

MacDill AFB

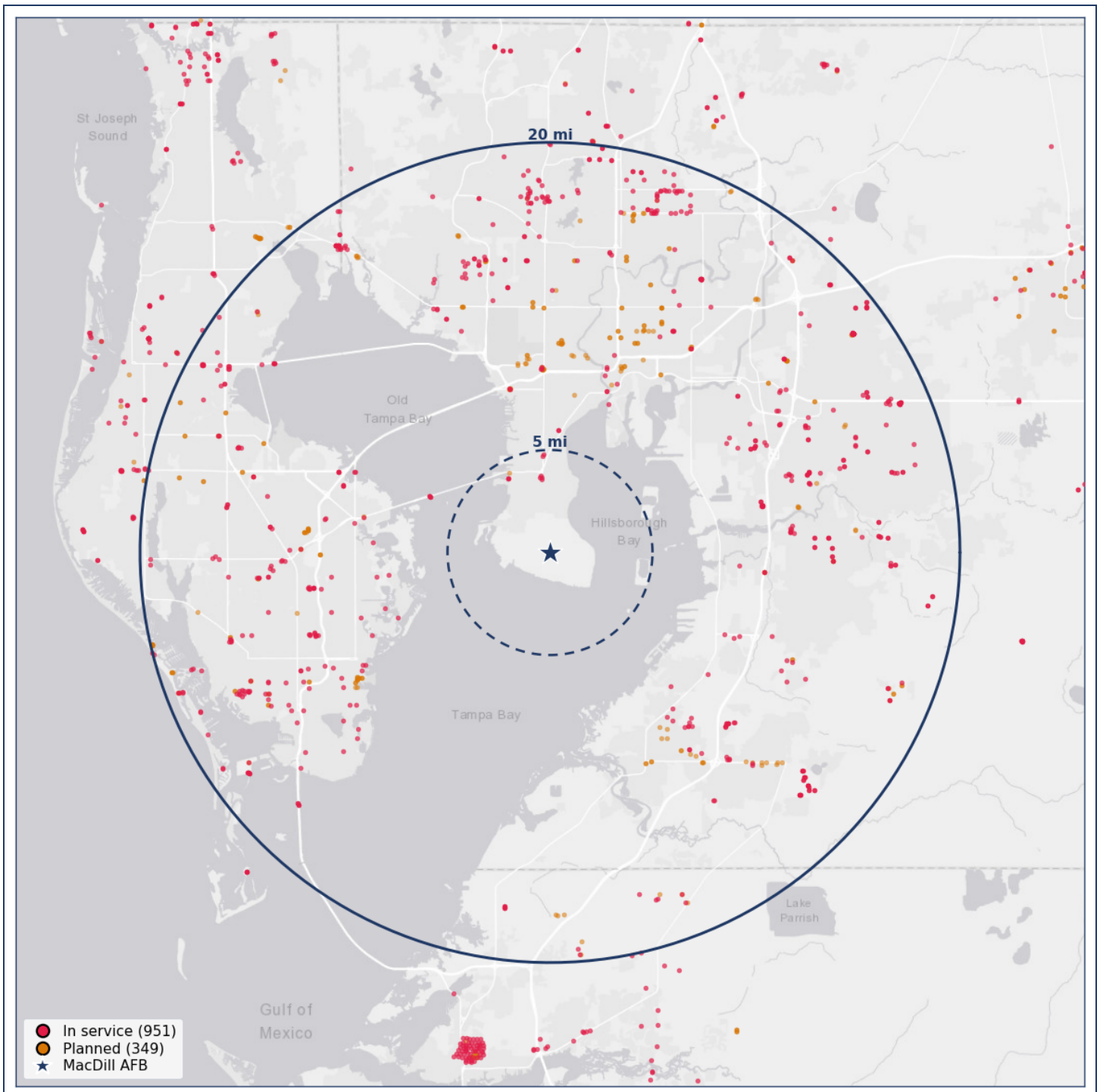
National Security Exposure Assessment

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

MacDill Air Force Base in Tampa is home to U.S. Central Command and U.S. Special Operations Command — two combatant-command headquarters, plus coalition staff from more than forty countries. An unusual gathering of CENTCOM, SOCOM, coalition, and communications traffic could mean one or both headquarters had just gone into crisis response.

