeFour, and Healthcare Safely host logic [L38]. The same client contains a Lucidus opt-out/redaction path. My opt-out request to Lucidus and Flock was not honored [L38].

Primary evidence path: FlockNova_Application_Capability_Enumeration.md and the preserved Nova JavaScript tree [L4].

Appendix F. Live Video, Edge, Mobile, and Federal Surfaces

The browser and ArcGIS vulnerabilities are part of a larger system. Local artifacts and public research document separate video, device, mobile, drone, and government-tier risks.

F.1 Live camera administration

Researcher-held screenshots show a Flock-branded HLS Stream Viewer / Video Admin Interface reached over cleartext HTTP on port 8900. Two distinct camera IDs displayed live or near-live street video. A file-content view enumerated on-device HLS segments with path, codec, duration, and size [L30].

Artifact	Content
`Raw Evidence/Screenshots/flock_camera_feed1.png`	Infrared street stream, timestamp, “Not Secure” browser state, camera ID
`Raw Evidence/Screenshots/flock_camera_feed_2.png`	Second camera ID and daytime street stream on the same admin class
`Raw Evidence/Screenshots/flock_camera_log.png`	On-device SD-card segment enumeration under the file-content view

404 Media independently reported AI-powered Flock cameras and feeds reachable over the open internet and demonstrated the risk through self-tracking [E25]. The local screenshots and journalism establish the surface class without claiming a current fleet-wide count.

F.2 Edge-device research

Published research and CVE records describe RCE, denial-of-service, and information-disclosure issues affecting Flock hardware and compute, including CVE-2025-59405, CVE-2025-59406, and a reported root shell on the Bravo compute box [L31, E30-E31, E41]. Falcon and Sparrow classes appear in the same research trail. These issues shift part of the threat model from cloud credentials to the sensor and compute equipment at the pole.

F.3 Mobile and drone applications

Client	Operational role	Security-relevant architecture
Field App	Technician installation and provisioning	Hardcoded internal backend, Wi-Fi gateway defaults, RTSP and camera-SSID flows
Flock on Patrol / Negroni	Officer plate and task client	Hardcoded backend, Auth0, analytics, and hotlist models
Sweetwater flagship app	Primary law-enforcement mobile client	Session replay, on-device detector assets, background location, microphone, media projection, and capture-related permissions
Aerodome	Drone-as-first-responder and dock operations	Drone/dock orchestration, mission video, operations and observability hosts

The APK evidence establishes architecture and endpoint classes. Live tenant behavior, current versions, and fleet prevalence are time-varying [L32-L33].

F.4 Government and GovCloud tier

The host corpus includes `*.gov.flocksafety.com`, `*.le.gov.flocksafety.com`, federal-oriented product names, and Aerodome architecture signals for AWS `us-gov-west-1` and S3-FIPS style endpoints [L5, L33-L34]. The evidence also contains federal, military, intelligence-community, and law-enforcement domain lists whose exact purpose is unresolved.

No live AWS credential is asserted. The issue is assurance. A vendor that runs government-segregated and GovCloud-region infrastructure should prove its development, credential, logging, mobile, and device controls meet the higher security expectation that tier implies.

Appendix G. Production Export Schema and Count Verification

G.1 Status and device counts

The December export contains 335,701 records. Status arithmetic is exact:

`214,073 inService + 83,427 inPlanning + 38,190 decommissioned + 11 unknown = 335,701`.

The most common device types were:

Device type	Records
Falcon	175,269
Picard	48,680
Wing	44,116
Raven	27,341
Condor	22,166
Falcon Highway	5,228
Falcon Flex	3,361
Avicore	2,359
Picard PTZ	1,647
Trailer	915
Multi-evidence device	749
Talkdown	743
Backhaul box	670
Wing Ubicquia	645
External	515
Wing Gateway	403

Smaller classes include drone and drone-support equipment, Sparrow, Automotus, LPR trailers, factory fixtures, Owl, and API/support records [L14].

G.2 Field semantics

Field	Interpretation
`id`, `externalId`	Internal and external identifiers for the record or device
`organizationId`	Organization relationship recorded on the row
`networkId`, `networkExternalId`	Network relationship and its external identifier

Field	Interpretation
`parentExternalId`	External identifier of a parent or gateway record when the row is a child component; it is a relationship field, not a location owner
`numOfChildren`, `numOfSiblings`	Recorded family/component counts
`Creator`, `Editor`	ArcGIS editor-tracking identities for row creation and last edit; they do not, by themselves, identify the camera manufacturer or the person currently operating the device
`CreationDate`, `EditDate`	ArcGIS creation and last-edit timestamps
`deviceType`	Source device-family label
`status`	Source lifecycle state used by the reachability filter
`active`	Separate integer flag; not substituted for `status`
`features`	Source capability or feature information
`direction`, `rotationAngle`	Orientation metadata
Geometry	Exact deployment coordinate in the source feature

Co-located Picard records can represent a component of another device. Parent relationships and identical geometry prevent those components from being treated as independent camera coverage merely because they occupy separate rows.

G.3 Detection-eligible filter

The study uses records whose `status` is `inService` or `inPlanning` and whose device type is one of:

`automotus`, `avicore`, `condor`, `external`, `falcon`, `falconFlex`, `falconHighway`, `lprTrailer`, `multiEvidenceDevice`, `picardPtz`, `sparrow`, `trailer`, `wing`, `wingGateway`, or `wingUbicquia`.

Decommissioned rows and support-only devices, including talkdown speakers and backhaul boxes, are excluded. Raven audio, drone support, factory fixtures, and ordinary Picard component rows do not inflate the route-blocking camera count under this filter.

Primary files:

- `Raw Evidence/ArcGIS/flocksafety_prod_arcgis_data/analysis_summary.json`
- `Raw Evidence/ArcGIS/flocksafety_prod_arcgis_data/count_verification.json`

- `Raw Evidence/ArcGIS/flocksafety_prod_arcgis_data/features_*.json`

Appendix H. Complete Installation Result Records

H.1 Result status

All 22 sites have a complete 5/20-mile pair in the V7 cohort `reachability-v7-audit-92bd2e6a45c3a7c6`. These are modeled route-coverage records, reported here with their per-scope weighted outcomes and the summary hash that binds each one.

All runs use routing engine `valhalla-3.6.3-auto-frozen-osm-camera-blind-directed-overlay-v6` under the V7 artifact contract, against the December 2025 `cameras.tsv` snapshot (SHA-256 prefix `f953e489d70c886f…`). The 5-mile artifact contains 1,000 near-stratum draws; the 20-mile artifact retains those records unchanged and adds 1,000 outer-stratum draws. Every draw remains in the denominator, including `excluded_unroutable` records.

The cells below are weighted percentages read as `U/C/P/R`: unobserved, confirmed, possible, and unresolved. They are reported for the single-policy **Primary H0** channel and the **Robust H0/H1/H2** channel, at each scope. Because the 20-mile estimator reweights the two strata by represented occupied housing, its weighted percentages are not raw count divided by 2,000. The summary SHA-256 binds each per-scope record.

Each record below shows the per-scope weighted U/C/P/R for both channels and the summary hash that binds it.

Site	Scope	Primary H0 U/C/P/R (%)	Robust H0/H1/H2 U/C/P/R (%)	Summary SHA-256
Anduril Industries Headquarters	5 mi	11.7/74.1/11.9/2.3	8.6/63.1/11.0/17.3	`953048e370c3f6f2c24cb09f484361ab5420ac497d9cd992123bbd1fc4abf45b`
Anduril Industries Headquarters	20 mi	1.2/69.5/27.8/1.6	0.9/61.7/26.2/11.3	`2d80679c7d97889373c631857a2b81e595da248e7455bc79bad1cb9921d640b3`

Site	Scope	Primary H0 U/C/P/R (%)	Robust H0/H1/H2 U/C/P/R (%)	Summary SHA-256
Buckley Space Force Base	5 mi	23.6/67.3/2.9/6.2	21.4/63.7/2.7/12.2	`db3bc7740ee4e618bd651d782332831f58a7efcd5cdb4ada928bde78ee1bce71`
Buckley Space Force Base	20 mi	5.5/88.6/2.4/3.5	4.9/81.1/2.6/11.3	`dc2f6a99ace9d94912ac8aac3592e4d34bab4e594cd07abd52eb5ffd5035c44b`
CIA Headquarters	5 mi	1.4/4.5/91.9/2.2	1.3/4.3/80.8/13.6	`0818cd99514031a58454659c83786a434c90103b3a4a54bebd9fde577fef5d5f`
CIA Headquarters	20 mi	1.2/70.6/24.5/3.7	0.7/62.1/21.2/15.9	`1a5f8851150d91b088c6b99a2e39b9359f69c755c26e23163e8f1ee122055d2c`
Camp Pendleton	5 mi	34.1/30.6/30.0/5.3	32.8/28.3/29.2/9.7	`6429bfc0df0eba25e2d8f9efb12ac4208c96194e5d73ecad007683da7cb51aa6`
Camp Pendleton	20 mi	4.9/58.7/32.3/4.0	4.8/54.8/30.4/10.0	`54ce229ad141a872281a0482e779a411de0e6803634c58c2151f0be50f48d4ad`
Eglin AFB	5 mi	17.9/78.7/0.0/3.4	17.8/77.4/0.1/4.7	`33ca0b11147d0523fe788624c398e8d694d000808d995422926230396e94026c`

Site	Scope	Primary H0 U/C/P/R (%)	Robust H0/H1/H2 U/C/P/R (%)	Summary SHA-256
Eglin AFB	20 mi	3.4/94.8/0.0/1.8	3.4/93.9/0.0/2.7	`1e16babf624a66e4ace6f01b0154b2f8de3aa97c79971f84ad1ed02f5e95ede7`
FBI Headquarters	5 mi	0.0/79.0/19.7/1.3	0.0/64.8/15.9/19.3	`cc9ffd1bccabb42276d1e1280e322decce79aa80e538f3e51eb09cfb21f9dc93`
FBI Headquarters	20 mi	0.0/73.0/24.6/2.4	0.0/65.0/21.6/13.4	`83c5b897f0af8176cc339e1152212c19f4972ff29c9bd18cac6ee12c12414e14`
Fort Benning	5 mi	23.1/29.5/39.9/7.5	23.1/24.7/44.7/7.5	`1b186ed5a8715a136f32bc8a7adc6c7ca1427ae78e6f4528ca724499f5f5020f`
Fort Benning	20 mi	13.4/59.0/17.5/10.0	12.9/56.9/18.9/11.3	`0e08d4ab5081ec987b92e78d95ee775a0e7fdf61751d1779cc1477474ec474ff`
Fort Cavazos (Hood)	5 mi	5.4/89.9/0.9/3.8	5.3/88.3/1.0/5.4	`cbd6489bf9ca360c039b61af832daa8bb43806e40542f53e451a69873d7b8954`
Fort Cavazos (Hood)	20 mi	4.5/87.2/0.4/7.9	4.5/85.7/0.7/9.2	`69be74d19cb9cea497af624dd9001a609f75a660b3ff3ff64fe0bcb2479582db`

Site	Scope	Primary H0 U/C/P/R (%)	Robust H0/H1/H2 U/C/P/R (%)	Summary SHA-256
Fort George G. Meade	5 mi	13.4/82.1/0.0/4.5	12.8/80.4/0.1/6.7	`a0f8b57a2a424ded3c49e5aa95007c090f09a737b52a84581e83f2cc585ead83`
Fort George G. Meade	20 mi	39.4/52.3/5.1/3.3	34.8/50.3/5.0/9.9	`6d757296f9cef904cdaf461d885903fb03098d939d1e7d05437ae3b1b6d0bc52`
Fort Lee	5 mi	0.1/95.5/0.0/4.4	0.1/89.4/0.4/10.1	`94c46816258e6ddfce09e2098fc9d9e85e4e30d09de76553c93cccf157f455c9`
Fort Lee	20 mi	0.0/92.0/0.0/8.0	0.0/89.2/0.1/10.7	`2d8dff1e32e8759277b512868da491c5673e8e03ece941aa9099276c099fe2dd`
Hurlburt Field	5 mi	37.6/61.6/0.0/0.8	37.5/61.4/0.2/0.9	`5d868f170bd962a497f3366feaebd0667ea4a47ced e6b7821b90d9bb3f83f038`
Hurlburt Field	20 mi	10.6/88.0/0.0/1.4	10.5/87.0/0.1/2.4	`4bc61cf84624ce7859b0ab396a7659f47896a6699a4f4dff885515f48cf846ae`
Jet Propulsion Laboratory	5 mi	10.2/87.7/0.9/1.2	9.7/85.5/1.6/3.2	`596a01ce33c7e692ac81a2afad5e6987e7aa96a96d651a4f745df1e9eb62346f`

Site	Scope	Primary H0 U/C/P/R (%)	Robust H0/H1/H2 U/C/P/R (%)	Summary SHA-256
Jet Propulsion Laboratory	20 mi	1.7/91.7/3.9/2.7	1.6/87.9/3.9/6.7	`8ff6fdf35df7c82215b00687ce82e62e0d41b1a69f6da22a16d802e69ad5461e`
Joint Base Andrews	5 mi	7.0/90.1/2.2/0.7	5.8/80.5/2.7/11.0	`a1144dec96565c8894041335a65dab46ef5987b6cb2119d9b57fff4e71c7f4fc`
Joint Base Andrews	20 mi	11.6/77.1/8.7/2.6	9.1/68.8/9.1/13.0	`5cd8a212a349dc1628ac607737f544dc15c342c59663b51c6e9e8996c41e5fb3`
Joint Expeditionary Base Little Creek	5 mi	14.3/79.3/5.0/1.4	13.4/75.9/4.3/6.4	`8ab3a120dd753b85346376de149708cbedd126ef0ab2dfd4dc9f3a390f2f9aa0`
Joint Expeditionary Base Little Creek	20 mi	2.2/95.0/2.0/0.7	2.1/89.4/1.8/6.7	`5011d8ed71873ef380a15e8aa498b89f4756855daf6cd13ef045a64c99085573`
Lockheed Martin Headquarters	5 mi	20.2/1.4/72.2/6.2	19.3/1.1/65.7/13.9	`0622fec836e97693938159bbeb5ff172a75f60aa294ca69da44d188e25f9935b`
Lockheed Martin Headquarters	20 mi	12.4/18.6/65.5/3.5	11.0/15.6/61.7/11.7	`c8e58a92531c37c3fdddb6fc053a65b615ec5125178523276e95d54028255f7f`

