

Northrop Grumman Headquarters

National Security Exposure Assessment

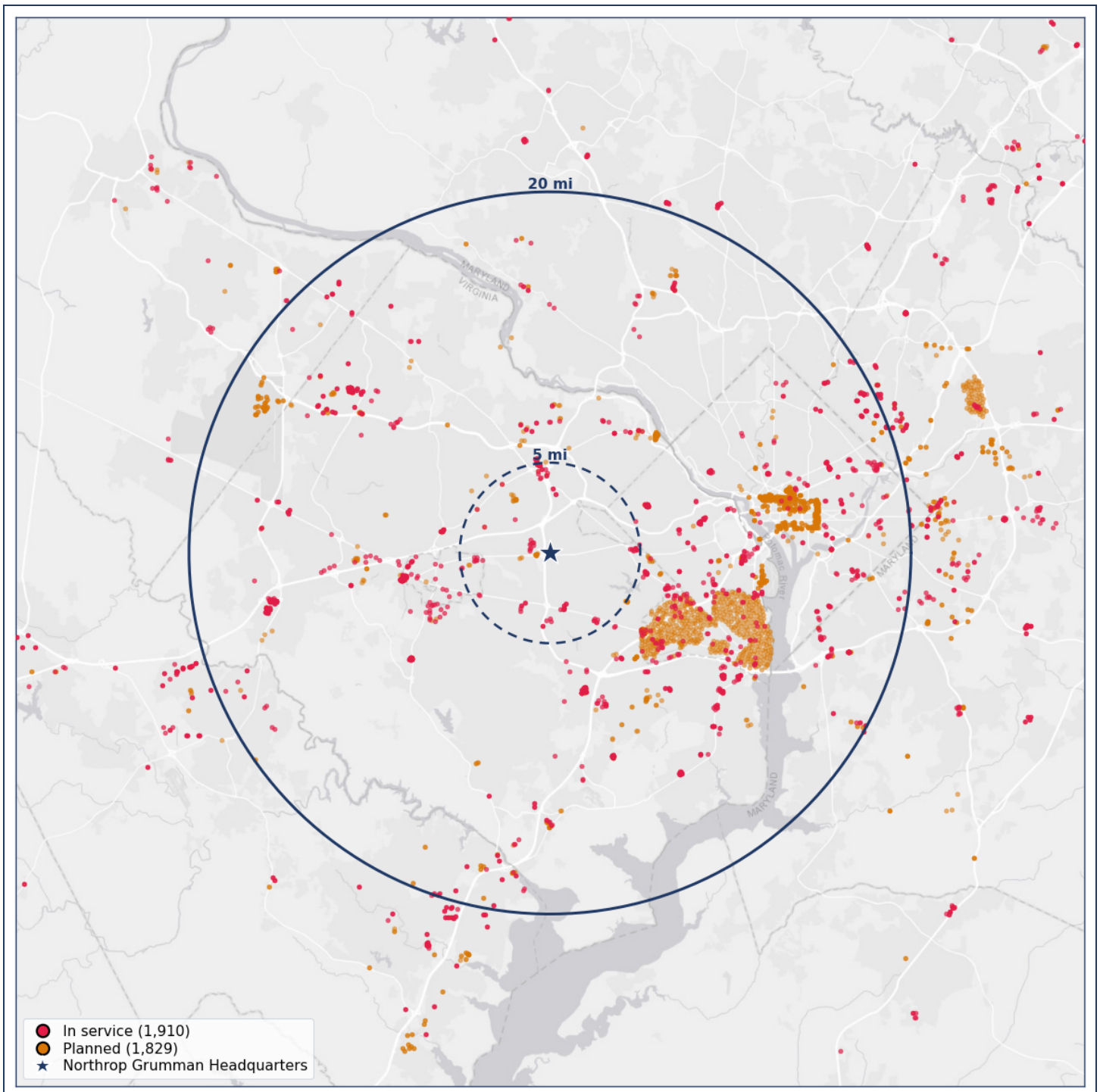
Joshua Michael

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

Northrop Grumman's headquarters in Falls Church is the corporate office for the company that builds the B-21 Raider and supports the Sentinel ICBM — most of the factory work is elsewhere, but the people who review those programs still come here. A rare overlap of Northrop leadership, Air Force officials, and strategic-deterrence staff could mark a B-21 or Sentinel senior review.

