

Eglin AFB

National Security Exposure Assessment

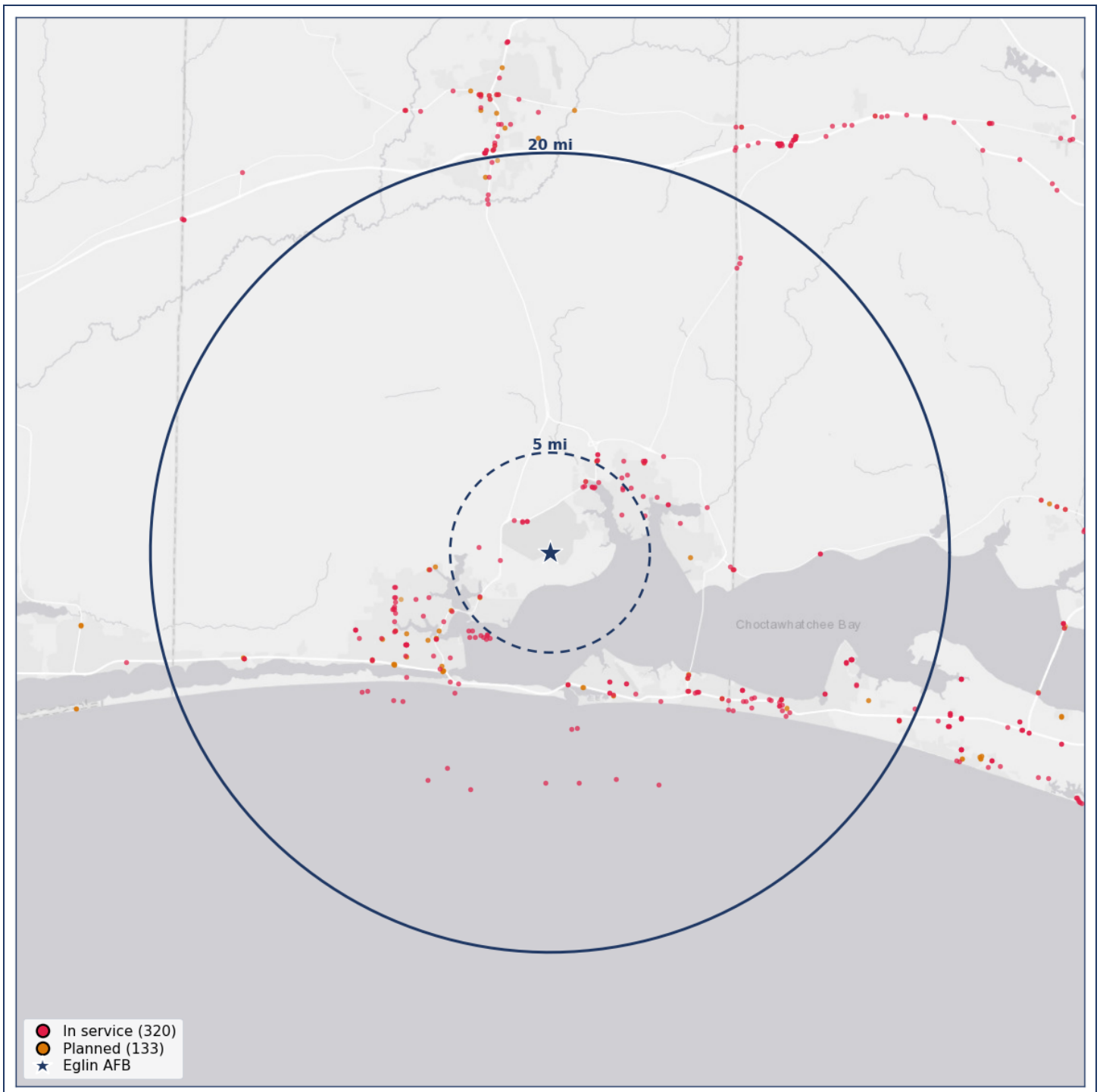
Joshua Michael

Email: josh@nexanet.ai



© 2026 Joshua Michael · [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/). Use with credit.

September 2, 2026



Executive Assessment

Eglin Air Force Base on the Florida Panhandle is the Air Force's big weapons-test range. The 96th Test Wing recently flight-tested the OA-1K Skyraider II here for special-operations support; the 7th Special Forces Group also sits on the reservation. If the same test pilots, maintainers, and specialists started moving together, that could mark a Skyraider II test milestone — without anyone publishing a press release.

This study asks a simple question: if someone drove from a nearby home to a gate and back, would they pass a Flock camera? The numbers are a model of possible drives, not a count of real people.