Site	Scope	Primary H0 U/C/P/R (%)	Robust H0/H1/H2 U/C/P/R (%)	Summary SHA-256
MacDill AFB	5 mi	95.8/1.6/0.9/1.7	94.9/1.0/1.1/3.0	`d53a19928964cb5950e3b55cd8b1b2e4adf4a6fc1ea052f15ae1383333d2b5dd`
MacDill AFB	20 mi	28.5/56.7/12.3/2.5	27.1/54.9/12.4/5.7	`97dcbf63a9418bd7f79baa5c188a4644a81d8cd736a8dbd8cdda0a62365f908d`
Naval Amphibious Base Coronado	5 mi	44.0/6.9/46.5/2.6	42.4/6.4/46.2/5.0	`06dca0440a817e14da0be701c4d30000098450b1b3e96ffa77d468c42b09a906`
Naval Amphibious Base Coronado	20 mi	0.6/94.7/0.6/4.1	0.6/84.9/0.6/13.9	`a98258bd913c041e7e5006ba2fc47c5271e68145b3873ededcdf525a2929d532`
Naval Base San Diego	5 mi	2.2/87.5/6.5/3.8	1.6/74.2/7.8/16.4	`7b35a3241fd3436e50a345dcfe6d09900496da0db8f547d020f79b96d6816c58`
Naval Base San Diego	20 mi	2.6/75.3/16.1/5.9	2.2/67.0/15.7/15.1	`0ed2ff7ddbc73b03cacc460a01726a5f5b77f37b1009ffc64f3c7d1dcf909961`
Naval Station Norfolk	5 mi	20.9/78.5/0.4/0.2	19.3/72.0/1.3/7.4	`bfadd5800eb08fe038341ccd110eb419bdffba34d863445031181628d3082953`

Site	Scope	Primary H0 U/C/P/R (%)	Robust H0/H1/H2 U/C/P/R (%)	Summary SHA-256
Naval Station Norfolk	20 mi	19.6/78.9/0.5/1.0	18.5/75.4/0.8/5.3	`93f76cf615d8dc07449365f119c2cdd7a41c37100c2f8fb9b501bd3c1a34f9fa`
Northrop Grumman Headquarters	5 mi	83.7/5.2/10.3/0.8	76.2/4.3/10.8/8.7	`3b48f6f29c502cfd6e655ef02eb4d33b119f9c66065281c8581eeb6de792fe9f`
Northrop Grumman Headquarters	20 mi	18.5/22.5/56.0/3.0	17.0/18.5/50.5/14.0	`b953a439dca39d4fd85a5f3a917a17eb6fef6fa58215147e327f7b3aa336ac5a`
Pentagon	5 mi	1.1/65.9/16.8/16.2	0.4/52.0/13.3/34.3	`8c856d5dc5f90044ead4570fd6f3f73dd1353247992bc25fc3c99ab74526702d`
Pentagon	20 mi	0.6/66.3/24.8/8.3	0.5/57.2/22.3/20.0	`88025d463bd743523e4eac23bb59cb384c4a745815fa4cf055d6a001c18dfa81`
RTX Corporation Headquarters	5 mi	7.3/88.2/2.6/1.9	4.4/70.4/2.8/22.4	`6146b8b5557805808db419d9b1bafc5ccb67bedaa12ad86f21eca99b0a9739e5`
RTX Corporation Headquarters	20 mi	4.7/64.5/28.9/1.9	4.0/55.9/27.4/12.7	`c632b4d37585eac46270a7f82ecbe039d6995da4cbc021b2560857af28324aad`

Fort Benning’s 5-mile view is a documented single-gate near-base view (see the protocol’s gate-placement note); its 20-mile primary view uses both gates.

H.2 Required context for each result record

Each staged pair records its pair and cohort IDs, seed, routing engine and artifact contract, source/runtime/implementation hashes, reviewed gates, blockers and boundary source, represented occupied housing, residential and proxy candidates, in-service and planned camera counts, bounded origin-access scenarios, direction/corridor evidence, all four draw outcomes, uncertainty intervals, influence checks, and generation timestamp. The summary hashes are recorded in the snapshot at L41.

Town labels may be reported for geographic interpretation, but they do not define the sample or its weights.

H.3 Setup review and failure rules

The researcher reviews gates manually before each run. Generation preserves every saved gate, blocker, boundary, and cantonment. The engine records rejected gate options and fails each access hypothesis closed if it cannot construct a legal ordinary round trip through a saved gate without crossing the protected boundary elsewhere. Unresolved draw weight stays in the denominator.

A record is treated as unreliable when a required stratum is empty; route, source, runtime, or setup provenance changes; the route exceeds its scope; an independent return or required camera/access field is missing; the nested 5-mile records change inside the 20-mile artifact; unresolved weight exceeds its guard; a high-influence camera lacks an exact source-hash-bound review; camera/corridor semantics fail validation; or any aggregate disagrees with the complete record. Where an origin-access or direction-sweep interval is wide, that width is reported alongside the estimate rather than hidden.

H.4 Complete artifact locations

The V7 results are recorded in the hash-bound snapshot at L41 (`Supporting Tools and Docs/project_support/planning_and_qa/reachability_v7_audit_development_snapshot.json`), which carries each scope's estimates, frame accounting, split uncertainty intervals, QA flags and warnings, seeds, and per-record SHA-256 summary hashes. The large per-origin staging artifacts (route geometry, frame classification, review packets) are not shipped in this package; the full per-origin records are retained by the researcher offline for authorized review.

Appendix I. Evidence Source Locator

This appendix maps the paper's load-bearing claims to the package artifacts from which they were derived. The full citation catalog in `Supporting Tools and Docs/master_report/Research_Paper_Citations.md` provides the corresponding source IDs, provenance notes, and public-source metadata.

Evidence class	Principal package paths	What the artifacts establish
Four reported vulnerabilities	`Supporting Tools and Docs/supporting_memoranda/FlockSafety_Four_Vulnerability_Chain.md`; `Raw Evidence/Documentation/My_Four_Vulnerabilities.md`; `Raw Evidence/Documentation/My_Four_vulnerabilities.txt`	Submission order, dates, affected surfaces, discovery narrative, and the relationship among Vulnerabilities 1-4 [L2].
Vulnerability 1: hardcoded Default ArcGIS API key	`Raw Evidence/FlockSafety/flock_hardcoded_api_check.json`; `Supporting Tools and Docs/supporting_documents/analyses/FlockSafety_Dev_Subdomain_Bundle_Enumeration.md`; archived article source at L20/P1	Repeated public exposure, the 53-instance research finding, 50 private ArcGIS item grants, 13 premium capabilities, and production mapping-plane context [L5, L8, L20, P1].

Evidence class	Principal package paths	What the artifacts establish
Vulnerability 2: FlockSafety wrong-layer bundles	`Raw Evidence/FlockSafety/`; `Supporting Tools and Docs/supporting_documents/analyses/FlockSafety_Dev_Subdomain_Bundle_Enumeration.md`; `Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Search_App_Data.md`; `Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Hotlist_App_Data.md`; `Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Mapped_Attributes.md`	Pre-authentication delivery of application logic; Search, Hotlist, and FlockOS schemas; route/API vocabulary; permissions; feature flags; ArcGIS layer construction; CAD/AVL, alert, device, and registry concepts [L5, L11-L13].
Vulnerability 3: Planner/Beefeater token minting	`Raw Evidence/FlockSafety/dev_app_flocksafety_com/dev-beefeater/`; `Raw Evidence/FlockSafety/dev_app_flocksafety_com/prod-beefeater/`; `Raw Evidence/ArcGIS/planner_flocksafety_com/Prod_ArcGIS_Permissions.json`; chain memorandum and source disclosure at L2/L37	Unauthenticated mapping-token issuance, production-scope credential behavior, request/response captures, and the path used to acquire the December production export [L2, L37].
Vulnerability 4: FlockNova wrong-layer bundles	`Raw Evidence/FlockNova/nova_flockdemo_com/js/`; `Supporting Tools and Docs/supporting_documents/analyses/FlockNova_Application_Capability_Enumeration.md`	148 JavaScript files; freeform and advanced search; person, vehicle, plate, signal, MAID/ad-ID, RMS, CAD, arrest, BWC, dark-data, and result-pivot models; client-visible authorization and feature gates [L4].

Evidence class	Principal package paths	What the artifacts establish
ArcGIS production camera/device export	`Raw Evidence/ArcGIS/flocksafety_prod_arcgis_data/analysis_summary.json`; `Raw Evidence/ArcGIS/flocksafety_prod_arcgis_data/count_verification.json`; row-level `features_*.json` files in the same evidence directory	335,701 records; status and device-type distributions; fields, identities, coordinates, organization/network metadata, and the distinction between `status` and the separate `active` field [L14, L15].
ArcGIS item and layer behavior	ArcGIS evidence indexed at L6-L10 and L21-L25; `Raw Evidence/Screenshots/ArcGIS_FeatureLayer_Evidence/`	Private-item grants, service capabilities, camera/device registry fields, detections, search results, device status, and private/police/mobile category examples [L6-L10, L21-L25].
Retention evidence	`Raw Evidence/Screenshots/data_extension.png`	Catalog entries for one-, three-, and five-year extended-data options, including recorded list prices and product scope [L26].
Nested route-exposure studies	SHA-256-bound V7 snapshot at L41; method in Appendix L	The V7 protocol and complete 5/20-mile pairs for 22 sites: weighted draws, bounded access hypotheses, independent legal returns, same-corridor field-of-view observations, four outcome classes, uncertainty intervals, fixed seeds, source/runtime/implementation snapshots, and aggregates [L41]. Section 5 and Appendix H transcribe these records.
Installation mission context	Selected official military and agency sources E32-E35, E48, E50-E63, E66-E67, E70-E72, E77-E79, and E100-E105 listed in `Supporting Tools and Docs/master_report/Research_Paper_Citations.md`	Official descriptions of installation missions, tenant organizations, and functions used to frame site-specific counterintelligence consequences.

Evidence class	Principal package paths	What the artifacts establish
Vendor scale and public posture	P-series and E-series sources in the citation catalog	Vendor statements about customer/network scale, public retention posture, and statements that the company had not been breached; congressional and agency context where cited.

The raw artifacts are the controlling evidence when a summary, memorandum, or public source conflicts with them. Derived tables must be regenerated or corrected to match the source artifact; the underlying record is not edited to fit the prose.

Appendix J. Validation Handoff

The following sequence lets counsel, an editor, or an independent technical reviewer reproduce the factual spine without repeating live testing against production systems.

Claim cluster	Primary check	Pass condition
Vulnerability 1	Compare the key-check artifact, bundle enumeration, permissions summary, and archived article evidence at L5/L8/L20	The same Default API key exposure is tied to the reported occurrence count, 50 private item grants, 13 premium capabilities, and the production ArcGIS mapping context.
Vulnerability 2	Inspect the captured FlockSafety bundle families and the Search/Hotlist/FlockOS enumerations at L5/L11-L13	The bundles expose the described application routes, data models, map construction, permission language, and endpoint classes before the application's login boundary.
Vulnerability 3	Inspect the archived Beefeater request/response material and production ArcGIS permissions artifact at L2/L37	The captures show unauthenticated token issuance with the reported production-scope mapping behavior and connect that path to export provenance.
Vulnerability 4	Re-run or inspect the static FlockNova bundle enumeration at L4	The 148-file corpus supports the listed search taxonomies, organization integrations, signal/MAID workflows, and pivot/result model.

Claim cluster	Primary check	Pass condition
Production export	Recompute counts from the row-level ArcGIS features and compare L14/L15	Total, status, active-field, and device-type counts reconcile exactly; `active` is not substituted for `status`.
Installation studies	Verify the L41 snapshot's per-scope aggregates, seeds, and per-record SHA-256 hashes; the full validator run against the staging root and routing engine is available on request for authorized review	Each pair uses the V7 artifact/engine contract; the 5-mile record contains 1,000 near-stratum draws; the 20-mile record retains them unchanged and adds 1,000 outer-stratum draws; all-hypothesis four-class composition, full denominators, uncertainty and influence fields, and source/runtime/implementation hashes agree across the snapshot's staged summaries.
Routing-heuristic accuracy	Re-score the blinded review labels against the sealed prediction key (Appendix O)	The camera-blind corridor rule matches blinded human judgment about 89.5% of the time. It is strong where access is simple and weaker in dense or contested geometry. Reported in full as a single-reviewer methods check in Appendix O.
Citations	Run source-path, source-ID, and URL-integrity checks	Every cited ID exists, every local source resolves, required public URLs are present, and no body citation points to an undefined source.
Publication artifact	Build the PDF from the report and citation catalog, then inspect the rendered result	The PDF includes the complete report, appendices, source catalog, readable tables, intact figures, and no unresolved entries.

Validation rules:

1. Treat the repository evidence as the primary record and public material as corroboration, context, or a statement attributable to its publisher.
2. Keep the four vulnerabilities in submission order. Vulnerability 1 is the hardcoded Default ArcGIS API key; Vulnerability 3 is the unauthenticated token-minting path.

3. Preserve the December export's provenance. It was acquired through the Vulnerability 3 path, not the Vulnerability 1 key.
4. Do not substitute a current live response for a preserved historical capture. Remediation can change a live system; it cannot erase what the dated artifact records.
5. Verify quantitative claims with the package scripts or direct structured-data queries. Do not reconcile numbers by editing prose alone.
6. Preserve the original evidence artifacts and any research attestations as the fixed record of what was collected; do not edit them to fit the prose.

Appendix K. Figure Index

Fig	Code	File	Purpose and principal sources
7	C1	`figures/figC1_status_breakdown.svg`	Status composition of the 335,701-record export [L14, L15].
8	C2	`figures/figC2_device_families.svg`	Largest device families in the export [L14, L15].
4	C3	`figures/figC3_credential_scope.svg`	Vulnerability 1 scope: 50 private item grants and 13 premium ArcGIS capabilities [L8].
Unnumbered	F1-A	`../../Raw Evidence/Screenshots/Hardcoded_Api_Unredacted.png`	Unredacted Default API key validation view and privilege list [L6, L8].
Unnumbered	F1-B	`figures/finding1/source/mobile_pd_camera_locations.png`	Public ArcGIS camera layer with fixed police, mobile police, and private categories [L10, L25, P1].
Unnumbered	F1-C	`figures/finding1/plate_camera_and_people_alerts.png`	Wing/livestream device fields and the people-detection alert model [L11-L13, P1].