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 54.9% of those modeled trips pass a camera. Another 12.4% might pass one, 27.1% avoid them, and 5.7% could not be determined. Closer in, at 5 miles, most trips (94.9%) avoid cameras; the dense coverage is farther out. This is a model of routes, not proof that anyone was watched.

HEADLINE RESULT · MODELED TRIPS TO A GATE

20 MILES OUT



- 54.9%** **Passes a camera**
A confirmed camera sits on every plausible road to a gate.
- 12.4%** **Might pass**
A camera is nearby, but facing could not be confirmed. The file's rotationAngle is a housing-orientation field, not travel direction, so unnamed or poorly oriented cameras are not counted as hits.
- 27.1%** **Avoids all cameras**
No confirmed camera on any plausible road.
- 5.7%** **Couldn't determine**
The model could not finish a legal round trip for these draws.

5 MILES OUT



1.0% Passes **1.1%** Might pass **94.9%** Avoids **3.0%** Couldn't determine

Installation Context

MacDill Air Force Base is a uniquely concentrated command site. Its official fact sheet identifies U.S. Central Command, U.S. Special Operations Command, the Joint Communications Support Element, two flying wings, and dozens of mission partners on the installation. The base also hosts personnel from more than forty nations and a large military, civilian, and contractor workforce [E136]. Those public facts establish that ordinary gate traffic can mix combatant-command staff, special-operations personnel, coalition representatives, deployable communications specialists, air-refueling personnel, and support organizations without revealing any individual's role from a single vehicle observation.

JCSE creates a second, distinct risk. U.S. Transportation Command describes the element as immediately deployable to provide enroute, early-entry, and scalable command, control, communications, and computer support to geographic combatant commands, Special Operations Command, and other agencies. Official MacDill reporting also describes JCSE teams deploying ahead of larger exercises to establish the communications architecture on which following forces depend [E137, E138]. A recurring vehicle cluster associated with that small deployable community would therefore be more operationally informative than generic base traffic.

The study uses these public mission facts only to identify realistic consequences if Tier B historical observations and Tier C identity or organizational enrichment became available. It did not identify a MacDill employee, command, household, plate, or mission. The route model covers the reviewed MacDill gate set; it does not establish where any command's personnel live or which gate any real person uses.

Installation-Specific Intelligence Scenarios

The quantitative study establishes Tier A coverage and deployment information: where included devices were recorded and how synthetic occupied-housing-weighted routes intersected their modeled observation corridors. The scenarios below require additional data not obtained in the research, including historical time-stamped plate observations and reliable links between vehicles and people, commands, organizations, or households.

Scenario 1: Detecting a CENTCOM or USSOCOM Crisis Activation and Senior-Leadership Convergence

Assume that a foreign intelligence service obtains a sufficiently long history of vehicle observations around MacDill and gradually associates recurring plates with probable command staff, coalition liaison elements, communications personnel, security staff, and senior leaders. The service would not need a complete roster. Repetition could distinguish vehicles that appear during ordinary business hours from those that recur during exercises, after-hours briefings, foreign-partner visits, or public crises.

The highest-value signal would be an abnormal convergence across normally distinct communities. Suppose vehicles associated with senior staff, operations and intelligence personnel, communications support, coalition representatives, and security personnel begin arriving outside their established patterns and remain through the night or weekend. A single vehicle would prove little. A sustained, multi-day activation involving several correlated clusters could indicate that a combatant-command headquarters was responding to an emerging contingency rather than conducting routine business.

The adversary might not know the command's decision, target, or intended operation. It could nevertheless learn that a headquarters response had begun, estimate when it accelerated, identify which foreign partners or mission organizations appeared involved, and correlate the movement change with diplomatic statements, military air activity, naval movements, cyber events, or developments inside the CENTCOM area of responsibility. That early warning could support intensified collection, deception, force dispersal, or counterintelligence activity before the United States publicly acknowledged the response.