At 20 miles, about 93.9% of those modeled trips pass a camera. 3.4% avoid them, and 2.7% could not be determined. Even at 5 miles, about 77.4% of those trips still pass a camera. This is a model of routes, not proof that anyone was watched.

HEADLINE RESULT · MODELED TRIPS TO A GATE

20 MILES OUT



- 93.9%** **Passes a camera**
 A confirmed camera sits on every plausible road to a gate.
- 0.0%** **Might pass**
 Almost every trip could be called a clear pass or a clear miss.
- 3.4%** **Avoids all cameras**
 No confirmed camera on any plausible road.
- 2.7%** **Couldn't determine**
 Almost all trips produced a complete route.

5 MILES OUT



■ **77.4%** Passes
 ■ **0.1%** Might pass
 ■ **17.8%** Avoids
 ■ **4.7%** Couldn't determine

Installation Context

Eglin's 96th Test Wing publicly describes developmental test and evaluation for air-delivered weapons, guidance and navigation, command and control, and Air Force Special Operations Command systems, including support to government and private-industry customers [E35]. In 2025, the 96th Test Wing, in coordination with U.S. Special Operations Command, conducted developmental testing of the OA-1K Skyraider II at Eglin. The Air Force described the aircraft as a crewed platform intended to support geographically isolated special-operations personnel in austere locations through mission sets that include close air support, precision strike, and armed intelligence, surveillance, and reconnaissance. The publicly described test effort included military airworthiness, manufacturer-performance verification, human factors, handling qualities, austere landing, and planned sensor and weapons evaluations [E106]. This provides a specific, publicly documented test community through which to explain how recurring movement records could expose both personnel and program milestones.

The Eglin reservation also hosts the 7th Special Forces Group (Airborne) at Camp Bull Simons. The group's public mission is to organize, equip, train, validate, and prepare forces for worldwide special operations, and its published regional area of responsibility includes Latin America, the Caribbean, adjacent waters, and associated territories [E107]. Official Army reporting independently places the group at Camp Bull Simons on Eglin Air Force Base [E108]. This provides a separate and higher-consequence operational example: longitudinal movement records could potentially disclose the coordinated departure and return of a special-operations element even when the underlying mission remains protected.

The study uses these public mission facts only to identify realistic consequences if longitudinal movement records and reliable identity context became available. They do not alter route outcomes, select favorable cameras, identify personnel, or establish that either community was actually tracked. The quantitative model routes synthetic origins only through the two reviewed Eglin gates. It does not measure routes to Camp Bull Simons. The OA-1K scenario is therefore directly connected to the principal Eglin cantonment represented by the study, while the 7th Special Forces Group scenario is a reservation-wide threat illustration rather than a unit-specific empirical finding.

Installation-Specific Intelligence Scenarios

The reachability studies establish Tier A exposure information: the location, status, type, and modeled corridor relationship of detection-eligible devices under the declared inputs. They do not provide Tier B historical plate reads or Tier C identity, employer, household, or organizational enrichment. The scenarios below describe what could become inferable if a hostile actor obtained those additional data classes. They are analytic threat models, not findings that either collection or exploitation occurred.

Scenario 1: Identifying the OA-1K Skyraider II Test Team and Inferring Program Milestones

In 2025, the 96th Test Wing, in coordination with U.S. Special Operations Command, conducted developmental testing of the OA-1K Skyraider II at Eglin. The Air Force described the aircraft as a cost-effective crewed platform intended to support geographically isolated special-operations personnel in austere locations, with mission sets including close air support, precision strike, and armed intelligence, surveillance, and reconnaissance. Public reporting described testing of military airworthiness, manufacturer-performance data, human factors, handling qualities, and austere landing performance, with sensor-quality and weapons-release testing identified as later phases [E106].

Assume that a relatively stable group of pilots, flight-test personnel, maintainers, range personnel, technical specialists, and, where applicable, contractor support repeatedly participates in the program. A foreign intelligence service with longitudinal ALPR access would not need their names at the outset. It could begin with vehicles whose appearances repeatedly coincide with publicly identifiable test periods, then use recurring co-occurrence and timing to separate a probable core test team from Eglin's much larger workforce. Registration information, commercial identity records, public professional histories, and previously breached datasets could then convert those recurring vehicles into a probable roster of individuals, employers, and households.

Once that baseline existed, changes in the group's collective movements could disclose more than identity. A sustained period of unusual attendance by the same pilots and technical personnel, combined with new maintenance, contractor, range-support, or program-office activity, could suggest that the program was approaching a significant sensor, weapons, austere-operations, or operational-evaluation event. If part of the group later disappeared from its Eglin routine and reappeared in association with another test or operational organization, an analyst could infer a transition in the program without obtaining a test report or penetrating a classified network.