Fig	Code	File	Purpose and principal sources
Unnumbered	F1-D	`figures/finding1/plate_detections_and_searches.png`	Public detections and cross-agency vehicle movement-history layers [L21, L23, L39, P1].
Unnumbered	F1-E	`figures/finding1/plate_registry_and_asset_status.png`	Camera-registry PII and municipal device-health/service fields [L22, L24, P1].
Unnumbered	F1-F	`figures/finding1/plate_flock911.png`	Flock911 ArcGIS-layer population and transcript timing model [L12, L13, P1].
Unnumbered	F1-G	`figures/finding1/plate_drone_telemetry.png`	Drone/video record and rendered operational state model [L13, L35, P1].
3	K1	`figures/figK1.svg`	Four-vulnerability chain in disclosure order [L2, L4, L5, L8, L11-L13].
Unnumbered	K2	`figures/figK2.svg`	Default-key ArcGIS blast-radius model [L6-L10, L20-L25].
Unnumbered	K3	`figures/figK3.svg`	FlockSafety Search, Hotlist, FlockOS, device, backend, and ArcGIS surfaces [L5, L8, L11-L13].
6	K4	`figures/figK4.svg`	FlockNova data-fusion, source-fanout, and pivot model [L4].
11	K7	`figures/figK7_disclosure_timeline.svg`	Disclosure, export, vendor-statement, and study chronology.
5	K8	`figures/figK8_beefeater_path.svg`	Vulnerability 3 token path and trust-boundary failure [L2, L37].

Fig	Code	File	Purpose and principal sources
1	K9	`figures/figK9_intersection_thesis.svg`	Intersection of the sensor mesh, control plane, and data-fusion layer.
9	K10	`figures/figK10_detection_gap.svg`	The two possible readings of the vendor's post-export no-breach statements.
Unnumbered	K11	`figures/figK11_edge_mobile_gov.svg`	Browser, mobile, edge, live-video, and federal deployment classes.
2	S1	`figures/figS1_escalation.svg`	One plate read escalating into an intelligence product across the platform stages [§1.4].
10	S2	`figures/figS2_threat_paths.svg`	Five access paths converging on the shared national movement record [§6.5].

The conceptual figures are hand-authored SVG in the report palette, and the SVG files are the publication masters; Mermaid sources remain for the K2 and K3 appendix diagrams. Screenshot provenance and captions are cataloged in Appendix N and the source registry.

Appendix L. Reachability Methodology Reproducibility Record

This appendix specifies the V7 vehicle-fingerprint nested residential route-exposure procedure used by cohort `reachability-v7-audit-92bd2e6a45c3a7c6`. The figures it produces are modeled estimates reported with uncertainty ranges, not empirical measurements. The detail below permits independent review and verification of the model outputs, for example by comparing the reported figures against the SHA-256-

bound snapshot at L41. This package does not ship the camera-blind routing engine or the route-level record needed to regenerate the cohort from scratch; those are retained by the author and are available on request for authorized review.

L.1 Inputs and shared parameters

Parameter	V7 value
Completed sample	1,000 draws from each distance stratum; sampling with replacement and probability proportional to occupied housing
Radius scopes	0-5 public-road miles and greater-than-5-to-20 public-road miles, determined by the larger of outbound and return gate distance
Nested artifacts	The 5-mile artifact contains the near-stratum draws; the 20-mile artifact contains those exact records unchanged plus the outer-stratum draws
Frozen controls	Pair-specific copies and SHA-256 hashes of saved gates, blockers, cantonment, military boundaries, camera source, base layer, implementation files, OSM PBF, Census PL file, and TIGER block file
Eligible gates	Manually reviewed gates understood to be open 24/7 to authorized traffic
Routing engine	`valhalla-3.6.3-auto-frozen-osm-camera-blind-directed-overlay-v6`, with the container image pinned by digest
Origin source	2020 Census PL occupied housing (`H0010002`) represented by frozen OSM residential buildings and addresses, with labeled block representative-point proxies only where needed
Origin access	Search vehicle-routable corridors within 150 m; deduplicate to at most H0/H1/H2; 2 m way-pinned route radius; endpoint nudge up to 8 m; 5 m node-snap escape when geometry permits; route and retain each hypothesis independently
Sampling	Deterministic from the recorded site seed; probability proportional to occupied housing within each distance stratum
Camera status	`inService` and `inPlanning` both count as operational and determine primary outcomes; each record keeps its original status so the `inService`-only floor is recoverable

Parameter	V7 value
Device eligibility	Detection-capable camera-device types listed in Appendix G; support devices and decommissioned records excluded
Route choice	Ordinary Valhalla `auto` outbound and independent legal return to the fastest legal in-scope saved gate for each access hypothesis, selected without camera locations
Camera model	Post-route field-of-view overlay; 150-foot primary range, 250-foot retained maximum, 75/150/250-foot curve, 35° primary direction gate, 25–60° sweep, and positive same-corridor evidence for confirmed exposure
Outcome lattice	`unobserved` and `confirmed_exposure` require agreement across every complete supported access hypothesis; disagreement/incompleteness is `possible_exposure`; `excluded_unroutable` remains in the denominator
Materiality controls	Origin-access interval span over 5 percentage points blocks; direction sweep and single-camera influence are tested; a camera moving the rate over 5 points requires an exact source-hash-bound review
Artifact contract	`nested-residential-origins-valhalla-primary-h0-dual-output-v7`
Cohort	`reachability-v7-audit-92bd2e6a45c3a7c6` (V7 run); modeled route-coverage estimates reported with uncertainty ranges

The integer `active` field is a separate source field and is not the camera-status filter. Planned devices disclose intended coverage and are counted as operational in the primary outcome under the stated December-2025-to-August-2026 assumption.

L.2 Data preparation and sampling

For each installation, the workflow performs these operations:

1. Copy and hash the saved gates, blockers, cantonment, military boundaries, camera source, base layer, and implementation files into a pair-specific workspace.
2. Acquire or reuse a verified Geofabrik state PBF, clip complete ways for the padded study area, and build a Valhalla graph with external enrichment downloads disabled.

3. Acquire or reuse verified 2020 Census PL and TIGER2020PL block files.
4. Assign occupied-housing weight to up to four frozen OSM residential points in each occupied Census block. Use a labeled block representative-point proxy only when no mapped residential point exists.
5. Exclude origins inside the protected target polygon. Discover vehicle-routable corridors within 150 meters, suppress only geometry-proven intersection-only branches, deduplicate physical ways, retain at most three bounded access hypotheses, and record whether the set is complete, truncated, or weakly supported.
6. Pin each hypothesis to its physical way and compute ordinary outbound and independent return distances to every saved gate. Reject a gate option when either route loses the selected access corridor, crosses the target boundary away from that gate, violates access rules, lacks complete directed trace provenance, or exceeds the applicable scope.
7. Assign each candidate to `0-5` or `>5-20` from the minimum legal round-trip gate distance.
8. Draw 1,000 observations with replacement from each stratum, using selection probability proportional to occupied housing.
9. Generate camera-blind outbound and independent legal return routes for every retained access hypothesis of each unique selected candidate, reusing the deterministic scenario set for repeated survey draws.
10. Overlay in-service and planned cameras on both fixed directed legs, require same-corridor evidence for confirmed exposure, collapse the hypotheses through the fail-closed status lattice, retain unresolved weight, calculate all uncertainty/influence diagnostics, and write the nested 5- and 20-mile artifacts.

The 20-mile estimator combines the stratum-specific rates using represented occupied housing. Town labels are attached for interpretation after sampling and have no effect on selection probability.

L.3 Ordinary routing and directed camera overlay

Valhalla `auto` costing generates ordinary travel-time routes from the frozen road graph. It accounts for road hierarchy, mapped access, one-way and turn restrictions, and ramp transitions. Camera locations are not passed into matrix, gate-selection, or route requests. Saved manual blockers remain 30-meter exclusion polygons because they represent analyst-declared road restrictions rather than sensor locations.

For each bounded origin-access hypothesis, gate candidates are considered in ordinary travel-time order. Outbound and independent return legs must retain the selected access corridor, remain within the stratum limit, and cross the protected boundary only through the saved gate. The engine tries the next saved gate when an option fails. A reversed outbound line is never substituted for the independently routed return. No gate, blocker, boundary, or cantonment is moved, rewritten, or removed.

After both route legs are fixed, each eligible camera is overlaid on the route by field of view. A camera confirms exposure only when the route passes within the selected range, travels in the camera's monitored direction within 35 degrees, and has positive same-corridor evidence. The primary status uses 150 feet, retained observations extend to 250 feet, and the summary reports the 75/150/250-foot curve plus a 25–60-degree direction-tolerance sweep. Direction is taken from the true road bearing at the camera rather than the noisy `rotationAngle`. An explicitly named `NB`, `SB`, `EB`, or `WB` device is confirmed when the vehicle travels in the named direction, while a directionless device is retained only as possible exposure on its road axis. Oncoming, perpendicular, parallel-but-separate, and grade-ambiguous traffic are not confirmed; nearby ambiguous encounters remain in the spatial-sensitivity record.

Unknown-direction cameras can produce possible exposure on the same physical way. A failed edge assignment cannot produce direction-confirmed exposure from proximity alone. A known-direction fallback must match the local route bearing, while an unknown-direction fallback remains possible. `inPlanning` matches classify exactly as `inService` matches do and are additionally recorded under their own status. Multiple co-located records and support components do not create independent primary barriers.

L.4 Classification algorithm

```
for each installation:
    frozen = freeze_and_hash_setup_sources_and_implementation()
    graph = build_pinned_valhalla_graph(frozen.osm_pbf)
    candidates = build_occupied_housing_frame(
        census_pl=frozen.census_pl,
        tiger_blocks=frozen.tiger_blocks,
        osm_residential_points=frozen.osm_pbf
    )

    access_sets = bounded_vehicle_access_hypotheses(
        candidates,
        search_radius=150_meters,
        max_hypotheses=3,
        route_pin_radius=2_meters,
        endpoint_nudge=8_meters
    )
    strata = assign_by_independent_legal_round_trip_gate_distance(
        access_sets, gates=frozen.saved_gates,
        scopes=[0_to_5_miles, over_5_to_20_miles], cameras=None
    )
    near = pps_with_replacement(strata.near, n=1000, seed=pair_seed)
    outer = pps_with_replacement(strata.outer, n=1000, seed=pair_seed)

    for unique candidate in near + outer:
        scenario_outcomes = []
        for hypothesis in candidate.access_hypotheses:
            outbound, independent_return = ordinary_valhalla_round_trip(
                hypothesis, gates=frozen.saved_gates,
                blockers=frozen.manual_blockers, cameras=None
            )
            observations = overlay_field_of_view_cameras(
                [outbound, independent_return], primary_range=150_feet,
                retained_max=250_feet, direction_tolerance=35_degrees,
                confirmed_requires_same_corridor=True
            )
            scenario_outcomes.append(classify(observations))

        outcome = all_hypotheses_lattice(scenario_outcomes)
        retain_unresolved_weight_in_full_denominator(outcome)

    write_5_mile_artifact(near)
    write_20_mile_artifact(near_unchanged=near, outer=outer)
    compute_access_direction_spatial_range_and_influence_diagnostics()
    verify_nested_records_and_frozen_hashes()
```

L.5 Outcome semantics

Each access hypothesis is classified first; each draw then receives one primary class from the all-hypotheses lattice:

Status	Meaning
`unobserved`	Every complete supported hypothesis is unobserved on both independently routed legs.
`confirmed_exposure`	Every complete supported hypothesis contains a direction-confirmed, same-corridor operational-camera observation.
`possible_exposure`	Hypotheses disagree, camera direction is unresolved, or access evidence is incomplete, truncated, or weakly supported.
`excluded_unroutable`	No legal, traceable route outcome can be established; the draw remains in the denominator as unresolved.

The public map surfaces these machine statuses under plain-English labels only: `confirmed_exposure` as “passes a camera,” `unobserved` as “avoids all cameras,” `possible_exposure` as “might pass a camera,” and `excluded_unroutable` as “couldn’t determine.” The labels are presentation aliases for the classes defined above and carry no separate semantics; in the primary single-hypothesis view, `possible_exposure` arises from unresolved camera direction or same-corridor edge on the one modeled route rather than from disagreement among roads.

The primary point estimate is the occupied-housing-weighted `unobserved` rate over the full sampled denominator. The summary also reports weighted confirmed, possible, and unresolved rates; raw draw counts and rates; origin-access, direction, and spatial/grade intervals; a 75/150/250-foot curve; a 25–60-degree direction sweep; single-camera influence; represented occupied housing; and a 95% Wilson sampling interval at the smaller of the design-effect-adjusted effective sample size and distinct-candidate count.

Gate or route failure is not recoded as camera exposure and is not dropped. A failed hypothesis broadens access uncertainty; a fully unresolved draw is `excluded_unroutable` on the full denominator. Empty strata, changed inputs, excessive route length, missing independent returns, incomplete observations, publication-material sensitivity, and unreviewed high camera influence fail generation QA instead of inflating precision.

This denominator invariant is verifiable from the released materials without the generator's origin-sampling source. The hash-sealed audit artifact and frozen decision record preserve the fixed draw count, the four classes that sum to the full denominator, and every sampled weight. The decision record fixes the sampling rule as 1,000 occupied-housing probability-proportional draws per stratum, with replacement, and states that no result weight is dropped, renormalized, or replaced by a substitute draw for an unroutable origin.

The package ships the fail-closed artifact contract and the validators alongside the sealed outputs. Neither the camera-blind routing engine used for the installation studies nor the sampler that selects origins is included; both are bound by hash and retained by the author, as stated at the head of this appendix. The no-backfill guarantee therefore rests on the reproducible arithmetic of the sealed artifact and the predeclared rule rather than on trust in unshipped code.

L.6 Why both radii are reported

Five miles concentrates on the immediate gate-approach market, where ordinary traffic has had less distance to disperse. Twenty miles is the primary broader housing-market approximation under the predeclared DoD-guided rationale. The 20-mile artifact includes the same near-base draws and routes, so the comparison no longer mixes two unrelated samples.

The headline rates remain separate and are never averaged. The 20-mile estimator instead weights the near and outer stratum estimates by represented occupied housing. A large difference therefore identifies a real contrast between the immediate and broader modeled residential markets under the same setup, route engine, camera overlay, and source snapshot.