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 18.5% of those modeled trips pass a camera. Another 50.5% might pass one, 17.0% avoid them, and 14.0% could not be determined. Closer in, at 5 miles, most trips (76.2%) 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



- 18.5%** **Passes a camera**
A confirmed camera sits on every plausible road to a gate.
- 50.5%** **Might pass**
The inventory's rotationAngle is not a true facing: among 72,971 named in-service cameras it matches the road only about 10% of the time (median error 90°) because it stores housing orientation, not travel. The model therefore does not use it to confirm a hit. Named NB/SB/EB/WB cameras take direction from the road, with the name used only to pick which way they watch. Cameras with no compass name are too noisy to confirm, so a nearby pass stays Might pass. A confirmed hit still needs the vehicle on the same corridor, traveling in that monitored direction within 35°.
- 17.0%** **Avoids all cameras**
No confirmed camera on any plausible road.
- 14.0%** **Couldn't determine**
Extra driveway or side-road options could not be fully routed, so those trips stay unresolved instead of being guessed.

5 MILES OUT



■ 4.3% Passes ■ 10.8% Might pass ■ 76.2% Avoids ■ 8.7% Couldn't determine

Installation Context

Northrop Grumman's principal executive offices are in Falls Church, Virginia. The company publicly states that most of its business is with the U.S. government, principally the Department of Defense and intelligence community, and describes work across aerospace, space, mission systems, networking, cyber, missile defense, and strategic deterrence [E116]. The headquarters is not treated here as a production or flight-test site; most program execution occurs across a distributed enterprise.

The headquarters can still generate unusually valuable association signals. Northrop Grumman is the prime contractor for the B-21 Raider and publicly supports the Sentinel intercontinental ballistic missile modernization program [E117, E118]. Rare overlap among corporate leadership, business-segment executives, government program officials, intelligence-community visitors, security personnel, and outside specialists could reveal which issue has reached senior review even when the technical work occurs elsewhere.

The study did not identify an employee, official, supplier, program participant, meeting, or household. A vehicle observed near the headquarters would not establish a role or affiliation, and the location's dense regional road network, shared destinations, rental cars, visitors, and neighboring properties create substantial uncertainty.

Headquarters-Specific Counterintelligence Scenarios

The scenarios below require historical observations and reliable identity or organizational enrichment beyond the Tier A deployment information used in the route model.

Scenario 1: Inferring a B-21 Program-Level Review or Crisis from Leadership Convergence

Assume that a foreign service obtains longitudinal plate observations and identifies vehicles associated with Northrop Grumman corporate leadership, Aeronautics Systems executives, U.S. Air Force program personnel, security officials, and individuals who normally work at distributed B-21 locations. The analyst's objective would not be to identify routine headquarters traffic. It would be to detect a rare and repeated combination of people whose simultaneous presence is unlikely to be accidental.

Suppose that combination appears after a public flight-test event, production announcement, congressional development, accident, cyber incident, or supplier problem. If senior technical, program, legal, financial, and security personnel converge outside their normal patterns, an adversary could infer that the B-21 program had reached a significant decision point or crisis. The movement record would not reveal the technical problem or decision, but it could show when the issue escalated to corporate and government leadership.

That warning could cue collection elsewhere. The service could intensify cyber activity against likely suppliers, observe lower-security off-site meetings, monitor travel from Palmdale or Air Force program offices, or prioritize individuals whose recurring appearance suggests they bridge test, production, and senior governance. Repetition around later public events could validate the inferred signature.

Operation Anarchist provides a direct advanced-aviation precedent. Reporting based on documents provided by Edward Snowden described a U.S.-British program that intercepted Israeli drone and fighter-aircraft video feeds to understand platform activity, military operations, and possible strike preparations [E119]. The collection medium differs, but the intelligence objective is closely related: exploit external signatures surrounding an advanced aviation capability to determine when it is active and what operational or program development may be underway.

This study does not show that B-21 personnel visited the headquarters or that a program review occurred. The scenario requires accurate person-to-vehicle attribution, a long baseline, and independent corroboration. Headquarters convergence alone could not identify a technical result.

Scenario 2: Mapping an Intelligence-Community or Sentinel Program Delegation

Northrop Grumman's public customer base makes rare visitor associations especially sensitive. Assume that an analyst identifies vehicles linked to intelligence-community offices, strategic-deterrence organizations, Northrop Grumman Space Systems or Defense Systems leadership, Sentinel personnel, and outside contractors. A one-time overlap could be coincidence. Repeated co-arrival at the headquarters, particularly around public acquisition milestones or urgent national-security events, could reveal a sustained relationship or a program-specific review group.

The intelligence value would come from narrowing the network. A foreign service might identify which government organization is working with which company leadership, which outside specialists recur, and which individuals bridge otherwise separate communities. That map could support tailored phishing, recruitment, surveillance, or collection against suppliers and partners with weaker security than the headquarters itself.

The scenario is particularly consequential for strategic deterrence. Public information can identify that Northrop Grumman supports Sentinel, but a recurring movement cluster could reveal the small set of people involved in a particular program problem, restructuring decision, security review, or technical milestone. The adversary would still lack the substance of the meeting, but it would know where to concentrate collection.