The movement history would also create a prioritized collection list. Pilots, flight-test personnel, maintainers, sensor specialists, and program personnel may possess knowledge of aircraft limitations, unresolved failures, sensor performance, maintenance burden, weapons integration, test results, or fielding timelines. Once their identities and residences were inferred, they could be selected for tailored cyber collection, elicitation, recruitment, coercion, device theft, or surveillance away from the installation. The vulnerability would not arise because the aircraft's technical data were stored in the ALPR system. It would arise because repeated movement could identify the small community most likely to possess those data.

A direct historical precedent is **Operation Anarchist**. Reporting based on documents disclosed by Edward Snowden described a joint U.S.-British intelligence program that intercepted electronic feeds, including video, from Israeli military drones and fighter aircraft over many years. The reported collection helped intelligence personnel observe Israeli military operations and monitor possible strike

preparations [E109]. The collection medium was different, but the intelligence objective was closely related: exploit external technical and behavioral signatures surrounding a sensitive aviation capability to determine what it could do, when it was active, and what operation it might be preparing to support.

The present study does not show that any OA-1K participant was tracked. Under the V7 modeled estimate conditional H0 policy, the twenty-mile weighted unobserved rate is 3.4%; the separate robust-lattice rate is 3.4%. This modeled result does not identify a test team or empirical read; it illustrates why repeated commuting by a stable specialized group could create a movement signature if historical reads and reliable identity enrichment became available.

Scenario 2: Detecting the Deployment and Return of a 7th Special Forces Group Element

The present Gate 1 and Gate 2 model does not measure routes to Camp Bull Simons and therefore does not produce a unit-specific result for the 7th Special Forces Group. The following is a reservation-wide threat illustration applying the same surveillance mechanism to a publicly documented Eglin tenant.

The 7th Special Forces Group's stated mission is to organize, equip, train, validate, and prepare forces for worldwide special operations, and its published regional responsibility includes Latin America, the Caribbean, adjacent waters, and associated territories [E107]. Official Army reporting places the group at Camp Bull Simons on Eglin Air Force Base [E108].

Assume that a hostile service obtains historical ALPR records from the civilian road network serving that cantonment and gradually identifies a recurring cluster associated with a small operational element and its support personnel. The service may not initially know which occupants are operators, communications specialists, medics, intelligence personnel, logisticians, or command staff. Repetition supplies that distinction. Vehicles that regularly appear during the same periods, exhibit recurring associations, or disappear together can be separated from the larger commuting population and linked through external records to probable identities and residences.

The most valuable signal may be coordinated absence. A preparatory period of changed activity among command, communications, logistics, and support personnel, followed by the simultaneous disappearance of the probable operational cluster, could indicate deployment. Because the group's regional responsibility is publicly known, the timing could be compared with political crises, diplomatic travel, exercises, hostage incidents, security-assistance activity, or other developments in the region. The adversary might not learn the precise destination or mission, but it could narrow the likely theater, estimate the departure date, identify at least some participating personnel, and recognize their eventual return.

That warning could have operational consequences. A government, proxy force, criminal organization, or armed group in the suspected area could increase security, change communications practices, relocate a potential target, alter travel, or initiate counterintelligence collection. The reappearance of the

same vehicle cluster days or weeks later could provide an approximate mission-completion date that could be compared with otherwise unattributed overseas events. Historical observations could also reveal probable homes, secondary household vehicles, family routines, and deployment-related absences, extending the exposure from the operational element to its households.

This threat model closely resembles a documented Russian intelligence campaign. In May 2025, the United Kingdom and allied governments attributed to Russian GRU Unit 26165 a cyber campaign that targeted organizations involved in moving assistance to Ukraine. The public advisory states that the unit also targeted internet-connected cameras at Ukrainian border crossings and near military installations to monitor and track aid shipments [E110]. The campaign demonstrates that a foreign military intelligence service will compromise distributed civilian camera infrastructure specifically to learn the timing and movement of military activity without first penetrating the military organization's classified network.

The direct relationship to Eglin is the intelligence value of the movement signature itself. In the GRU campaign, cameras did not need to reveal the contents of every shipment or the orders directing it. Timing, route, recurrence, and association were sufficient to support military intelligence. Applied to Camp Bull Simons, the comparable risk is that a recurring cluster of privately owned vehicles could become an indicator of the availability, departure, and return of a special-operations capability.