L.7 Reviewer checks

1. Confirm the pair uses artifact contract `nested-residential-origins-valhalla-primary-h0-dual-output-v7`, routing engine `valhalla-3.6.3-auto-frozen-osm-camera-blind-directed-overlay-v6`, and one frozen cohort/runtime/implementation snapshot.
2. Confirm 1,000 draws in the 5-mile artifact and 2,000 in the 20-mile artifact, with 1,000 observations in each distance stratum.
3. Confirm every 5-mile feature appears byte-for-byte unchanged in the 20-mile artifact.

4. Confirm `unobserved + confirmed_exposure + possible_exposure + excluded_unroutable` equals the total, every sampled weight remains in the denominator, and weighted rates reconcile to represented housing.
5. Confirm identical pair and cohort IDs, seed, gates, blockers, target boundary, source/runtime/implementation hashes, camera filter, and camera snapshot.
6. Confirm each access hypothesis is way-pinned and independently routed, every resolved scenario has outbound and legal return geometry, each leg stays within scope, and gate-boundary and directed-trace checks pass.
7. Confirm every feature has complete scenario-specific camera arrays and direction/corridor/assignment evidence; display-route fields must not mix cameras from another hypothesis.
8. Compare `report.md`, `summary.json`, `study.csv`, `study.geojson`, `gate_pressure.json`, and the formal aggregate.
9. Review all blockers, warnings, access/direction/spatial intervals, range curves, unresolved rates, and camera-influence rows rather than deleting or normalizing them.
10. Use only the V7 cohort for the figures in this report; do not mix cohorts.

Appendix M. Claim-Confidence Matrix

This matrix is the report's factual audit layer. It records the principal support and the interpretation that must survive editing. It is intentionally more granular than the public narrative.

Confidence	Meaning
Proven	Directly established by a preserved repository artifact, structured-data calculation, or completed study output.
Completed model output	Directly transcribed from a complete V7 artifact and reported here as a modeled estimate with its uncertainty ranges.
Strong	Established by multiple artifacts or by repository evidence with independent or official corroboration.
Strong inference	The evidence supports the conclusion, but the conclusion combines facts rather than quoting one artifact.

Confidence	Meaning
Moderate inference	A plausible operational or policy consequence that should remain labeled as analysis rather than an observed event.

Claim	Confidence	Primary support	Interpretation / reviewer action
The four reported vulnerabilities form one exposure chain in submission order: hardcoded geospatial credential, FlockSafety application-map exposure, unauthenticated token minting, and FlockNova data-fusion exposure.	Strong	L2, L4, L5, L8, L11-L13, L20	Preserve the chronology and the distinct role of each vulnerability.
Vulnerability 1 exposed an active ArcGIS Default API key in public development/ demo assets.	Proven	L2, L5, L8, L20, P1	The repository and disclosure record establish the credential class and exposure.
The author's published research documented the same Default API key in 53 exposed instances.	Strong	L20, P1	Use 53 as the published exposure count.
Validation of the Default API key recorded 50 private ArcGIS item grants and 13 premium ArcGIS capabilities.	Proven	L8, L9	Keep both counts tied to the same validated credential-scope artifact.
The key was embedded in the unified FlockOS ArcGIS map component alongside dynamic, feature, marker, clustered-marker, heatmap, and custom-layer inputs.	Proven	L13, L20, P1	Establishes a production FlockOS mapping-plane role.

Claim	Confidence	Primary support	Interpretation / reviewer action
After validating Vulnerability 1's grant count and service scope, the author did not open any of the 50 private items or retrieve private police-department records behind them; the data-class reconstruction instead used public municipality, police-department, and Flock ArcGIS applications, FlockOS code, the production export, and human-source corroboration.	Author-attested method with repository corroboration	L10, L20-L25, P1	Preserve the ethical collection boundary and distinguish OSINT reconstruction from any direct inspection of private items.
The key's validated scope, FlockOS integration, granted private items, connected data classes, and customer scale support the conclusion that it likely exposed a broad ArcGIS-backed geospatial layer serving FlockOS deployments associated with roughly 5,000 police departments, 6,000 private communities, and 1,000 businesses.	Strong inference	L2, L8-L15, L20-L25, P1	Describe this as likely scope established from connected evidence, not as a claim that the key was a complete user-session token.

Claim	Confidence	Primary support	Interpretation / reviewer action
The connected ArcGIS/FlockOS evidence models surveillance infrastructure, law-enforcement location assets, people and vehicle alerts, hotlists, investigative search geography, camera-registry PII, device health, Flock911 incident/transcript/audio state, and drone telemetry.	Strong	L10-L14, L20-L25, L35, P1, E80	The evidence supports the data classes and mapping architecture; the exact contents of each private item were not obtained.
Production camera FeatureServer metadata documented anonymous query and Create/Update/Delete capability flags, creating an integrity and tamper-risk class in addition to confidentiality risk.	Proven for service metadata	L29	No destructive write was attempted.
Vulnerability 2 delivered FlockSafety Search, Hotlist, and FlockOS client bundles before the application's intended authentication boundary.	Strong	L2, L5, L11-L13	The vulnerability concerns wrong-layer application-logic exposure; tested backend behavior is cited separately.
The canonical FlockSafety host footprint is 370 hosts, distinct from a 387-host broader corpus, a 213-host strict development/preview subset, and 80 artifact-local hosts.	Proven	L5	Keep each count attached to its defined population.

Claim	Confidence	Primary support	Interpretation / reviewer action
Search/Monaco models plate, vehicle, geofence, camera selection, case/ reason, agency-contact, and people-search workflows.	Proven	L11	Application and request-shape evidence.
Hotlist/Strawberry-Soju models watchlists, alerts, hit history, people detections, CAD/Prepared911, drones, visual alerts, and regions of interest.	Proven	L12	Organization enablement may vary; the exposed model is established.
FlockOS code models CAD/AVL, officer and patrol assets, body-camera and drone layers, Flock911, Raven/audio, and alert-map surfaces.	Proven	L13	The application model and map-layer construction are preserved in source.
Flock Safety markets FlockOS and FlockNova as complementary layers of one platform: physical-detection visibility in FlockOS and data context in Nova.	Strong	E23, L4, L11-L13	This establishes one vendor-operated product stack; credentials and authorization boundaries remain technically distinct.
The Flock911/ Prepared911 integration models caller audio, transcripts, addresses, call metadata, transcript timing, audio playback state, incident selection, token retrieval, and browser caching in the same operational map context.	Proven	L12, L13	Preserve the distinction between the integrated application context and the credentials used by each downstream service.

Claim	Confidence	Primary support	Interpretation / reviewer action
Vulnerability 3 exposed pre-login issuance of ArcGIS and Google mapping tokens through the Planner/ Beefeater path.	Proven	L2, L37	Request/response captures establish the token-minting behavior.
The December 14, 2025 production device/deployment export was obtained through the Vulnerability 3 token path.	Proven	L2, L14, L37	Keep export provenance separate from Vulnerability 1.
The author did not separately notify Flock that the December export had been acquired.	Author-attested fact	L2, L14, L37	Preserve as part of the research chronology and accounting analysis.
After the export, Flock published categorical no-hack, no-breach, and no-exfiltration statements, then reinforced them while attacking a November 2025 video featuring the author.	Proven as vendor statement and source attribution	E26, E97, E98	Attribute the statements to Flock; its video criticism does not resolve the separate production-export event.
The post-export statements create two material possibilities: Flock accounted for the access but excluded it from its public framing, or its monitoring did not account for the bulk production-data access.	Strong inference	E26, E97, L2, L14, L37	This is the detection/ accounting dilemma; it does not require attribution to another actor.
Vulnerabilities 1 and 3 establish two distinct credential-control failures rather than one isolated leaked secret.	Strong	L2, L5, L8, L20, L37	Keep static-key leakage and pre-login token issuance analytically distinct.

Claim	Confidence	Primary support	Interpretation / reviewer action
Vulnerability 4 exposed 148 FlockNova JavaScript files before the intended application boundary.	Proven	L2, L4	File count and bundle corpus are recorded in the enumeration.
Nova models freeform and advanced searches across identity, online accounts, dark-data inputs, signals, IPs, LPR, RMS, CAD, arrests, body-worn camera records, and result pivots.	Proven	L4	The code establishes product structure; source availability varies by organization.
Nova can classify one input identifier, fan the search across configured identity, account, address, vehicle, LPR, signal, public-record, dark-data, and organization sources, normalize returned objects, and expose them for relationship pivots.	Proven	L4	This is the preserved client data flow, not a claim that every source returns a match for every search.
Nova models email-to-location, hashed-email device, registration-ID, advertising-ID/MAID, IP-to-signal, and geographic signal-search workflows.	Proven	L4	These are frontend workflow and identifier classes.
Nova's bulk-signal loader contains a 500,000-row client-side limit and tracks total points, registration IDs, IP addresses, and time ranges.	Proven	L4	The number is a client limit, not a statement that every tenant receives a 500,000-row result.

Claim	Confidence	Primary support	Interpretation / reviewer action
The preserved Nova client accepts high-sensitivity dark-data inputs and renders `darkDocs` plus breach/leak fields including crawl date, network, leak name, leak host, and download location.	Proven	L4, L27, L36	The client establishes a breach-oriented product capability; source population and tenant availability require separate evidence.
Nova's visible client enforcement gap is strongest outside the freeform pipeline, making consistent backend authorization essential.	Proven for frontend behavior	L4	Backend enforcement is a control requirement derived from the observed client behavior.
Flock's patent describes a device-agnostic dynamic surveillance network that uses neural networks to classify people by male/female and race classes, clothing, height, and weight and vehicles by make/model, color, and plate information; FreeForm markets natural-language people and vehicle search across enabled video and LPR sources.	Proven as patent and vendor description	E7, E37	The patent establishes Flock's described architecture; preserved client and product evidence establish the separately cited implemented search fields.
Vehicle movement can be searched through visible attributes such as color, body type, markings, damage, equipment, and logos even when a plate is unreadable.	Strong	E7, E37	This follows the patented object-query model and public FreeForm description.

Claim	Confidence	Primary support	Interpretation / reviewer action
Independent public-records reporting documented ALPR searches associated with protest activity, including searches connected to the “No Kings” protests.	Strong	E38, E39	Use as documented-use context, not as an event performed in this research.
The device-admin evidence records HLS live-video and on-device recording-list surfaces over plain HTTP on port 8900; independent reporting corroborates the open-internet camera-feed risk class.	Strong	L30, E25, E43	Surface existence is established; fleet-wide prevalence is not quantified.
Published CVEs and independent Bravo compute-box research document remote-code-execution, denial-of-service, information-disclosure, and root-shell risk classes in Flock edge devices.	Strong	L31, E30, E31, E41	Remediation status is time-dependent.
Field, Negroni, Sweetwater, Aerodome, and other mobile clients extend the system beyond the browser and expose additional endpoints, credentials, telemetry, and device permissions.	Strong	L32, L33	Architecture and application evidence.

Claim	Confidence	Primary support	Interpretation / reviewer action
Government-segregated hostnames, federal-domain references, and Aerodome `us-gov-west-1` configuration establish a GovCloud/federal deployment footprint.	Proven for architecture	L5, L33, L34	The evidence establishes deployment context, not compromise of a GovCloud workload.
The ArcGIS export contains 335,701 device/deployment records.	Proven	L14	Dated production snapshot.
The export contains 214,073 `inService`, 83,427 `inPlanning`, and 38,190 decommissioned records.	Proven	L14, L15	Status counts sum to the full snapshot.
The primary detection-exposure universe is 297,500 records: 214,073 `inService` plus 83,427 `inPlanning`.	Proven arithmetic	L14, L15	Planned devices keep their source label in every artifact and are counted as operational in the headline under the stated December-2025-to-August-2026 assumption.
The separate integer field `active=1` counts 214,233 records, 160 more than `status=inService`; the study correctly filters on status and device type instead.	Proven	L15	Do not substitute `active` for the canonical camera specification.

Claim	Confidence	Primary support	Interpretation / reviewer action
The V7 method uses one frozen 20-mile frame, occupied-housing probability proportional to size (PPS) sampling, nested 5/20-mile artifacts, bounded access hypotheses, independent legal returns, camera-blind Valhalla routing, and a post-route same-corridor field-of-view camera overlay over the full sampled denominator.	Proven protocol	L41, §4, Appendix L	Section 5 transcribes the completed V7 modeled outputs with their uncertainty ranges.
Public sources establish the acknowledged missions and institutional roles used to interpret all 22 selected installations and sites.	Proven as public context	E32-E35, E48, E50-E63, E66-E67, E70-E72, E77-E79, E100-E105	Public mission descriptions frame consequence; installation measurements shown in Section 5 are V7 modeled route-coverage outputs.
Repeated corridor observations can support pattern-of-life, association, organizational-tempo, and anomaly analysis even when each individual observation appears routine.	Strong analytical inference	L4, L11-L15, E24, E37	This is the counterintelligence mechanism analyzed by the paper.

Claim	Confidence	Primary support	Interpretation / reviewer action
A national device inventory combined with investigative fusion tooling can expose sensitive-site coverage, planned deployment, and the relationships among vehicles, people, organizations, and locations.	Strong inference	L4, L8-L15, L20-L25	The conclusion combines the proven inventory, application model, and credential scope.
National off-base housing statistics support treating civilian road corridors as a force-protection concern: GAO reports roughly two-thirds of service members live off base, while CRS reports about 58% receive BAH and obtain housing in the civilian market.	Strong	E44-E47	The national statistics motivate the study; installation outcomes come from the model rather than a local housing census.
Flock's public default retention period is approximately 30 days, while catalog evidence records optional one-, three-, and five-year extended-retention products.	Proven	E2, L26	Keep the default and extension products distinct.
Longer retention and identity-fusion tooling increase the feasibility of historical pattern-of-life and re-association analysis, including risk to protected persons and their close contacts.	Strong inference	E2, E36, L4, L11-L13, L26	Consequence analysis, not an assertion that this research identified a protected person.