The physical-security consequence is equally serious. Once vehicles are associated with senior leaders or protective personnel, historical observations can expose probable residences, family vehicles, recurring off-base meetings, and locations where official security is reduced. The intelligence value is therefore not limited to organizational tempo; it can become a targeting and coercion file on the people directing the response.

A direct historical precedent was reported by the Associated Press in 2026. According to AP sources, Israel exploited Iran's street- and traffic-camera infrastructure to build movement and relationship intelligence on senior Iranian officials and their protective personnel, including addresses, routes, parking locations, and occasions when multiple officials were present together [E131]. The report is not evidence of compromise at MacDill. It demonstrates that a state will convert civilian surveillance infrastructure into a leadership-location and convergence-detection system when the target is strategically important.

The present MacDill study does not show that a command activation occurred or that any leader was identified. It demonstrates modeled route exposure around a site where two combatant-command headquarters and their supporting communities are publicly concentrated. The crisis inference would require Tier B history, Tier C enrichment, a defensible baseline, and independent corroboration.

Scenario 2: Identifying the Deployment of a JCSE Early-Entry Communications Package

JCSE's public mission makes coordinated absence unusually informative. Assume that an analyst identifies a stable cluster of vehicles associated with expeditionary communicators, network and satellite technicians, planners, equipment specialists, and a small support element. Over time, recurring co-arrival, exercise participation, and disappearance patterns could distinguish that cluster from MacDill's much larger workforce even if the analyst initially knew none of the occupants' names.

Before a deployment, the analyst might observe a short period of changed attendance, additional equipment or logistics support, and unusual overlap among technicians and planners. The core cluster could then disappear from ordinary MacDill movement at roughly the same time. Because JCSE is designed to deploy early and establish communications before larger headquarters or forces arrive, the disappearance could function as warning that the United States was preparing command-and-control support for an emerging operation.

The destination might remain unknown. Correlation with a regional crisis, military airlift activity, allied exercises, or public reporting could narrow the likely theater and supported command. The cluster's later reappearance could indicate mission completion, rotation, or return. Historical repetition would make the model stronger: after observing several exercises or acknowledged deployments, the adversary could learn which preparatory sequence tends to precede a real early-entry mission.

The personnel consequences extend beyond operational warning. Identifying a small cadre of highly skilled communications specialists creates a prioritized target list for cyber intrusion, credential theft, social engineering, recruitment, device compromise, or surveillance of households during deployment-related absences. The classified communications themselves may remain secure while the people and timing required to establish them become visible.

This scenario closely resembles a documented Russian intelligence campaign. In May 2025, the United Kingdom, United States, and partner governments attributed to GRU Unit 26165 a campaign that targeted logistics and technology organizations involved in assistance to Ukraine and internet-connected cameras at border crossings and near military installations to monitor and track aid shipments [E110]. The cameras did not need access to military orders. Their value came from revealing the physical movement and timing of an enabling capability.

The MacDill route study did not identify JCSE vehicles or observe a deployment. It establishes the modeled surveillance surface around the installation. The JCSE inference would require historical records, reliable organizational attribution, and corroboration beyond anything collected in this assessment.

Combined Significance

The two scenarios expose different levels of operational risk. The combatant-command scenario concerns strategic warning and leadership protection: movement changes could reveal that a headquarters has activated and who is participating. The JCSE scenario concerns operational enablement: a small communications package may deploy before the larger force it supports. Together, they show how unclassified roadway observations could provide both the warning that a U.S. response is beginning and the identity of the people building its first command-and-control link.

Primary Reachability Findings

Modeled route-coverage estimate, reported for both scopes with its uncertainty ranges.

Field	5-mile near-base	20-mile primary
Result label	V7 modeled estimate	V7 modeled estimate
Publication status	Modeled estimate (2 caveats)	Modeled estimate (4 caveats)
Headline channel	robust_lattice	robust_lattice
Primary H0 U/C/P/R	95.8%/1.6%/0.9%/1.7%	28.5%/56.7%/12.3%/2.5%
Robust H0/H1/H2 U/C/P/R	94.9%/1.0%/1.1%/3.0%	27.1%/54.9%/12.4%/5.7%
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 **-67.3** percentage points; separate robust H0/H1/H2 lattice **-67.8** percentage points. These channels answer different questions and are not averaged. [L41]

Legislative Significance

MacDill demonstrates why ALPR governance should account for the mission of the location being observed, not merely the sensitivity of an individual plate read. A network that records traffic around two combatant-command headquarters and a rapidly deployable communications element can create strategic-warning and leadership-protection risks even when each observation was lawfully collected for an unrelated public-safety purpose.