Combined Significance

The two scenarios represent different categories of national-security loss. The OA-1K scenario is a research, development, and acquisition-intelligence risk: movement records could help identify the personnel and support network behind a sensitive aviation program and reveal changes consistent with test milestones or operational transition. The 7th Special Forces Group scenario is an operational-warning risk: movement records could help identify a probable team, detect its coordinated absence, narrow the timing and regional context of a deployment, and expose its members and households.

In both cases, the decisive intelligence would emerge from aggregation rather than from a single plate read. Unclassified observations of ordinary travel could become an identifying signature, an organizational map, and an operational indicator when retained over time and combined with external identity data. A top-secret clearance would not be required if unclassified movement records could be assembled into a top-secret conclusion.

Why This Research Was Conducted

I conducted this assessment after four separate disclosures revealed failures across credentials, development assets, environment boundaries, and a data-fusion application. The sequence matters. A public development artifact contained an active ArcGIS credential, and other development bundles exposed application structure before the proper access boundary. A Planner/Beefeater path then issued

production-scope mapping credentials before login, while FlockNova bundles exposed the structure of a broader fusion and search environment [L2, L4, L5, L8, L37]. None of those facts alone proves universal backend access. Together they justified examining what sensitive geospatial information became available and what defensive questions that information could answer.

The production ArcGIS export captured on December 14, 2025 contains **a total of 335,701 records** spanning multiple device types and statuses; it is not a count of simultaneously active cameras. The status fields record 214,073 `inService`, 83,427 `inPlanning`, 38,190 decommissioned, and 11 unknown records. The study loads detection-eligible `inService` and `inPlanning` records from the shared source frame and counts both toward the primary route-exposure classification: because the December 2025 snapshot is applied to this August 2026 study, a planned device is treated as operational roughly eight months later, and the conservative `inService`-only floor is preserved in the artifacts. The separate `active` integer is not the study filter [L14, L15].

Repository evidence also shows why location data cannot be evaluated as a camera-count problem alone. Exposed application materials model plate and vehicle search, camera selection, hit history, alerts, people-search paths, map layers, CAD and AVL concepts, Raven/audio sensors, device access, and identity-adjacent fusion permissions [L4, L11-L13, L35]. Flock's patent describes a dynamic surveillance and object-query architecture, including video-content analysis and attribute-oriented search, but a patent describes claimed architecture and possible functions rather than proving deployment of every patented capability [E37]. The report therefore separates observed code and export fields from product descriptions and from hypothetical intelligence use.

The force-protection concern arises because military and sensitive-facility personnel routinely use civilian roads outside a protected perimeter. National evidence indicates that many service members live in local communities, and the military housing system uses civilian markets when government quarters are not provided [E44-E46]. Those national facts do not reveal where a person assigned to Eglin AFB lives. They establish only that off-installation movement is a legitimate research surface rather than a hypothetical edge case.

The policy concern is broader than this one installation. Longitudinal location information can expose associations and patterns that isolated observations do not. Supreme Court decisions concerning long-term GPS tracking and historical location records provide relevant Fourth Amendment context, while not deciding the legality of this specific vendor, dataset, or study [E20, E21]. The constitutional and privacy implications therefore belong in policy and legal review, not in unsupported declarations that every collection or search is unlawful.

My analytical judgment is that commercial growth and quarter-to-quarter profit must not displace United States national-security, force-protection, constitutional, and public-accountability obligations. That is a normative conclusion, not evidence that profit caused a particular breach or that a specific

customer misused data. Its factual premises are the documented vulnerability chain, the status-precise deployment inventory, the exposed search and fusion models, and the concentration of ordinary travel around sensitive facilities [L2, L4, L14, L15, L40].

Four Reported Vulnerabilities

Finding	Observed condition	Evidence boundary	Disclosure and remediation status	Source(s)
1	An active ArcGIS Default API key was hardcoded in a public development/demo asset and repeated key material was found across development assets.	The validation establishes key scope and private item grants; it does not prove that every granted item was read or altered by another party.	Reported 2025-06-11; remediation reported 2025-07-01.	L2, L5, L8, L20
2	FlockSafety development application and module-federation bundles were served before the correct authentication boundary.	The bundles expose application logic, routes, models, and permission concepts; frontend visibility does not prove anonymous access to every backend or production record.	Reported 2025-11-13 with follow-ups on 2025-11-14 and 2025-11-19; no closure or remediation detail appears in the disclosure record.	L2, L5, L11-L13
3	Planner/Beefeater endpoints issued ArcGIS and Google mapping credentials before login, including a production-scope path used to obtain the analyzed export.	Wire records prove anonymous HTTP 200 token responses and establish provenance; they do not prove every downstream service permitted every operation.	Reported 2025-11-13 with follow-ups on 2025-11-14 and 2025-11-19; no closure or remediation detail appears in the disclosure record.	L2, L14, L15, L37