Claim	Confidence	Primary support	Interpretation / reviewer action
The combined evidence supports treating Flock's security as national-security infrastructure governance rather than only vendor application security.	Strong inference	L2, L4, L5, L8, L11-L15, L20, L29-L37, L40, L41	This is the report's central conclusion; L41 is the modeled route-coverage support.
The 22 per-site 20-mile modeled unobserved estimates, their conditional primary H0 values, and per-site summary SHA-256 hashes.	Completed model output	L41, §5, Appendix H	Transcribed in the Section 5 and Appendix H tables; each is a modeled estimate reported with its uncertainty ranges. Not re-listed row-by-row here to avoid duplicating those tables.

Appendix N. Visual Evidence Catalog

The SVG files are the figure masters and are embedded in the PDF as vectors. Raw screenshots remain in `Raw Evidence/Screenshots/` and are indexed by source ID in `Supporting Tools and Docs/master_report/Research_Paper_Citations.md`. The retired reachability schematic and result chart remain excluded.

N.1 Figures embedded in the report

- **Figure 1 · intersection thesis:** `figures/figK9_intersection_thesis.svg`.
- **Figure 2 · observation-to-intelligence escalation:** `figures/figS1_escalation.svg`.
- **Figure 3 · four-vulnerability chain:** `figures/figK1.svg`.
- **Figure 4 · credential scope:** `figures/figC3_credential_scope.svg`.
- **Vulnerability 1 visual evidence:** F1-A through F1-G; unredacted repository screenshot plus exact P1 image assets and mechanically combined publication plates. Provenance and hashes are in `figures/finding1/README.md`.
- **Figure 5 · Vulnerability 3 token path:** `figures/figK8_beefeater_path.svg`.
- **Figure 6 · Nova data-fusion:** `figures/figK4.svg`.
- **Figure 7 · export status composition:** `figures/figC1_status_breakdown.svg`.

- **Figure 8 · device families:** `figures/figC2_device_families.svg`.
- **Figure 9 · production-access accounting dilemma:** `figures/figK10_detection_gap.svg`.
- **Figure 10 · threat-path convergence:** `figures/figS2_threat_paths.svg`.
- **Figure 11 · disclosure timeline:** `figures/figK7_disclosure_timeline.svg`.

N.2 Supporting publication figures

- `figures/figK2.svg` and `figures/figK2.mmd`: ArcGIS credential blast-radius model.
- `figures/figK3.svg` and `figures/figK3.mmd`: connected FlockSafety application surfaces.
- `figures/figK11_edge_mobile_gov.svg`: edge, mobile, live-video, and government-tier surfaces.

N.3 Primary screenshot groups

- **Default key and ArcGIS scope:** key exposure, ArcGIS permissions, item/layer metadata, public mobile/fixed/private camera mapping, detections, movement histories, registry PII, device health, Flock911, drone state, and FeatureLayer field evidence [L6, L8-L13, L20-L25, L29, L35, L39, P1].
- **FlockSafety capabilities:** Search, Hotlist, FlockOS, map, camera/device, Prepared911, and alert evidence [L11-L13].
- **FlockNova capabilities:** search taxonomy, signal and MAID workflows, dark-data inputs, organization integrations, and pivot/result views [L4, L27, L28, L35, L36].
- **Edge and live video:** HLS viewer, camera feeds, recording index, and supporting device evidence [L30, L31].
- **Mobile and federal architecture:** APK and bundle evidence for Field, Negroni, Sweetwater, Aerodome, government tiers, and GovCloud configuration [L32-L34].
- **Retention and movement history:** extended-retention catalog evidence and single-plate map history [L26, L39].

The screenshot catalog is evidentiary, not decorative. Captions in the citation catalog identify what each image proves and prevent a cropped interface image from carrying a broader claim than its fields support.

Appendix O. Routing-Heuristic Accuracy Check

The installation estimates depend on a camera-blind rule that selects the corridor a vehicle would use to reach the road network from each origin. This appendix compares that rule with blinded human judgment across all 440 sampled origins. The reviewer assessed the route without seeing camera locations and identified the corridor a vehicle would most likely take. This is a methods-quality check on routing, not a claim about the exposure estimates, and the complete result is reported below.

O.1 What was checked

The model chooses each origin's access corridor with one camera-blind rule (address-first, with nearest-auto as the alternate). The check asks whether that automatic choice matches a blind human reviewer's choice. It measures the route-**selection heuristic**, not the exposure estimates. The same 440-origin review packet is embedded verbatim in the V7 cohort (identical origins and corridor options), so the result applies directly to the V7 routing.

O.2 How it was scored

A prediction counts as correct when the rule's chosen corridor is one the reviewer also selected and the origin was not flagged as ambiguous. Accuracy is weighted by each origin's design weight and broken out by site, distance band, sampling stratum, named status, and hypothesis set for subgroups of at least 20 origins. The internal target was 95% overall, with every subgroup above 90%. Because this run is a single-reviewer methods check, the results are a diagnostic of where routing is strong or weak, not an independent multi-reviewer validation.

O.3 Result

A single reviewer completed a blinded review of all **440** origins (22 installations × 20 origins across two scopes) and assigned every label with high confidence and supporting evidence. The camera-blind rule agrees with the reviewer's corridor judgment **about 89.5% of the time** (address-first 89.46%, nearest-auto 89.63%):

Policy	Weighted accuracy	One-sided 95% lower bound	Incompatible selections	Subgroups below floor
address-first	**89.46%**	86.33%	8	14 of 31

Policy	Weighted accuracy	One-sided 95% lower bound	Incompatible selections	Subgroups below floor
nearest-auto	**89.63%**	86.51%	9	15 of 31

Accuracy is highest where access is unambiguous and lower in dense or contested geometry, as shown in the full breakdown below. The automatic corridor conflicted with the reviewer's choice for 8 address-first origins and 9 nearest-auto origins, and several dense-area subgroups fall below 90%. This is a single-reviewer methods check, not an independent multi-reviewer validation.

Complete per-subgroup accuracy (all adequately sized subgroups, n ≥ 20). Weighted corridor-selection accuracy (%). † marks a subgroup below 90%. The 17 unnamed origins (n < 20) are not individually broken out.

By installation site (n = 20 each):

Site	address-first	nearest-auto
FBI Headquarters	68.38 †	93.30
Naval Base San Diego	77.37 †	94.80
Fort George G. Meade	78.87 †	100.00
Anduril Industries HQ	79.10 †	68.35 †
Buckley Space Force Base	81.10 †	93.67
RTX Corporation HQ	82.31 †	92.67
Jet Propulsion Laboratory	82.55 †	77.52 †
Naval Amphibious Base Coronado	85.58 †	93.61
MacDill AFB	91.18	91.18
Fort Lee	91.93	85.80 †
Northrop Grumman HQ	92.48	89.96 †
Camp Pendleton	93.01	86.35 †
The Pentagon	93.49	79.31 †
Fort Cavazos (Hood)	93.84	93.84
Fort Benning	93.99	93.99
Joint Expeditionary Base Little Creek	94.88	100.00
CIA Headquarters	95.52	84.81 †
Eglin AFB	100.00	100.00

Site	address-first	nearest-auto
Hurlburt Field	100.00	100.00
Joint Base Andrews	100.00	93.32
Lockheed Martin HQ	100.00	100.00
Naval Station Norfolk	100.00	71.45 †

By distance band, sampling stratum, named status, and hypothesis set:

Subgroup	n	address-first	nearest-auto
Distance band > 5–20 mi	253	88.29 †	89.99 †
Distance band 0–5 mi	187	91.24	89.08 †
Stratum: weak singleton	23	85.25 †	85.25 †
Stratum: address matched	184	86.67 †	86.47 †
Stratum: multiple hypotheses	121	89.67 †	89.67 †
Stratum: ordinary named access	97	96.55	96.55
Named origins	423	89.53 †	89.70 †
Hypothesis set: multiple	219	81.54 †	81.86 †
Hypothesis set: single	221	97.90	97.90
Overall (all 440)	**440**	**89.46**	**89.63**

The pattern is consistent across both policies. Accuracy is high where access is unambiguous (single-hypothesis origins 97.9%, ordinary named access 96.6%) and degrades where the access geometry is genuinely contested (multiple-hypothesis origins about 81 to 82%, address-matched about 86 to 87%). The two policies also trade weaknesses across sites, and neither dominates.

O.4 What this means for the estimates

The routing rule is right about nine times in ten, and strongest exactly where access is simple. Where it is weaker, in dense, multi-gate, or contested geometry, that uncertainty is already carried by the origin-access and direction ranges reported next to every site in Section 5 and Appendix H, and a wrong corridor pick tends to shift an origin between *confirmed* and *possible* rather than flip whether a camera is encountered at all. The check is printed in full so a reader can judge the routing's limits directly.

O.5 Scope and limitations

This check concerns the corridor-selection heuristic only; it says how well the route model matches human judgment, not anything about real plate reads or any share of personnel, commuters, or observed travelers. It used a single reviewer, so the 89.5% is a single-rater figure, informative but not an independent multi-reviewer result. It covers the 22 sites in this study and does not generalize beyond them. All figures trace to the sealed prediction key and the frozen review labels for the 440-origin packet shared by both cohorts.

Research Paper Citations

Prepared: 2026-08-21
Updated: 2026-08-21 for the consolidated public report and unredacted counsel package

This citation inventory is shared across the entire disclosure package. It covers the master report `Supporting Tools and Docs/master_report/Flock Safety - Vulnerability Disclosure and National Security Analysis (Michael 2026).md`, the supporting memoranda, and the 22 per-site documents under `National Security Exposure Studies/`. It separates **my** repository evidence, collected from Flock-exposed assets during my vulnerability-disclosure research, from external public context. When statements conflict, prioritize repository L-sources over current public vendor language. External E-sources are for product framing, policy context, and third-party corroboration.

Scope and numbering. Because the inventory is package-wide, not every code is cited in every document. In particular, most installation mission, unit, and deployment references (roughly E106–E175) are cited in the per-site `National Security Exposure Studies/` documents rather than in the master report; the master report's appended bibliography lists only the sources it cites, so those installation-only sources do not appear there and their absence is expected, not an omission. E-code numbering also contains intentional gaps (for example E68–E69, E75–E76, E115) where candidate sources were dropped during review; a gap is a skipped number, not a missing citation.

Inventory counts. Camera/device inventory totals and status breakdowns (335,701 total; 214,073 `inService`; 83,427 `inPlanning`; 38,190 decommissioned; 11 unknown; `active=1` 214,233) are from the package feature dump under `Raw Evidence/ArcGIS/flocksafety_prod_arcgis_data/` (`features_*.json`), summarized in `analysis_summary.json` and verified in `count_verification.json` [L14, L15].

Label note: Findings 1–4 are in **submission order**: Finding 1 is the hardcoded Default ArcGIS API key first reported on 2025-06-11. L2 uses the same labels.

Package Document Inventory

Package path	Role
`README.md`	Package purpose, top-level hierarchy, and export context.
`MANIFEST.md`	Complete zip-hierarchy manifest for the Markdown disclosure package.
`PATH_MAP.md`	Working-repo → package-local path map.
`PDF_EXPORT.md`	Markdown → PDF conversion guide for zip distribution.
`Supporting Tools and Docs/supporting_documents/finding_cards/Finding_01_Hardcoded_ArcGIS_Default_API_Key.md`	Cure53-style card: Finding 1.
`Supporting Tools and Docs/supporting_documents/finding_cards/Finding_02_FlockSafety_Wrong_Layer_Bundles.md`	Cure53-style card: Finding 2.
`Supporting Tools and Docs/supporting_documents/finding_cards/Finding_03_Planner_Beefeater_Token_Minting.md`	Cure53-style card: Finding 3.
`Supporting Tools and Docs/supporting_documents/finding_cards/Finding_04_FlockNova_Wrong_Layer_Bundles.md`	Cure53-style card: Finding 4.
`Supporting Tools and Docs/master_report/Flock Safety - Vulnerability Disclosure and National Security Analysis (Michael 2026).md`	Primary technical report (full intersection narrative).

Package path	Role
`Supporting Tools and Docs/master_report/Research_Paper_Citations.md`	Citation inventory and source hierarchy.
`Supporting Tools and Docs/supporting_documents/evidence_annex/FlockSafety_FlockNova_Evidence_Annex.md`	Exhibit index and validation map.
`Supporting Tools and Docs/supporting_documents/analyses/FlockNova_Application_Capability_Enumeration.md`	Canonical FlockNova capability and access-control enumeration.
`Supporting Tools and Docs/supporting_documents/analyses/FlockSafety_Dev_Subdomain_Bundle_Enumeration.md`	Canonical FlockSafety host, bundle, and dev-subdomain enumeration.
`Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Search_App_Data.md`	Search/Monaco data-model and workflow evidence.
`Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Hotlist_App_Data.md`	Hotlist, alerting, hit-history, and Prepared911/CAD evidence.
`Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Mapped_Attributes.md`	FlockOS map-plane, device/layer, CAD/AVL, and integration evidence.
`Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Shared_Layer_Inference.md`	Bounded analysis of shared ArcGIS layer implications.
`Supporting Tools and Docs/supporting_memoranda/FlockSafety_Four_Vulnerability_Chain.md`	Formal four-finding disclosure chronology in submission order.
`National Security Exposure Studies/`	22 per-site coverage assessments (PDFs in the folder; markdown under `Markdown/`).

My Repository Evidence

ID	Source	Use
L2	`Supporting Tools and Docs/supporting_memoranda/FlockSafety_Four_Vulnerability_Chain.md`; `Supporting Tools and Docs/supporting_documents/finding_cards/Finding_01_…` – `Finding_04_…`; source-evidence: `Raw Evidence/Documentation/My_Four_Vulnerabilities.md`	Vulnerability timeline, Cure53-style finding cards, chain framing, remediation status.
L4	`Supporting Tools and Docs/supporting_documents/analyses/FlockNova_Application_Capability_Enumeration.md`	Nova search, access-control, and client-side enforcement-gap findings.
L5	`Supporting Tools and Docs/supporting_documents/analyses/FlockSafety_Dev_Subdomain_Bundle_Enumeration.md`	370-host headline footprint, dev bundle families, and repeated-key evidence.
L6	`Raw Evidence/Screenshots/Hardcoded_Api_Unredacted.png`; `Raw Evidence/Screenshots/arcgis_perms.png`	Unredacted API-key metadata, item-grant list, premium-capability list, and ArcGIS-permission screenshot evidence; the first image is embedded as Finding 1 plate F1-A.