Britain's reported Royal Concierge program demonstrates why intelligence services value this kind of mundane association data. Documents disclosed by Edward Snowden described automated monitoring of hotel reservations to identify foreign diplomats' travel plans and prepare additional technical or human collection before their arrival [E114]. The program exploited the fact that who appears at the same place and time can be more revealing than the reservation itself.

The Falls Church route study did not identify an intelligence-community visitor or Sentinel participant. The scenario depends on Tier B history, Tier C enrichment, and corroboration, and it remains vulnerable to false association from shared roads, rental vehicles, ride services, and unrelated headquarters business.

Combined Significance

The B-21 scenario concerns program warning: movement could reveal that an advanced aircraft issue has escalated to senior review. The second scenario concerns relationship intelligence across the defense and intelligence communities, including strategic deterrence. Together, they show why a corporate headquarters can expose both the timing of a sensitive decision and the otherwise low-visibility network of people responsible for making it.

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	83.7%/5.2%/10.3%/0.8%	18.5%/22.5%/56.0%/3.0%
Robust H0/H1/H2 U/C/P/R	76.2%/4.3%/10.8%/8.7%	17.0%/18.5%/50.5%/14.0%
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 **-65.2** percentage points; separate robust H0/H1/H2 lattice **-59.2** percentage points. These channels answer different questions and are not averaged. [L41]

Legislative Significance

Northrop Grumman Headquarters illustrates a counterintelligence risk that ordinary location-privacy rules do not fully capture. A long-lived ALPR archive can reveal rare government–industry and intelligence-community associations even when every individual trip appears mundane and no classified data is stored in the vehicle record.

A sensitive-site statutory framework should include major defense and intelligence contractors’ corporate headquarters. Appropriate controls include short retention of non-hit observations, narrow external sharing, case-specific historical queries, immutable search logs, strict vendor and subcontractor access, and prompt notification to federal counterintelligence and industrial-security authorities after a breach.

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 counterintelligence and mission-assurance concern arises because employees, contractors, government counterparts, visitors, and partners use public roads outside the site's controlled perimeter. The occupied-housing frame is a standardized residential-distribution proxy; it does not identify where anyone associated with Northrop Grumman Headquarters lives, establish an employment relationship, or estimate actual commute volume.

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

To preserve comparability across the multi-site assessment, the analysis applies the same five-road-mile near-site scope and twenty-road-mile primary scope used for military installations. The twenty-mile distance was originally selected from DoD Manual 4165.63 as a transparent commuting-area

approximation [E49]. At Northrop Grumman Headquarters, it functions only as a standardized sensitive-site catchment. It is not a claim about employee residences, commute norms, company or laboratory policy, or the location of any real worker.

Five miles isolates the immediate approach area. Twenty miles adds the broader occupied-housing stratum while retaining every near-site draw and route unchanged. Reporting both shows how the modeled observation surface changes with a wider road network without converting the sample into an employee or visitor estimate.

Limitations and Non-Claims

This is a model over dated deployment, Census, and road snapshots. Occupied housing is a residential-distribution proxy, not a Northrop Grumman Headquarters workforce or visitor roster; it does not weight origins by employer, role, clearance, shift, measured traffic, public transit use, remote work, or actual residential location.

Camera location and status fields can be incomplete, stale, planned, duplicated, moved, or differently interpreted. OpenStreetMap roads and address points can omit valid travel or include obsolete topology. Gate or access-point availability and site geometry depend on analyst review. The route engine models corridor exposure and a geometric field of view; it does not model optical character recognition probability, weather, plate condition, device uptime, 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. Shared roads, neighboring destinations, rental vehicles, ride services, carpools, public transit, and unrelated visitors create substantial alternative explanations at a corporate or research headquarters.