Finding	Observed condition	Evidence boundary	Disclosure and remediation status	Source(s)
4	FlockNova application bundles were served before the correct access boundary and revealed search, pivot, fusion, and client-side permission assumptions.	The exposed code establishes application structure and data-source concepts; it does not establish that every modeled backend endpoint lacked authorization or that every modeled dataset was populated.	Reported 2025-12-05; no reply or remediation detail appears in the disclosure record.	L2, L4, L35

The findings are distinct but composable. Findings 2 and 4 exposed the vocabulary and architecture of search, alerting, mapping, and fusion workflows. Findings 1 and 3 exposed two different credential failures: a static production-scoped ArcGIS key and a pre-login credential-issuance path. Finding 3 supplied the provenance for the production map-point export used here. The combination supports a conclusion about systemic credential and environment-boundary weakness during the research period, while remaining narrower than a claim of universal platform compromise [L2, L8, L37].

The disclosure record also cannot establish a negative. Responsible reporting and a known remediation date for Finding 1 do not prove that no other person accessed the exposed surfaces, just as the absence of a returned closure notice for Findings 2 through 4 does not prove that they remain exploitable today. The reports preserve the observed condition, collection date, and known response status so that legal and technical reviewers can distinguish evidence from present-tense assumptions.

V7 Result Record

Modeled route-coverage estimate [L41].

Field	5-mile near-base	20-mile primary
Result label	V7 modeled estimate	V7 modeled estimate
Publication status	Modeled estimate (2 caveats)	Modeled estimate (2 caveats)
Headline channel	robust_lattice	robust_lattice
Primary H0 U/C/P/R	17.9%/78.7%/0.0%/3.4%	3.4%/94.8%/0.0%/1.8%
Robust H0/H1/H2 U/C/P/R	17.8%/77.4%/0.1%/4.7%	3.4%/93.9%/0.0%/2.7%
H0 validation	single-reviewer check	single-reviewer check

The complete modeled result record for both scopes - all sensitivity intervals, gate/direction/range sweeps, camera-cluster influence, modeling caveats, seeds, and SHA-256 hashes - is in the V7 Modeled Result Record under Evidence and Reproducibility below.

20-mile minus 5-mile weighted unobserved-rate difference: primary conditional H0 **-14.5** percentage points; separate robust H0/H1/H2 lattice **-14.4** percentage points. These channels answer different questions and are not averaged. [L41]

Reachability Results

Five-Mile Near-Base Scope

Publication state: Modeled estimate (2 caveats).

The 5-mile primary H0 channel contains 1,000 draws on the full in-frame sampled denominator: 179 unobserved (17.9%), 787 confirmed exposure (78.7%), 0 possible exposure (0.0%), 34 unresolved model (3.4%). The separate robust H0/H1/H2 lattice reports 178 unobserved (17.8%), 774 confirmed exposure (77.4%), 1 possible exposure (0.1%), 47 unresolved model (4.7%). Neither channel drops or renormalizes unresolved-model weight.

H0 uncertainty intervals: direction-H0 17.9% to 21.3%; fixed-H0-gate access 17.8% to 22.6%; joint 17.8% to 22.6%; spatial/grade-H0 17.9% to 21.2%. These are distinct sensitivity results and are not averaged. Candidate-frame accounting:

```
{
  "all_saved_gates_evaluated": true,
  "certificate_artifact_path": "frame_classification.json",
  "certificate_artifact_sha256": "84cd92c57846f21b75399b5a08c97d2af4dcb9d388d5a13f34214e39f4bd3f72",
  "classifier_contract": "h0-all-saved-gates-directed-per-leg-frame-v1",
  "classifier_version": 1,
  "closure": {
    "count_matches_source": true,
    "weight_matches_source": true
  },
  "count_by_status": {
    "frame_unknown": 0,
    "near": 2006,
    "outer": 5579,
    "proven_out_of_frame": 4861
  },
  "per_leg_scope_rule": "outbound_and_return_each_lte_declared_scope_radius",
  "source_count": 12446,
  "source_weight": 101757.99999999999,
  "weight_by_status": {
    "frame_unknown": 0.0,
    "near": 12607.00000000000002,
    "outer": 54045.25,
    "proven_out_of_frame": 35105.749999999985
  },
  "weight_semantics": "pre_sampling_occupied_housing_candidate_weight"
}. Sampled-frame accounting:
{
  "count_by_status": {
    "artifact_error": 0,
    "frame_unknown": 0,
    "in_frame": 1000,
    "proven_out_of_frame": 0
  },
  "rate_by_status": {
    "artifact_error": 0.0,
    "frame_unknown": 0.0,
    "in_frame": 100.0,
    "proven_out_of_frame": 0.0
  },
  "source_count": 1000,
  "source_weight": 12606.999999999973,
  "weight_by_status": {
    "artifact_error": 0.0,
    "frame_unknown": 0.0,
    "in_frame": 12606.999999999973,
    "proven_out_of_frame": 0.0
  }
}.
```