ID	Source	Use
L7	`Raw Evidence/ArcGIS/planner_flocksafety_com/Ethical_DIsclosure.json`; `Raw Evidence/Documentation/My_Four_Vulnerabilities.md`	Original disclosure and follow-up context. The ArcGIS token in the ethical-disclosure notes was rotated after validation and is retained as historical evidence.
L8	`Raw Evidence/FlockSafety/flock_hardcoded_api_check.json`	Primary validation artifact for key scope and 50 item grants.
L9	`Raw Evidence/FlockSafety/portal_app_access_item_urls.txt`	50 ArcGIS item URL inventory; unresolved item contents remain item-specific.
L10	`Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Shared_Layer_Inference.md`	Shared-layer architecture and access-universe analysis; records the ethical decision not to retrieve records from all 50 private items, the public municipality/police/Flock ArcGIS OSINT reconstruction, and participating police-department human-source corroboration.
L11	`Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Search_App_Data.md`	Search app data model, people-search device pool, plate/vehicle/search workflows.
L12	`Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Hotlist_App_Data.md`	Hotlist, alerts, hit history, and alerting data model.

ID	Source	Use
L13	`Supporting Tools and Docs/supporting_documents/analyses/ArcGIS_Mapped_Attributes.md`	FlockOS/map layers and attributes; CAD/AVL, patrol/mobile, body-camera, drone, Raven/audio, and Flock911 surfaces; Flock911 incident-layer state, audio/transcript token classes, per-word start/end timing, selected-event state, and playback/scrub controls.
L14	`Raw Evidence/ArcGIS/flocksafety_prod_arcgis_data/analysis_summary.json`; source dump: `Raw Evidence/ArcGIS/flocksafety_prod_arcgis_data/features_*.json`	2025-12-14 ArcGIS export summary: 335,701 records, status/device-family counts from the package feature dump.
L15	`Raw Evidence/ArcGIS/flocksafety_prod_arcgis_data/count_verification.json`	Field verification: total/status breakdown; `active=1` (214,233) vs `status=inService` (214,073) split; confirms scale claims use `status`, not `active`.
L20	`Raw Evidence/Documentation/My_Four_Vulnerabilities.md`; P1	Repository disclosure record and published article for my 53-exposure research, Finding 1 scope analysis, and public ArcGIS corroboration method.
L21	`Raw Evidence/Screenshots/ArcGIS_FeatureLayer_Evidence/arcgis_search_results_featurelayer.png`	Screenshot evidence of a publicly exposed ArcGIS FeatureLayer containing Flock search-result fields: plate, capture time, capture network/camera, and coordinate columns.
L22	`Raw Evidence/Screenshots/ArcGIS_FeatureLayer_Evidence/camera_registry_demo_featurelayer.png`	Screenshot evidence of a camera-registry demo FeatureLayer containing contact, location, location-type, and camera-count fields.

ID	Source	Use
L23	`Raw Evidence/Screenshots/ArcGIS_FeatureLayer_Evidence/flock_detections_featurelayer.png`	Screenshot evidence of a publicly exposed Flock detections FeatureLayer containing vehicle-detection fields such as plate, state, reason, network, and camera.
L24	`Raw Evidence/Screenshots/ArcGIS_FeatureLayer_Evidence/flock_camera_device_status_featurelayer.png`	Screenshot evidence of a Flock camera/device FeatureLayer containing location, serial-number, uptime, status, and support-status fields.
L25	`Raw Evidence/Screenshots/ArcGIS_FeatureLayer_Evidence/flock_camera_inventory_categories_featurelayer.png`	Screenshot evidence of a Flock camera FeatureLayer containing camera names/numbers, direction, private/PD/mobile categories, on/off state, and camera-type fields.
L26	`Raw Evidence/Screenshots/data_extension.png`	Vendor pricing / product catalog rows for sellable extended-retention SKUs: `extended_data_1_year` (up to 1 year, USD 600 list), `extended_data_3_years` (NJ 3 years, USD 1,000 list), `extended_data_5_years` (LA County 5 years, USD 1,700 list), each described as extended data retention for one LPR / law-enforcement-grade camera. Proves multi-year retention is a priced product option, not only a vague contract exception; list prices are retention-option evidence, not current customer invoices.

ID	Source	Use
L27	`Raw Evidence/FlockNova/nova_static/static/js/558.9638ce82.chunk.js`; `Raw Evidence/Screenshots/darkdata_returned_by_api.png`; `Raw Evidence/Screenshots/darkdocs_rms.png`; `Raw Evidence/Screenshots/flocknova_adult_websites.png`	Nova online-account / dark-web enrichment evidence. The chunk contains a hardcoded dictionary mapping web domains (a large set of adult/escort/dating sites) to `occurrences` counts and `riskLevel` values (`HIGH` / `MEDIUM` / `LOW`), and a result-detail component rendering profile fields including `bio` and `Breach`. A companion table renders leak/breach records with columns `Crawl Date`, `Network`, `Leak Name`, `Leak Host`, `Download Location`, `Open`; result buckets include `darkDocs` ("Dark Documents") and `rmsPersons` ("RMS Persons").
L28	`Raw Evidence/Screenshots/Nova_gives_you_address_from_food_delivery_App.png`	Flock's own marketing material (a Gary, Indiana RTCC case-study slide, "Gary PD RTCC Homicide Solve") stating that after a plate search, "Nova returns known associate's address from recent food delivery service." Vendor-sourced confirmation that Nova resolves home addresses from consumer-app / commercial data. Use for vendor-described capability only.
L29	`Raw Evidence/ArcGIS/planner_flocksafety_com/layer0.json` (and related planner/prod permission metadata)	Production FeatureServer `flock_safety_production` metadata: anonymous query flag, Create/Update/Delete support, attachments enabled. Used for the integrity/tamper capability class.
L30	`Raw Evidence/Screenshots/flock_camera_feed1.png`; `Raw Evidence/Screenshots/flock_camera_feed_2.png`; `Raw Evidence/Screenshots/flock_camera_log.png`	Unauthenticated live camera HLS viewer over plain HTTP on device admin port (`:8900/.../hls/videoAdmin`) and on-device recording-segment enumeration. Screenshots from my research.

ID	Source	Use
L31	`Raw Evidence/Screenshots/404_blog_post.png`; `Raw Evidence/Screenshots/flock_blog_post.png`; E41	Preserved context for edge-device security research, CVE-2025-59405, CVE-2025-59406, and the GainSec Bravo compute-box root-shell writeup.
L32	`Raw Evidence/Apps/` APK inventory	Mobile APK inventory: Field App (`zima.flocksafety.com`, Wi-Fi gateway defaults, RTSP), Negroni/Patrol (`negroni.flocksafety.com`), flagship Sweetwater 1.52.0 (FullStory session replay, on-device detector models), Aerodome package identity.
L33	`Raw Evidence/Apps/aerodome_apk/`	Aerodome drone C2 surface: dock/drone orchestration, mission video, ops hostnames, and GovCloud-region architecture signals.
L34	`Supporting Tools and Docs/supporting_documents/analyses/FlockSafety_Dev_Subdomain_Bundle_Enumeration.md`; `Raw Evidence/Apps/aerodome_apk/`	Federal/GovCloud-tier host footprint: `*.gov.flocksafety.com`, `*.le.gov.flocksafety.com`, Aerodome `us-gov-west-1` / S3-FIPS region signals.
L35	`Raw Evidence/Screenshots/permissions_dronetoo.png`; `Raw Evidence/FlockNova/nova_flockdemo_com/js/nova_flockdemo_com_App.js`	Permission vocabulary including `canCaravanSearch`, Aerodome access, device tunnels, AVL sharing, nationwide lookup, and ArcGIS sign-in.

ID	Source	Use
L36	`Supporting Tools and Docs/supporting_documents/analyses/FlockNova_Application_Capability_Enumeration.md`; source-evidence pointers: `Raw Evidence/Screenshots/lucidus_opt_out.png`; `Raw Evidence/Screenshots/all_data_context.png`; `Raw Evidence/Screenshots/dark_data_ingestion.png`; `Raw Evidence/Screenshots/search_darkdata_by_ui.png`	Lucidus identity-broker redaction string; expanded Nova result taxonomy; dark-data UI accepting SSN/CCN/crypto/Discord/Telegram-class inputs. Structure only.
L37	`Raw Evidence/FlockSafety/dev_app_flocksafety_com/dev-beefeater`; `Raw Evidence/FlockSafety/dev_app_flocksafety_com/prod-beefeater`	Burp XML wire records for Finding 3: anonymous GETs to Beefeater `/api/v1/token/esri` and `/token/google` returning HTTP 200 with tokens; no cookie/authorization.

ID	Source	Use
L38	`Raw Evidence/FlockNova/nova_flockdemo_com/js/nova_flockdemo_com_App.js` (`RoutesWrapper` / `isLucidusTech`); `Raw Evidence/FlockNova/nova_static/static/js/558.9638ce82.chunk.js` (Lucidus redaction component); `Raw Evidence/Screenshots/lucidus_opt_out.png`	Shared-codebase / provenance proof: the Nova frontend served from `nova.flockdemo.com` (from which the code was pulled in early December 2025) treats `nova.flockdemo.com`, `app.flocknova.com` (production), and `stage.flocknova.com` identically to the acquired `app.lucidustech.com`, `stage.lucidustech.com`, `app.codefour.ai`, and `app.healthcaresafely.com` in its `isLucidusTech()` host allowlist - i.e., demo and production run the same build, rebutting any "demo, not production" characterization. Same code base carries the in-app "Legally Requested Redaction from the Lucidus Database" opt-out path (`mailto:system@lucidustech.com`); my opt-out request to both Lucidus and Flock was not honored. Indicates Nova is assembled from acquired products (CodeFour.ai, Healthcare Safely, Lucidus).
L39	`Raw Evidence/Screenshots/ArcGIS_Map.png`	My screenshot of a publicly exposed police-department ArcGIS map loading a Flock "Search Results" FeatureLayer that plots a single license plate's geotagged reads across named cameras with timestamps and coordinate columns - concrete, agency-exposed proof that an individual vehicle's movement history can be materialized on a map from Flock data. Same public/agency-exposed posture as L21–L25.

ID	Source	Use
L40	Superseded pre-V7 (V4/V5) detailed run. The full per-origin paired study records are retained by the researcher offline for authorized review and are not shipped in this package.	The granular per-origin records (synthetic origins, gates, blocks, selected and attempted routes, blocked-camera observations, outcome records, seeds, and summary hashes) come from the earlier V4/V5 method run. They were removed from the shipped package because they were superseded by the V7 run and contain exact per-origin routes near the installations. The canonical V7 route-coverage estimates and their SHA-256 summary bindings are in L41 and control any transcription conflict.
L41	`Supporting Tools and Docs/project_support/planning_and_qa/reachability_v7_audit_development_snapshot.json`; full stage recorded by `source.stage_path` in that snapshot	V7 documentation source for cohort `reachability-v7-audit-92bd2e6a45c3a7c6` (the corrected run): exact 22-pair/44-scope estimates, four full-denominator outcome classes, access/direction/spatial/sampling sensitivity fields, known-limitation and warning fields, pair IDs/seeds, methodology identifiers, and SHA-256 bindings to every staged summary. These are modeled route-coverage estimates reported with their uncertainty ranges.

Published Research by Joshua Michael

ID	Source	Use
P1	https://nexanet.ai/blog/53-times-flocksafety-hardcoded-the-password-for-americas-surveillance-infrastructure	Joshua Michael's January 8, 2026 research article for the 53 repeated key exposures, reported network/customer scale, FlockOS "one map" framing, public ArcGIS OSINT reconstruction, and original visual exhibits preserved at `Supporting Tools and Docs/master_report/figures/finding1/`.

ID	Source	Use
P2	https://nexanet.ai/blog/license-plate-reader-company-flock-said-it-does-not-use-dark-web-data-my-analysis-of-their-code-tells-a-different-story	Joshua Michael's published research article for FlockNova dark-data/code analysis.

External Public Sources

ID	Source	Use
E1	Flock Safety, "License Plate Reader (LPR)" product page, https://www.flocksafety.com/products/license-plate-readers	Current public product framing for LPR capture, search, and retention caveats; includes FAQ-style claims that LPR cameras do not collect personal information or facial recognition (used for marketing-boundary analysis only).
E2	Flock Safety, "Flock Evidence Policy," https://www.flocksafety.com/legal/flock-evidence-policy	Vendor-claimed default 30-day retention statement and customer/legal retention caveats; cite alongside L26 because 1-, 3-, and 5-year extension SKUs are evidenced in the repository.

ID	Source	Use
E4	Flock Safety, “Not All License Plate Readers are Equal,” https://www.flocksafety.com/blog/not-all-license-plate-readers-are-equal-when-plate-data-fails-how-do-investigations-continue	Public claim that the network processes more than 20 billion vehicle reads each month across 49 states and connects thousands of law-enforcement agencies.
E6	Flock Safety, “FlockOS,” https://www.flocksafety.com/products/flock-os	Official FlockOS framing: “One Map. Smarter Response,” 24/7 situational awareness, and integration of video, LPR, sensors, CAD, RMS, drones/DFR, 911, gunshot detection, FreeForm, sharing, and geospatial mapping. Accessed 2026-07-22.
E7	Flock Safety, “Flock FreeForm,” https://www.flocksafety.com/products/flock-freeform	Official FreeForm framing: AI-assisted natural-language search and alerts across enabled video and LPR evidence for people and vehicles using clothing, visible accessories, vehicle type/color/damage, and other non-biometric visual descriptions. Accessed 2026-07-22.

ID	Source	Use
E20	U.S. Supreme Court, Carpenter v. United States opinion, https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf	Digital location privacy policy/legal context.
E21	Library of Congress, United States v. Jones, 565 U.S. 400, https://www.loc.gov/item/usrep565400/	GPS tracking/location surveillance policy/legal context.
E22	Justia, Riley v. California, 573 U.S. 373, https://supreme.justia.com/cases/federal/us/573/373/	Digital privacy and search policy/legal context.
E23	Flock Safety, “Why Public Safety Needs a New Kind of Platform,” https://www.flocksafety.com/blog/why-public-safety-needs-a-new-kind-of-platform	Official Flock framing that Nova and FlockOS are complementary layers of one platform: FlockOS provides visibility into physical detections, Nova provides data context, and the marketing phrase is “search once and see everything.” Accessed 2026-07-22.
E24	Senator Ron Wyden and Representative Raja Krishnamoorthi, letter to FTC Chair Andrew N. Ferguson regarding Flock Safety, November 3, 2025, https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_ftc_on_flockpdf.pdf	Congressional policy corroboration that Flock’s movement data and cybersecurity posture raise FTC, hacker/foreign-spy, MFA, unauthorized-access, and sensitive-location privacy concerns.