Legislators should consider heightened cybersecurity, short default retention, restricted nationwide sharing, particularized historical-search requirements, immutable auditing, and rapid breach notification for ALPR systems whose coverage encompasses combatant-command headquarters and

other designated national-security sites. The designation process should be developed with the Department of Defense and should not publicly identify camera gaps, preferred approaches, or routes that would aid evasion.

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.

Methodology

Research and Data Basis

This assessment follows four separate disclosures involving credentials, development assets, environment boundaries, and a data-fusion application. A public development artifact contained an active ArcGIS credential; other development bundles exposed application structure before the expected access boundary; a Planner/Beefeater path issued production-scope mapping credentials before login; and FlockNova bundles exposed the structure of a broader fusion and search environment [L2, L4, L5, L8, L37]. None of those findings alone proves universal backend access. Together, they justified examining what sensitive geospatial information became available and what defensive questions it could support.

The production ArcGIS export captured on December 14, 2025 contains 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 route study loads detection-eligible `inService` and `inPlanning` records and preserves a separate `inService`-only floor. The `active` integer is not the study filter [L14, L15].

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, but a patent describes claimed architecture rather than proving deployment of each patented capability [E37]. The report therefore separates observed code and export fields from product descriptions and hypothetical intelligence use.

The force-protection concern arises because personnel assigned to MacDill AFB routinely use civilian roads outside a protected perimeter. National evidence indicates that many service members live in local communities and use civilian housing markets when government quarters are not provided [E44-E46]. Those national facts do not reveal where any person assigned to MacDill AFB lives; they establish only that off-installation movement is a legitimate research surface.

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 policy and legal context without deciding the legality of this vendor, dataset, or study [E20, E21]. The constitutional and privacy implications belong in legal and policy review, not in unsupported declarations that every collection or search is unlawful.

My analytical judgment is that commercial growth and procurement convenience must not displace United States national-security, counterintelligence, 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.

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 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 MacDill 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 MacDill 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 `macdill_afb`. It binds cohort `reachability-v7-audit-92bd2e6a45c3a7c6`, pair `macdill_afb-158713a0c1728242`, seed `2941548377`, index SHA-256 `3d0755cb6fcc7dd165c6b9dd53ade8bfe5402773231904ea3807d1f17dc3b96b`, five-mile summary SHA-256 `d53a19928964cb5950e3b55cd8b1b2e4adf4a6fc1ea052f15ae1383333d2b5dd`, and twenty-mile summary SHA-256 `97dcbf63a9418bd7f79baa5c188a4644a81d8cd736a8dbd8cdda0a62365f908d`. [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.