Modeling caveats: 1. corridor routing is a single-reviewer accuracy check (~89.5%; see the report's Appendix O)2. primary H0 unresolved weight is 3.400%**QA and artifact warnings:** None [L41]

Twenty-Mile Primary Scope

Publication state: Modeled estimate (2 caveats).

The 20-mile primary H0 channel contains 2,000 draws on the full in-frame sampled denominator: 179 unobserved (3.4%), 1,773 confirmed exposure (94.8%), 0 possible exposure (0.0%), 48 unresolved model (1.8%). The separate robust H0/H1/H2 lattice reports 178 unobserved (3.4%), 1,752 confirmed exposure (93.9%), 1 possible exposure (0.0%), 69 unresolved model (2.7%). Neither channel drops or renormalizes unresolved-model weight.

H0 uncertainty intervals: direction-H0 3.4% to 5.2%; fixed-H0-gate access 3.4% to 6.1%; joint 3.4% to 6.1%; spatial/grade-H0 3.4% to 5.0%. These are distinct sensitivity results and are not averaged.

Candidate-frame accounting: {"all_saved_gates_evaluated": true, "certificate_artifact_path": "frame_classification.json", "certificate_artifact_sha256": "84cd92c57846f21b75399b5a08c97d2af4dcb9d388d5a13f34214e39f4bd3f72", "classifier_contract": "h0-all-saved-gates-directed-per-leg-frame-v1", "classifier_version": 1, "closure": {"count_matches_source": true, "weight_matches_source": true}, "count_by_status": {"frame_unknown": 0, "near": 2006, "outer": 5579, "proven_out_of_frame": 4861}, "per_leg_scope_rule": "outbound_and_return_each_lte_declared_scope_radius", "source_count": 12446, "source_weight": 101757.99999999999, "weight_by_status": {"frame_unknown": 0.0, "near": 12607.000000000002, "outer": 54045.25, "proven_out_of_frame": 35105.749999999985}, "weight_semantics": "pre_sampling_occupied_housing_candidate_weight"}. Sampled-frame accounting: {"count_by_status": {"artifact_error": 0, "frame_unknown": 0, "in_frame": 2000, "proven_out_of_frame": 0}, "rate_by_status": {"artifact_error": 0.0, "frame_unknown": 0.0, "in_frame": 100.0, "proven_out_of_frame": 0.0}, "source_count": 2000, "source_weight": 66652.25000000132, "weight_by_status": {"artifact_error": 0.0, "frame_unknown": 0.0, "in_frame": 66652.25000000132, "proven_out_of_frame": 0.0}}.

Modeling caveats: 1. corridor routing is a single-reviewer accuracy check (~89.5%; see the report's Appendix O)2. primary H0 unresolved weight is 1.778%**QA and artifact warnings:** None [L41]

Relationship Between the Two Scopes

20-mile minus 5-mile weighted unobserved-rate difference: primary conditional H0 **-14.5** percentage points; separate robust H0/H1/H2 lattice **-14.4** percentage points. These channels answer different questions and are not averaged. Each directed outbound and return leg must independently satisfy its declared 5/20-road-mile scope; the total round trip may approach 10/40 miles. An origin with no unchanged saved gate qualifying under H0 is outside that scope before sampling [L41].

Methodology

Estimand and Synthetic Origins

The V7 primary estimand is the occupied-housing-weighted distribution across unobserved, confirmed exposure, possible exposure, and unresolved model under one predeclared, camera-blind H0 access-and-route policy. H0 defines the pinned origin, eligible unchanged saved gates, 5/20-road-mile frame, final per-leg scope, and primary conditional result. Every in-frame sampled weight remains in the four-class denominator; proven out-of-frame origins are excluded before sampling, while frame-unknown, unresolved-model, and artifact-error states remain explicit.

Each directed outbound and return leg must be no more than the declared radius. A qualifying round trip can therefore approach 10 miles in the 5-mile scope or 40 miles in the 20-mile scope. This is not a total-round-trip cap of 5 or 20 miles.