ID	Source	Use
E25	404 Media, “Flock Exposed Its AI-Powered Cameras to the Internet, We Tracked Ourselves,” https://www.404media.co/flock-exposed-its-ai-powered-cameras-to-the-internet-we-tracked-ourselves/	Independent reporting that Flock AI-powered cameras/feeds were exposed to the open internet (journalists tracked themselves). Primary public corroboration of the live-camera / open-device-admin video exposure class also documented in author-held screenshots [L30]. Also used as security-posture context against blanket “never breached” claims. Accessed 2026-07-13.
E43	YouTube video, “This Flock Camera Leak is like Netflix For Stalkers,” https://www.youtube.com/watch?v=vU1-uiUlHTo	Secondary public coverage of the same Flock live-camera leak issue reported in 404 Media [E25]; useful as accessible context for the open-feed risk class. L30/E25 remain the primary technical basis. Accessed 2026-07-14.

ID	Source	Use
E26	Flock Safety, “Has Flock Been Hacked?,” https://www.flocksafety.com/blog/has-flock-been-hacked (anchors `#has-flock-been-hacked` and `#has-flock-ever-had-a-data-breach`)	Vendor page originally published 2026-01-06. The live page displayed a 2026-07-24 revision date when rechecked. It repeats the denial in at least three formulations: never hacked/no leak; cloud infrastructure never compromised/no customer-data access or exfiltration by an attacker; and never had a data breach/no customer data compromised. Accessed 2026-07-27.
E28	Flock Safety, “Update on Limited Condor Device Configuration Issue,” https://www.flocksafety.com/blog/update-on-limited-condor-device-configuration-issue	Vendor disclosure acknowledging a device-configuration issue affecting Condor devices; used as a documented security-relevant incident. Accessed 2026-07-13.
E29	Flock Safety, “Response to Compiled Security Research on Flock Safety Devices,” https://www.flocksafety.com/blog/response-to-compiled-security-research-on-flock-safety-devices	Vendor public response contesting/downplaying compiled third-party security research on Flock devices. Accessed 2026-07-13.

ID	Source	Use
E30	GainSec, “Formalizing My Flock Safety Security Research,” November 5, 2025, https://gainsec.com/2025/11/05/formalizing-my-flock-safety-security-research/	Primary page for an independent researcher’s compiled Flock Safety security research; corroborates that other researchers publicly examined the same platform. Accessed 2026-07-13.
E31	GainSec, “anti-crime-ecosystem-research” (GitHub repository), https://github.com/GainSec/anti-crime-ecosystem-research	Independent researcher’s public repository compiling Flock Safety / anti-crime-ecosystem security research; the body of third-party work Flock’s response [E29] addresses. Accessed 2026-07-13.
E32	U.S. Air Force, Hurlburt Field, “1st Special Operations Wing” fact sheet, https://www.hurlburt.af.mil/About-Us/Fact-Sheets/Fact-Sheets/Article/204524/1st-special-operations-wing/	Public mission framing: 1st SOW at Hurlburt Field under AFSOC; specialized/ contingency airpower for special operations worldwide. Accessed 2026-07-13.
E33	U.S. Air Force, Hurlburt Field, “Air Force Special Operations Command” fact sheet, https://www.hurlburt.af.mil/About-Us/Fact-Sheets/Fact-Sheets/Article/2559811/air-force-special-operations-command/	Public AFSOC framing: specialized aircraft and special-operations airpower; 1st SOW at Hurlburt. Accessed 2026-07-13.

ID	Source	Use
E34	U.S. Air Force, Hurlburt Field, “361st Intelligence, Surveillance, Reconnaissance Group” fact sheet, https://www.hurlburt.af.mil/About-Us/Fact-Sheets/Fact-Sheets/Article/204546/361st-intelligence-surveillance-reconnaissance-group/	Public mission framing: 361st ISRG provides specialized ISR support / threat warning and situational awareness for AFSOC aircrews. Accessed 2026-07-13.
E35	U.S. Air Force, Eglin AFB, “96th Test Wing” fact sheet, https://www.eglin.af.mil/About-Us/Fact-Sheets/Display/Article/390959/96th-test-wing/	Public mission framing: Eglin-hosted developmental test and evaluation of air-delivered weapons, guidance/navigation, C2, AFSOC systems, and related acquisition support, including private-industry customers. Accessed 2026-07-13.

ID	Source	Use
E36	U.S. Marshals Service, “Witness Security,” https://www.usmarshals.gov/what-we-do/witness-security	Public description of the federal Witness Security Program: security/safety of government witnesses and authorized family members whose lives are endangered by testimony; relocation and new-identity framing. Used only for program existence and protective purpose, not operational methods. Accessed 2026-07-13.

E37	Flock Group Inc., U.S. Patent No. 11,416,545 B1, “System and Method for Object-Based Query of Video Content Captured by a Dynamic Surveillance Network,” issued Aug. 16, 2022, https://patents.google.com/patent/US11416545B1/en	Flock’s own patent. Confirmed language: a “dynamic surveillance network” that is device-agnostic and ingests video from “unrelated surveillance devices” (neighborhood, residential, business, traffic, portable/mobile cameras); a “dynamic surveillance and object-based query” (DSOQ) server/system; object-based query of video “based on content of the video footage and not just time and location”; attribute profiling of people (“male, female, race,” height/weight/clothing) and vehicles (make/model/color/plate); and “face recognition data points”/facial-similarity feature-vector matching. Used only for the vendor’s own described architecture and intended capability; the report does not claim Flock has deployed any specific patented

ID	Source	Use
		function, including facial recognition. Accessed 2026-07-13.
E38	Electronic Frontier Foundation, “How Cops Are Using Flock Safety’s ALPR Network to Surveil Protesters and Activists,” November 2025, https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists	EFF public-records investigation: more than 12 million Flock searches logged by over 3,900 agencies between December 2024 and October 2025, including dozens of searches by nineteen agencies tied specifically to the “No Kings” protests and hundreds of protest-related searches by more than fifty federal, state, and local agencies (including U.S. Border Patrol), sometimes explicitly referencing demonstrations and sometimes using vague terms to obscure surveillance of protected speech. Used as documented First Amendment / protest-surveillance use of the network. Accessed 2026-07-13.

ID	Source	Use
E39	The Record (Recorded Future News), “Flock Safety cameras used to monitor protesters, rights group finds,” https://therecord.media/flock-safety-rights-group-eff	Independent reporting corroborating the EFF finding that Flock ALPR searches were run in connection with protest activity. Accessed 2026-07-14.
E40	Flock Safety, “Correcting the Record: Flock Nova Will Not Supply Dark Web Data,” May 30, 2025, https://www.flocksafety.com/blog/correcting-the-record-flock-nova-will-not-supply-dark-web-data	Dated vendor public statement that Nova will not supply dark-web data. Used as the specific denial against which the exposed dark-data code (SSN/credit-card/crypto/messaging-handle lookups; breach/leak table) is contrasted. Accessed 2026-07-14.
E41	NVD, CVE-2025-59405, https://nvd.nist.gov/vuln/detail/CVE-2025-59405 ; Tenable, CVE-2025-59406, https://www.tenable.com/cve/CVE-2025-59406 ; GainSec, “Root Shell on Flock Safety’s Bravo Compute Box” writeup PDF (linked from local research notes)	Public edge-device vulnerability and root-shell research on Flock camera/compute hardware.

ID	Source	Use
E44	U.S. Government Accountability Office, *Military Housing: DOD Should Address Critical Supply Shortages* (GAO-25-106208), product page, https://www.gao.gov/products/gao-25-106208	GAO summary states that about **two-thirds of service members in the U.S. live off base in local communities**. Used for national off-base housing share context for force-protection commute exposure. Not an installation-level census. Accessed 2026-07-16.
E45	Congressional Research Service, *Military Housing* (CRS Report R47728), https://www.congress.gov/crs-product/R47728	CRS reports that about **58% of servicemembers** receive a tax-free housing allowance (BAH) and obtain housing from the local housing market outside their installation. Complements E44 (slightly different metric: BAH recipients vs "live off base"). Used for off-base housing / civilian-market commute framing. Accessed 2026-07-16.

ID	Source	Use
E46	DoD Travel Management Office / Defense Travel Management Office, Basic Allowance for Housing overview, https://www.travel.dod.mil/Allowances/Basic-allowance-for-Housing/	Official BAH framing: compensation based on local civilian housing markets when government quarters are not provided; members choose off-base housing in the civilian market. Used only for policy mechanism (BAH → civilian infrastructure), not for a percentage. Accessed 2026-07-16.
E47	U.S. Air Force Housing (Hurlburt Field), Military Housing Office orientation, https://www.housing.af.mil/Home-depricated/Units/Hurlburt-Field/	Installation housing office materials: members choose on-base privatized housing or the local community; notes privatized family housing eligibility structures (e.g., rank/time-in-service thresholds for some family housing). Used only for public installation housing-option framing near Hurlburt, not as a person-level census. Accessed 2026-07-16.

ID	Source	Use
E48	U.S. Navy, Commander, Navy Region Mid-Atlantic / Commander, Navy Installations Command, Naval Station Norfolk installation page, https://cnrma.cnic.navy.mil/Installations/NAVSTA-Norfolk/	Public mission framing: Naval Station Norfolk is the world's largest naval station and the headquarters and homeport of U.S. Fleet Forces Command and four carrier strike groups; Port Services publicly reports controlling on the order of 3,100 ship movements per year. Used only for publicly acknowledged mission context. Accessed 2026-07-18.

ID	Source	Use
E49	U.S. Department of Defense, DoD Manual 4165.63, *DoD Housing Management*, incorporating Change 3, April 1, 2025, Enclosure 3, section 1.c.(2), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/416563m.pdf	Official housing-market-analysis guidance: market-area boundaries may use a 20-mile or one-hour peak-traffic commute, with military/public information and installation-command recommendations supporting local adjustment. Used to justify a predeclared 20-road-mile primary reachability scope, not to claim that most personnel at a particular installation live within that distance. Accessed 2026-07-20.
E50	U.S. Space Force, Buckley Space Force Base, “Space Base Delta 2” fact sheet, https://www.buckley.spaceforce.mil/About-Us/Fact-Sheets/Display/Article/322399/space-base-delta-2/	Official Buckley mission and population context: installation support for space-based missile warning, space surveillance, space communications, resident air operations, and more than 110 mission partners; published personnel categories are used only as installation-level context. Accessed 2026-07-21.

ID	Source	Use
E51	U.S. Space Force, Buckley Space Force Base, *Stormwater Management Plan*, *Revision 2*, April 2025, https://www.buckley.spaceforce.mil/Portals/13/documents/Environmental/Final%20BSFB%20SWMP%20Revision%202%20April%202025.pdf?ver=Q_QI3YgoVtwRDzRlfYzwLA%3D%3D	Official installation document describing Buckley mission support for uninterrupted missile warning, intelligence, and cyber operations. Used only for public mission context, not operational schedules or classified functions. Accessed 2026-07-21.
E52	U.S. Marine Corps, Marine Corps Base Camp Pendleton, “About the Base,” https://www.pendleton.marines.mil/About/Base-Information/About-the-Base/	Official description of Camp Pendleton as the Marine Corps’ largest West Coast expeditionary training facility, its terrain, training role, and publicly named major commands and tenant organizations. Accessed 2026-07-21.

ID	Source	Use
E53	U.S. Marine Corps, Marine Corps Base Camp Pendleton, “Welcome Aboard,” https://www.pendleton.marines.mil/Base-Info/Welcome-Aboard/	Official installation context identifying the major resident commands and reporting that approximately 70,000 people work and live aboard the base. Used as a dated public population statement, not a commute census. Accessed 2026-07-21.
E54	Central Intelligence Agency, “CIA Headquarters,” https://www.cia.gov/legacy/headquarters	Official public history and location context for the Langley headquarters campus and its role as a workplace for thousands of CIA personnel. Used without inferring internal organization, schedules, or classified activity. Accessed 2026-07-21.

ID	Source	Use
E55	Central Intelligence Agency, “About CIA,” https://www.cia.gov/about/	Official description of CIA’s foreign-intelligence, all-source analysis, mission-center, technical, and digital responsibilities. Used only for publicly acknowledged mission context. Accessed 2026-07-21.
E56	Federal Bureau of Investigation, “FBI Headquarters,” https://www.fbi.gov/contact-us/fbi-headquarters	Official description of headquarters functions: directing and coordinating FBI activity, setting priorities and policies, serving as an intelligence and information hub, supporting field and overseas operations, and coordinating national crises. Accessed 2026-07-21.
E57	Federal Bureau of Investigation, “About,” https://www.fbi.gov/about	Official FBI mission and priority context, including counterterrorism, counterintelligence, cyber, public corruption, civil-rights, and major-crime responsibilities. Accessed 2026-07-21.

ID	Source	Use
E58	Federal Bureau of Investigation, “New FBI Headquarters in Washington, D.C.,” July 1, 2025, https://www.fbi.gov/news/press-releases/new-fbi-headquarters-in-washington-dc	Official announcement selecting the Ronald Reagan Building for a new FBI headquarters. Used to disclose the time-and-location limitation of a study configured around the package’s 935 Pennsylvania Avenue headquarters point; it does not retroactively change that modeled input. Accessed 2026-07-21.
E59	U.S. Air Force, Eglin Air Force Base, “53rd Wing Factsheet,” https://www.eglin.af.mil/About-Us/Fact-Sheets/Display/Article/813642/53rd-wing-factsheet/	Official context for operational test and evaluation across Combat Air Forces platforms and geographically distributed units. Used with E35 to frame test, evaluation, and mission-support scenarios without asserting nonpublic program activity. Accessed 2026-07-21.

ID	Source	Use
E60	U.S. Army, “Fort Benning,” https://www.army.mil/Benning	Official mission statement for the Maneuver Center of Excellence and Fort Benning: training combat-ready Soldiers and leaders and developing maneuver doctrine and capabilities. Accessed 2026-07-21.
E61	U.S. Army Garrison Fort Benning, “About,” https://home.army.mil/benning/About	Official installation description identifying the Maneuver Center of Excellence, Armor and Infantry schools, Ranger and other resident organizations, installation geography, and published community scale. Accessed 2026-07-21.
E62	U.S. Army Garrison Fort George G. Meade, “Mission,” https://home.army.mil/meade/about/mission	Official description of Fort Meade as a platform for intelligence, information, and cyber operations and of the garrison’s readiness-support role. Accessed 2026-07-21.