V7 Modeled 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 (4 caveats)
V7 cohort	reachability-v7-audit-92bd2e6a45c3a7c6	reachability-v7-audit-92bd2e6a45c3a7c6
Pair ID	macdill_afb-158713a0c1728242	macdill_afb-158713a0c1728242
Pair seed	2941548377	2941548377
Generated at	2026-08-12T07:15:38.126611+00:00	2026-08-12T07:15:38.126611+00:00
Summary SHA-256	d53a19928964cb5950e3b55cd8b1b2e4a df4a6fc1ea052f15ae1383333d2b5dd	97dcbf63a9418bd7f79baa5c188a4644a8 1d8cd736a8dbd8cdda0a62365f908d
Routing engine	valhalla-3.6.3-auto-frozen-osm-camera- blind-directed-overlay-v6	valhalla-3.6.3-auto-frozen-osm-camera- blind-directed-overlay-v6
Synthetic draws	1000	2000
Headline channel	robust_lattice	robust_lattice
Primary H0 U/C/P/R counts	958/16/9/17	1189/627/141/43
Primary H0 U/C/P/R	95.8%/1.6%/0.9%/1.7%	28.5%/56.7%/12.3%/2.5%
Robust H0/H1/H2 U/C/P/R counts	949/10/11/30	1165/602/144/89
Robust H0/H1/H2 U/C/P/R	94.9%/1.0%/1.1%/3.0%	27.1%/54.9%/12.4%/5.7%
Direction H0 interval	95.8% to 98.4%	28.5% to 43.3%
Fixed-gate access interval	94.9% to 98.8%	27.1% to 33.0%
Joint interval	94.9% to 99.0%	27.1% to 45.1%
Spatial H0 interval	95.8% to 97.2%	28.4% to 30.6%
Gate reselection diagnostic	fixed 95.7%; reselected 95.7%; absolute difference 0.0 pp	fixed 28.1%; reselected 28.1%; absolute difference 0.0 pp
H0 gate near-tie sensitivity	60s: 0.0% disagreement weight; 120s: 0.0% disagreement weight; 300s: 0.0% disagreement weight	60s: 0.0% disagreement weight; 120s: 0.0% disagreement weight; 300s: 0.0% disagreement weight

Field	5-mile near-base	20-mile primary
H0 range sensitivity U/C/P/R	75ft: 96.0%/1.6%/0.7%/1.7%; 150ft: 95.8%/1.6%/0.9%/1.7%; 250ft: 95.3%/1.6%/1.4%/1.7%	75ft: 29.7%/56.3%/11.4%/2.5%; 150ft: 28.5%/56.7%/12.3%/2.5%; 250ft: 26.7%/57.4%/13.3%/2.5%
H0 direction sensitivity U/C/P/R	25deg: 95.8%/1.6%/0.9%/1.7%; 30deg: 95.8%/1.6%/0.9%/1.7%; 35deg: 95.8%/1.6%/0.9%/1.7%; 40deg: 95.8%/1.6%/0.9%/1.7%; 45deg: 95.8%/1.6%/0.9%/1.7%; 60deg: 95.8%/1.6%/0.9%/1.7%	25deg: 29.6%/56.7%/11.2%/2.5%; 30deg: 28.6%/56.7%/12.2%/2.5%; 35deg: 28.5%/56.7%/12.3%/2.5%; 40deg: 28.5%/56.7%/12.3%/2.5%; 45deg: 28.5%/56.7%/12.3%/2.5%; 60deg: 28.1%/56.7%/12.7%/2.5%
Deployment-status sensitivity U/C/P/R	declared_policy: 95.8%/1.6%/0.9%/1.7%; in_service_only: 97.4%/0.0%/0.9%/1.7%	declared_policy: 28.5%/56.7%/12.3%/2.5%; in_service_only: 32.8%/40.1%/24.6%/2.5%
Physical-camera-cluster influence	maximum removal shift 1.6 pp; 0 material clusters	maximum removal shift 8.1 pp; 1 material cluster
H0 validation	single-reviewer check	single-reviewer check
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 1.700%	1. corridor routing is a single-reviewer accuracy check (~89.5%; see the report's Appendix O)2. primary H0 unresolved weight is 2.533%3. fixed-gate access-policy interval spans 5.936 pp4. one or more physical camera clusters exceed the influence materiality limit
QA and artifact warnings	None	None

20-mile minus 5-mile weighted unobserved-rate difference: primary conditional H0 **-67.3** percentage points; separate robust H0/H1/H2 lattice **-67.8** 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: 958 unobserved (95.8%), 16 confirmed exposure (1.6%), 9 possible exposure (0.9%), 17 unresolved model (1.7%). The separate robust H0/H1/H2 lattice reports 949 unobserved (94.9%), 10 confirmed exposure (1.0%), 11 possible exposure (1.1%), 30 unresolved model (3.0%). Neither channel drops or renormalizes unresolved-model weight.