H1/H2 remain identity-keyed alternative access policies used only for the separate robustness lattice and fixed-H0-gate access sensitivity. H1/H2 cannot rescue a failed H0, set the primary status, change H0 frame membership, or contribute cameras to the H0 result. The two channels are co-located and never averaged [L41].

Reviewed 24/7 Gates

The paired study used Gate 1 and Gate 2 as the reviewed gate set. Only gates treated during setup as continuously open to authorized traffic are eligible. A part-time, visitor-only, commercial-only, or schedule-limited gate would create a modeled route that disappears outside its operating window, so including it as continuously available would overstate practical access. The gate decision concerns availability, not secrecy; coordinates and identifiers remain in the unredacted annexes.

The same gate set was used at both radii. The saved study state also contained 0 analyst-defined road blocks. Gates and blocks are inputs rather than outputs. A high or low unobserved rate does not validate the gate review, so an installation reviewer should read the exact saved identifiers and artifact warnings when judging whether the modeled access assumptions match local practice.

Cameras, Roads, and Routing

The V7 route and gate policy receives no camera coordinates, encounter results, or camera-derived costs. It uses the frozen routing and inventory assumptions bound into the completed cohort (`valhalla-3.6.3-auto-frozen-osm-camera-blind-directed-overlay-v6`). Outbound and return routes are legal directed requests and are evaluated independently against the declared per-leg scope.

Camera encounters remain geometry, corridor, bearing, lifecycle-status, and capture-model inferences rather than observed plate reads. The H0 point channel retains direction and spatial/grade sensitivity separately. Camera influence is computed by physical camera cluster so colocated compute/support records are not counted as independent roadside sensors. Planned-device and in-service-only status variants remain sensitivity evidence rather than claims of confirmed real-world operation [L41].

Why Five and Twenty Miles

DoD Manual 4165.63 permits housing-market boundaries based on a twenty-mile or one-hour peak-traffic commute, with military and public information and installation-command input supporting local adjustment [E49]. The study predeclared the distance limb as a uniform, transparent approximation of the broader off-installation housing and commuting area. It does not assert that most personnel at Eglin AFB live exactly twenty miles away, and it does not model one hour of peak traffic.

Five miles isolates the immediate area where travel converges toward a limited gate set. Twenty miles adds the broader housing-market stratum while retaining every near-base draw unchanged. Reporting both shows whether corridor concentration near the facility differs from the surrounding occupied-housing geography without changing the near-base sample.

Limitations and Non-Claims

This is a model over dated deployment, Census, and road snapshots. Occupied housing is a residential-distribution proxy, not an installation workforce roster; it does not weight origins by military assignment, employer, rank, duty status, shift, or measured traffic. National off-base housing evidence supports the scope choice but cannot identify where personnel assigned to Eglin AFB live [E44-E46].

Camera location and status fields can be incomplete, stale, planned, duplicated, moved, or differently interpreted. OSM roads and address points can omit valid travel or include obsolete topology. Gate availability and cantonment geometry depend on analyst review. The route engine models corridor blocking, accepted alternatives, and a geometric field-of-view capture; it does not model OCR probability, optical obscuration, weather, plate condition, device uptime, data retention, customer sharing, legal process, or whether a backend user queried a record.

A V7 unobserved H0 classification is a conditional modeled-policy result: under the frozen H0 access, gate, routing, inventory-status, and capture rules, the legal directed round trip had no qualifying modeled encounter. It is not a share of people, drivers, commuters, households, actual trips, or empirical camera reads. The separate robust lattice and access, gate-choice, direction, spatial/grade, range, deployment-status, sampling, and camera-cluster sensitivities must remain visible qualifications. Source omissions, device uptime, weather, plate visibility, temporary road conditions, and camera movement can change real-world collection.

Evidence and Reproducibility

The V7 drafting packet was built from the complete validated cohort for `eglin_afb`. It binds cohort `reachability-v7-audit-92bd2e6a45c3a7c6`, pair `eglin_afb-51adfc2c9b93d2e1`, seed `1949606558`, index SHA-256 `3d0755cb6fcc7dd165c6b9dd53ade8bfe5402773231904ea3807d1f17dc3b96b`, five-mile summary SHA-256 `33ca0b11147d0523fe788624c398e8d694d000808d995422926230396e94026c`, and twenty-mile summary SHA-256 `1e16babf624a66e4ace6f01b0154b2f8de3aa97c79971f84ad1ed02f5e95ede7`. [L41].