ID	Source	Use
E63	U.S. Army Garrison Fort George G. Meade, “Col. Sapp takes command of U.S. Army Garrison Fort George G. Meade,” https://home.army.mil/meade/about/Garrison/public-affairs/digital-meade/col-sapp-takes-command-us-army-garrison-fort-george-g-meade	Dated official context describing Fort Meade’s multi-service and civilian workforce and installation population. Used only as public scale context, not as a current person-level census. Accessed 2026-07-21.
E66	U.S. Air Force, Joint Base Andrews, “About the 316th Wing,” https://www.jba.af.mil/About/About-the-316th-Wing/	Official host-wing context: installation support to multiple wings, headquarters, and tenant organizations; National Capital Region contingency response; and security for a high-visibility flight line. Accessed 2026-07-21.
E67	U.S. Air Force, Joint Base Andrews, “89th Airlift Wing,” https://www.jba.af.mil/About/Fact-Sheets/Display/Article/336383/89th-airlift-wing/	Official description of global Special Air Mission airlift, logistics, and communications for senior U.S. leaders, including alert and continuous-support responsibilities. Used only for public mission framing. Accessed 2026-07-21.

ID	Source	Use
E70	U.S. Navy, Naval Base Coronado, “Naval Amphibious Base Coronado,” https://cnrsw.cnic.navy.mil/Installations/NAVBASE-Coronado/About/Installations/Naval-Amphibious-Base-Coronado/	Official description of West Coast amphibious, littoral, unconventional, and special-warfare training terrain and publicly named tenant commands at Naval Amphibious Base Coronado. Accessed 2026-07-21.
E71	U.S. Navy, Naval Base Coronado, “Mission and Vision,” https://cnrsw.cnic.navy.mil/Installations/NAVBASE-Coronado/About/Mission-and-Vision/	Official base-operations mission supporting warfighters, operating-force combat readiness, and ashore and afloat commands at Naval Base Coronado. Accessed 2026-07-21.

ID	Source	Use
E72	Naval Facilities Engineering Systems Command Mid-Atlantic, *Naval Station Norfolk Site Management Plan, Fiscal Years 2024-2028*, https://www.navfac.navy.mil/Portals/68/Documents/Business-Lines/Environmental/Environmental-Restoration/NAVFAC-Mid-Atlantic/Norfolk-NS/Final_NSN_SMP_FY_2024-2028.pdf?ver=yH5_mVb2SFTZp35UFu2LUA%3D%3D	Official installation description and mission context for Atlantic Fleet readiness, port infrastructure, airfield operations, and the developed waterfront. Used with E48; published infrastructure and ship-movement figures are dated and not treated as a current operational schedule. Accessed 2026-07-21.
E77	U.S. Department of Defense, “About,” Pentagon Tours, https://www.defense.gov/About/Pentagon-Tours/	Official statement that the Pentagon is Department of Defense headquarters and that DoD provides military forces to deter war and ensure national security. Used for institutional context, not for current occupancy or schedules. Accessed 2026-07-21.

ID	Source	Use
E78	U.S. Department of Defense, Office of the Director of Administration and Management, “About,” https://dam.defense.gov/About-DA-M/index.html	Official description of Pentagon Reservation governance, administrative support, continuity, security, law-enforcement, and emergency-management responsibilities supporting senior defense leadership and headquarters tenants. Accessed 2026-07-21.
E79	Washington Headquarters Services, “Facilities Services Directorate,” https://www.whs.mil/About-WHS/Directorates/Facilities-Services-Directorate-FSD/	Official public context for continuous Pentagon Reservation facility readiness and support to Office of the Secretary of Defense, Joint Staff, defense agencies, and military departments across the National Capital Region. Accessed 2026-07-21.

ID	Source	Use
E80	Flock Group Inc., *Flock Safety + SC - Sullivan's Island PD*, budgetary quote C-112082, November 8, 2024, public municipal procurement copy, https://cleargov.com/resource/cg-prod-v2/projects/documents/8491cdf11839242bf5e2.pdf	Vendor proposal describing the Esri-based FlockOS map as consolidating data streams and connected-asset locations into a common operating picture; also lists custom map layers, floor plans, external GIS data, Axon body-worn-camera locations, camera registry, network access, searches, hotlists, and Wing integration. Accessed 2026-07-22.

ID	Source	Use
E97	Flock Safety, Chris Castaldo, “Flock Safety Cybersecurity: How We Protect Customer & Community Data,” published March 27, 2026, https://www.flocksafety.com/blog/flock-safety-cybersecurity-how-we-protect-customer-community-data	Vendor cybersecurity-posture statement. It repeats that January hacking claims were false or misleading; directly criticizes a November 2025 video and characterizes an 80,000-camera hacking claim as false and misleading; describes Flock’s security, monitoring, incident-response, and third-party-assurance program; and concludes that Flock will continue to lead the industry in cybersecurity. The live page displayed a 2026-07-24 revision date when rechecked. Used as Flock’s own statement, not independent validation of its controls. Accessed 2026-07-27.

ID	Source	Use
E98	Benn Jordan, “We Hacked Flock Safety Cameras in under 30 Seconds,” YouTube, November 16, 2025, https://www.youtube.com/watch?v=uB0gr7Fh6lY	November video addressed by Flock in E97. The source description credits Joshua Michael, links his channel and original ArcGIS report, and incorporates his finding into the broader camera-security discussion. Used to establish the identity and author participation of the video Flock criticized; individual technical findings retain their primary repository and published sources. Accessed 2026-07-27.

ID	Source	Use
E99	Flock Safety, “What Makes a Public Safety Platform Secure,” published June 10, 2026, https://www.flocksafety.com/blog/what-makes-a-public-safety-platform-secure	Vendor security-posture page. It again answers “No, Flock’s cloud platform has not been hacked,” and attributes the reported activity to a single camera that had never been deployed to a customer, had not received software updates, and had never been connected to Flock’s cloud environment, distinguishing “a broad customer data breach” from “an isolated issue involving an undeployed device,” and closing that “security conversations are strongest when they’re grounded in facts, context, and transparency rather than assumptions.” A June 2026 reaffirmation of the January 6 (E26) and March 27 (E97) denials. Used as Flock’s own statement, not independent validation. Accessed 2026-07-27.

ID	Source	Use
E100	U.S. Army Fort Hood, “Mission and Vision,” https://home.army.mil/hood/about/mission-and-vision	Official description of III Armored Corps’ global multi-domain mission and the garrison’s role enabling units to train and deploy while supporting Soldiers, families, civilians, and retirees. The canonical study retains its saved label, Fort Cavazos (Hood), while the current official site uses Fort Hood. Accessed 2026-07-29.
E101	U.S. Army Fort Hood, “Home,” https://home.army.mil/hood/	Current official installation context describing Fort Hood as the Army’s premier installation for training and deploying heavy forces, supporting multiple units, a corps headquarters, and a mobilization mission across 214,968 acres. Used for public mission and scale context, not current unit movement. Accessed 2026-07-29.

ID	Source	Use
E102	U.S. Air Force, Nellis Air Force Base, “U.S. Air Force Warfare Center,” https://www.nellis.af.mil/About/Fact-Sheets/Display/Article/284150/us-air-force-warfare-center/	Official mission description for live and virtual operational test and evaluation, tactics development, and advanced training for joint all-domain combat operations; identifies the Warfare Center units based at Nellis. Current as of September 2025; accessed 2026-07-29.
E103	U.S. Air Force, Nellis Air Force Base, “57th Wing,” https://www.nellis.af.mil/About/Fact-Sheets/Display/Article/284155/57th-wing/	Official description of Nellis-based advanced multi-domain training, flight operations, the Weapons School, Red Flag, maintenance and munitions training, and professional aggressor functions. Used without inferring a current exercise, platform status, or participant. Accessed 2026-07-29.

ID	Source	Use
E104	U.S. Navy, Naval Base San Diego, “About San Diego,” https://cnrsw.cnic.navy.mil/Installations/NAVBASE-San-Diego/Resources/About-San-Diego/	Official description of Naval Base San Diego as the Navy’s premier Pacific Fleet surface-force installation, its homeported ships, tenant commands, Navy Region Southwest headquarters, medical complex, and family housing. Published ship and tenant counts are dated site context, not an operational schedule. Accessed 2026-07-29.
E105	U.S. Navy, Naval Base San Diego, “Mission and Vision,” https://cnrsw.cnic.navy.mil/Installations/NAVBASE-San-Diego/About/Mission-and-Vision/	Current official mission and vision emphasizing installation support, resilience, and operational readiness for the Fleet, Fighters, and Families. Used as public mission framing without inferring ship status, sailing time, or personnel assignments. Accessed 2026-07-29.

1. The disclosure chronology, anonymous Planner/Beefeater response captures, and production export are preserved as [L2], [L37], and [L14].↩

2. Flock Safety's "Has Flock Been Hacked?" page, originally published January 6, 2026 and subsequently revised [E26].↩
3. Flock Safety's March 27 cybersecurity post and Benn Jordan's November 16 video crediting Joshua Michael [E97, E98].↩
4. Flock Safety's "What Makes a Public Safety Platform Secure" page, published June 10, 2026 [E99].↩
5. Disclosure context, ArcGIS validation, application artifacts, production inventory, and connected FeatureLayer evidence [L2, L8-L15, L20-L25, P1].↩
6. Default-key enumeration, validated scope, FlockOS integration, and the author's published 53-instance research [L5, L8, L13, L20, P1]. The "dynamic surveillance network" description is Flock's own patent language [E37].↩
7. V7 cohort `reachability-v7-audit-92bd2e6a45c3a7c6` and its SHA-256-bound snapshot [L41]. These are modeled route-coverage estimates reported with uncertainty ranges rather than empirical plate-read observations.↩
8. Flock's platform description of FlockOS and Nova as complementary sensor and data layers, corroborated by the preserved FlockSafety and Nova clients [E23, L4, L11-L13].↩
9. FlockSafety Search, Hotlist, FlockOS, and Nova application evidence [L4, L11-L13]. Detailed inventories appear in Appendices D and E.↩
10. Flock Group Inc., U.S. Patent 11,416,545 B1 [E37].↩
11. Flock FreeForm product material, Search/Hotlist application evidence, and Wing/Business Network evidence [E7, L11-L13, L35].↩
12. My January 2026 publication records more than 30 billion monthly vehicle detections and the 5,000-department, 6,000-community, and 1,000-business context [P1, L2, L20]. Flock's current public page independently states more than 20 billion monthly reads across 49 states [E4].↩
13. Flock public evidence policy and retained catalog SKUs [E2, L26].↩
14. FlockSafety Search, Hotlist, FlockOS, Flock911, and FlockNova workflow evidence [L4, L11-L13, L27, L35-L36].↩

15. My January 2026 publication records more than 30 billion monthly vehicle detections, an undisclosed volume of people detections, and the customer/deployment context used here [P1]. Flock's current public material independently states more than 20 billion monthly vehicle reads [E4].↩
16. The "One map. Smarter Response." framing appears in my published Vulnerability 1 account [P1]. The quoted Esri-based map description is from a Flock proposal in a public municipal procurement record [E80].↩
17. Published 53-instance research [L20, P1].↩
18. ArcGIS key-scope validation and grant reconciliation [L8, L9].↩
19. FlockOS mapped-attribute analysis and the preserved Vulnerability 1 source record [L13, L20, P1].↩
20. Shared-layer architecture, public ArcGIS examples, code paths, and human-source corroboration [L10, L20-L25, P1].↩
21. Original publication images and article context [P1], with overlapping repository originals and schemas at [L10-L13, L21-L25, L39].↩
22. Production FeatureServer capability metadata [L29].↩
23. Canonical host and bundle enumeration [L5].↩
24. Search, Hotlist, and FlockOS application analyses [L11-L13].↩
25. Disclosure chronology and complete anonymous Beefeater response captures [L2, L37].↩
26. FlockNova application capability enumeration and disclosure record [L4, L2].↩
27. Nova result, source, signal, dark-data, and organization-integration evidence [L4, L27, L35, L36].↩
28. Shared Nova build and Lucidus evidence [L38].↩
29. Production ArcGIS export and verified field/count analysis [L14, L15].↩
30. Production export schema, ownership-field analysis, device relationships, and count verification [L14, L15].↩
31. Count verification distinguishing the integer `active` field from source `status` [L15].↩

32. Flock Safety's January 6 security-posture page and March 27 cybersecurity post, together with the November 16 video source identifying the author's contribution [E26, E97, E98].↩

33. Independent and local evidence concerning exposed feeds, device configuration, and edge research [E25, E28-E31, L30-L31].↩

34. DoD Manual 4165.63 housing-market guidance [E49] and the frozen V7 route-exposure method and snapshot [L41].↩

35. The SHA-256-bound V7 snapshot records the complete staged cohort and its source path [L41]. These are modeled route-coverage estimates, not empirical plate-read observations.↩

36. The SHA-256-bound V7 snapshot records the complete staged cohort and its source path [L41]. These are modeled route-coverage estimates, not empirical plate-read observations.↩

37. The SHA-256-bound V7 snapshot records the complete staged cohort and its source path [L41]. These are modeled route-coverage estimates, not empirical plate-read observations.↩

38. GAO, CRS, and DoD housing context [E44-E47].↩

39. Official public mission sources for Hurlburt, Eglin, Fort Cavazos/Hood, Buckley, and Joint Base Andrews [E32-E35, E50-E51, E59, E66-E67, E100-E103].↩

40. Flock retention evidence and Nova convoy, signal, identity, and pivot classes [E2, L4, L26, L35-L36].↩

41. Official Navy mission context for Norfolk, Coronado, and Naval Base San Diego [E48, E70-E72, E104-E105].↩

42. Official public mission sources for Fort Meade, CIA, the Pentagon, FBI, and Andrews [E54-E58, E62-E63, E66-E67, E77-E79].↩

43. U.S. Marshals Service public Witness Security Program description [E36].↩

44. *Carpenter v. United States*, 585 U.S. 296 (2018), and the report's legal-policy sources [E20-E22].↩

45. Flock LPR and FreeForm materials, the Flock patent, and Nova identity/pivot evidence [E1, E7, E37, L4].↩