H0 uncertainty intervals: direction-H0 95.8% to 98.4%; fixed-H0-gate access 94.9% to 98.8%; joint 94.9% to 99.0%; spatial/grade-H0 95.8% to 97.2%. 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":
  "fb58364255ea84b61774ef7d39e86ccf624091724d95ec3287979e0d13e2d501", "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": 3918, "outer": 43785, "proven_out_of_frame": 58338},
  "per_leg_scope_rule": "outbound_and_return_each_lte_declared_scope_radius", "source_count":
  106041, "source_weight": 968276.9999999995, "weight_by_status": {"frame_unknown": 0.0, "near":
  29838.75, "outer": 370123.750000000076, "proven_out_of_frame": 568314.49999999988},
  "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":
  29838.749999999734, "weight_by_status": {"artifact_error": 0.0, "frame_unknown": 0.0,
  "in_frame": 29838.749999999734, "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 1.700% **QA and artifact warnings:** None [L41]

Twenty-Mile Primary Scope

Publication state: Modeled estimate (4 caveats).

The 20-mile primary H0 channel contains 2,000 draws on the full in-frame sampled denominator: 1,189 unobserved (28.5%), 627 confirmed exposure (56.7%), 141 possible exposure (12.3%), 43 unresolved model (2.5%). The separate robust H0/H1/H2 lattice reports 1,165 unobserved (27.1%), 602 confirmed exposure (54.9%), 144 possible exposure (12.4%), 89 unresolved model (5.7%). Neither channel drops or renormalizes unresolved-model weight.

H0 uncertainty intervals: direction-H0 28.5% to 43.3%; fixed-H0-gate access 27.1% to 33.0%; joint 27.1% to 45.1%; spatial/grade-H0 28.4% to 30.6%. 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":
  "fb58364255ea84b61774ef7d39e86ccf624091724d95ec3287979e0d13e2d501", "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": 3918, "outer": 43785, "proven_out_of_frame": 58338},
```

```
"per_leg_scope_rule": "outbound_and_return_each_lte_declared_scope_radius", "source_count":
106041, "source_weight": 968276.9999999995, "weight_by_status": {"frame_unknown": 0.0, "near":
29838.75, "outer": 370123.750000000076, "proven_out_of_frame": 568314.49999999988},
"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":
399962.500000000943, "weight_by_status": {"artifact_error": 0.0, "frame_unknown": 0.0,
"in_frame": 399962.500000000943, "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 2.533% 3. fixed-gate access-policy interval spans 5.936 pp 4. one or more physical camera clusters exceed the influence materiality limit

QA and artifact warnings: None [L41]

Relationship Between the Two Scopes

20-mile minus 5-mile weighted unobserved-rate difference: primary conditional H0 **-67.3** percentage points; separate robust H0/H1/H2 lattice **-67.8** 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].

References

ID	Source and use in this report
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.

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.
E136	U.S. Air Force, MacDill AFB, "MacDill Air Force Base" fact sheet, https://www.macdill.af.mil/About-Us/Fact-Sheets/Article/4160667/macdill-air-force-base/ - Official installation context for USCENTCOM, USSOCOM, JCSE, coalition participation, mission partners, and workforce scale. Accessed 2026-08-08.
E137	U.S. Transportation Command, Joint Enabling Capabilities Command, "Joint Communications Support Element," https://www.jecc.ustranscom.mil/Subordinate-Commands/JCSE/ - Official JCSE mission: immediate deployment of enroute, early-entry, and scalable C4 support. Accessed 2026-08-08.
E131	Associated Press via PBS NewsHour, "Iran built a vast camera network to control dissent. Israel used it to track targets, AP sources say," March 23, 2026, https://www.pbs.org/newshour/world/iran-built-a-vast-camera-network-to-control-dissent-israel-used-it-to-track-targets-ap-sources-say - Reported precedent for state exploitation of traffic and street cameras to map senior officials, protective personnel, routes, and meetings. Accessed 2026-08-08.
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 that GRU Unit 26165 targeted internet-connected cameras near military installations and border crossings to monitor aid movement. Accessed 2026-08-08.

ID	Source and use in this report
E138	U.S. Air Force, MacDill AFB, "JCSE enables DAF's DLE series," August 7, 2025, https://www.macdill.af.mil/News/Article/4270725/jcse-enables-dafs-dle-series/ - Official example of JCSE personnel deploying early to establish communications architecture for a large exercise. 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].