Both scopes retain the primary H0 and robust-lattice partitions, full frame accounting, per-policy outcomes and failures, directed route geometry, modeled camera encounters, split uncertainty intervals, gate-choice sensitivity, physical-camera-cluster influence, frozen source snapshot, and independent QA. All QA flags and warnings remain unsuppressed in the hash-bound V7 snapshot [L41].

The narrative is subordinate to those structured artifacts. If a sentence, table cell, or later export conflicts with a canonical summary or origin-level record, the validated structured record controls and the narrative must be corrected. Joshua Michael independently reviews each material claim, citation, inference, and numerical value as the accountable author.

References

ID	Source and use in this report
E20	U.S. Supreme Court, <i>Carpenter v. United States</i> opinion, https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf - Digital location privacy policy/legal context.
E21	Library of Congress, <i>United States v. Jones</i> , 565 U.S. 400, https://www.loc.gov/item/usrep565400/ - GPS tracking/location surveillance policy/legal context.
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 and use in this report
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 function, including facial recognition. Accessed 2026-07-13.
E44	U.S. Government Accountability Office, <i>Military Housing: DOD Should Address Critical Supply Shortages</i> (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, <i>Military Housing</i> (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.
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.

ID	Source and use in this report
E49	U.S. Department of Defense, DoD Manual 4165.63, <i>DoD Housing Management</i>, 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.
E106	U.S. Air Force, "Skyraider II testing continues at Eglin AFB," July 30, 2025, https://www.af.mil/News/Article-Display/Article/4259407/skyraider-ii-testing-continues-at-eglin-afb/ - Official account of 96th Test Wing and U.S. Special Operations Command developmental testing of the OA-1K at Eglin, including its special-operations mission sets and publicly described test objectives. Accessed 2026-08-08.
E107	U.S. Air Force, Eglin AFB, "7th Special Forces Group (Airborne)," https://www.eglin.af.mil/About-Us/Fact-Sheets/Display/Article/810637/7th-special-forces-group-a/ - Official mission and regional-area-of-responsibility description for the 7th Special Forces Group. Accessed 2026-08-08.
E108	U.S. Army, "7th Special Forces Group (Airborne) opens Red Empire Week with ceremony, capabilities exercise," June 8, 2026, https://www.army.mil/article/293105/7th_special_forces_group_airborne_opens_red_empire_week_with_ceremony_capabilities_exercise - Official Army reporting placing the 7th Special Forces Group at Camp Bull Simons on Eglin Air Force Base. Accessed 2026-08-08.
E109	<i>The Guardian</i>, "Snowden files reveal US and UK spied on feeds from Israeli drones and jets," January 29, 2016, https://www.theguardian.com/world/2016/jan/29/snowden-files-us-uk-spied-feeds-israeli-drones-jets - Reporting on Operation Anarchist, used as a precedent for intelligence collection against external video and technical signatures surrounding a sensitive aviation capability. Accessed 2026-08-08.

ID	Source and use in this report
E110	United Kingdom National Cyber Security Centre, "UK and allies expose Russian intelligence campaign targeting western logistics and technology organisations," May 21, 2025, https://www.ncsc.gov.uk/news/uk-partners-expose-russian-intelligence-campaign - Joint-government attribution stating that GRU Unit 26165 targeted internet-connected cameras at Ukrainian border crossings and near military installations to monitor and track aid shipments. Accessed 2026-08-08.
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.
L8	Raw Evidence/FlockSafety/ flock_hardcoded_api_check.json - Primary validation artifact for key scope and 50 item grants.
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 and use in this report
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.
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.
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 and use in this report
L40	Superseded earlier 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 an earlier 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	Complete V7 snapshot and staged cohort <code>reachability-v7-audit-92bd2e6a45c3a7c6</code> (index SHA-256 <code>3d0755cb6fcc7dd165c6b9dd53ade8bfe5402773231904ea3807d1f17dc3b96b</code>); primary conditional H0 and robust H0/H1/H2 results, methodology, frame accounting, split uncertainty, QA flags and warnings, hashes, and annexes. Canonical source: the hash-bound V7 snapshot at <code>../Supporting Tools and Docs/project_support/planning_and_qa/reachability_v7_audit_development_snapshot.json</code> .

Per-site records

The V7 result for this installation - primary conditional H0 and robust H0/H1/H2 outcomes, frame accounting, uncertainty intervals, QA flags, seeds, and SHA-256 summary bindings - is recorded in the hash-bound V7 snapshot [L41]. The large per-origin staging artifacts (route geometry, frame classification, review packets) are not shipped in this package; the full records are retained by the researcher offline for authorized review [L40].