Evidence and Reproducibility

The V7 drafting packet was built from the complete validated cohort for

`northrop_grumman_headquarters`. It binds cohort `reachability-v7-audit-92bd2e6a45c3a7c6`, pair `northrop_grumman_headquarters-068562f93fbe2e48`, seed `507436146`, index SHA-256 `3d0755cb6fcc7dd165c6b9dd53ade8bfe5402773231904ea3807d1f17dc3b96b`, five-mile summary SHA-256 `3b48f6f29c502cfd6e655ef02eb4d33b119f9c66065281c8581eeb6de792fe9f`, and twenty-mile summary SHA-256 `b953a439dca39d4fd85a5f3a917a17eb6fef6fa58215147e327f7b3aa336ac5a`. [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	northrop_grumman_headquarters-068562f93fbe2e48	northrop_grumman_headquarters-068562f93fbe2e48
Pair seed	507436146	507436146
Generated at	2026-08-12T14:12:48.322119+00:00	2026-08-12T14:12:48.322119+00:00
Summary SHA-256	3b48f6f29c502cfd6e655ef02eb4d33b119f9c66065281c8581eeb6de792fe9f	b953a439dca39d4fd85a5f3a917a17eb6fef6fa58215147e327f7b3aa336ac5a
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	837/52/103/8	978/289/693/40
Primary H0 U/C/P/R	83.7%/5.2%/10.3%/0.8%	18.5%/22.5%/56.0%/3.0%
Robust H0/H1/H2 U/C/P/R counts	762/43/108/87	892/238/639/231
Robust H0/H1/H2 U/C/P/R	76.2%/4.3%/10.8%/8.7%	17.0%/18.5%/50.5%/14.0%
Direction H0 interval	83.7% to 94.8%	18.5% to 77.5%
Fixed-gate access interval	76.2% to 86.1%	17.0% to 31.3%
Joint interval	76.2% to 95.7%	17.0% to 81.5%

Field	5-mile near-base	20-mile primary
Spatial H0 interval	81.2% to 84.2%	17.9% to 20.5%
Gate reselection diagnostic	fixed 81.3%; reselected 81.3%; absolute difference 0.0 pp	fixed 18.1%; reselected 18.1%; 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
H0 range sensitivity U/C/P/R	75ft: 89.1%/5.2%/4.9%/0.8%; 150ft: 83.7%/5.2%/10.3%/0.8%; 250ft: 74.2%/5.2%/19.8%/0.8%	75ft: 50.2%/22.4%/24.4%/3.0%; 150ft: 18.5%/22.5%/56.0%/3.0%; 250ft: 13.7%/23.2%/60.0%/3.0%
H0 direction sensitivity U/C/P/R	25deg: 84.3%/5.2%/9.7%/0.8%; 30deg: 84.3%/5.2%/9.7%/0.8%; 35deg: 83.7%/5.2%/10.3%/0.8%; 40deg: 83.7%/5.2%/10.3%/0.8%; 45deg: 83.7%/5.2%/10.3%/0.8%; 60deg: 82.7%/5.2%/11.3%/0.8%	25deg: 18.7%/22.5%/55.7%/3.0%; 30deg: 18.7%/22.5%/55.7%/3.0%; 35deg: 18.5%/22.5%/56.0%/3.0%; 40deg: 18.5%/22.5%/56.0%/3.0%; 45deg: 18.5%/22.5%/56.0%/3.0%; 60deg: 15.3%/22.5%/59.1%/3.0%
Deployment-status sensitivity U/C/P/R	declared_policy: 83.7%/5.2%/10.3%/0.8%; in_service_only: 83.7%/4.7%/10.8%/0.8%	declared_policy: 18.5%/22.5%/56.0%/3.0%; in_service_only: 18.9%/19.3%/58.7%/3.0%
Physical-camera-cluster influence	maximum removal shift 3.6 pp; 0 material clusters	maximum removal shift 7.3 pp; 2 material clusters
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. fixed-gate access-policy interval spans 9.900 pp	1. corridor routing is a single-reviewer accuracy check (~89.5%; see the report's Appendix O)2. primary H0 unresolved weight is 3.050%3. fixed-gate access-policy interval spans 14.306 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 **-65.2** percentage points; separate robust H0/H1/H2 lattice **-59.2** 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: 837 unobserved (83.7%), 52 confirmed exposure (5.2%), 103 possible exposure (10.3%), 8 unresolved model (0.8%). The separate robust H0/H1/H2 lattice reports 762 unobserved (76.2%), 43 confirmed exposure (4.3%), 108 possible exposure (10.8%), 87 unresolved model (8.7%). Neither channel drops or renormalizes unresolved-model weight.

H0 uncertainty intervals: direction-H0 83.7% to 94.8%; fixed-H0-gate access 76.2% to 86.1%; joint 76.2% to 95.7%; spatial/grade-H0 81.2% to 84.2%. 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":
  "84c68c08cc9ea2f4f4ffacd9e11fd0ceed8433cd420c20e927a9a0fc6c7da980", "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": 460, "near": 4070, "outer": 53260, "proven_out_of_frame": 47753},
"per_leg_scope_rule": "outbound_and_return_each_lte_declared_scope_radius", "source_count":
105543, "source_weight": 1803160.0000000012, "weight_by_status": {"frame_unknown": 5299.5,
"near": 63258.49999999999, "outer": 947039.4166666671, "proven_out_of_frame":
787562.5833333341}, "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": 63258.500000001666, "weight_by_status": {"artifact_error": 0.0, "frame_unknown": 0.0, "in_frame": 63258.500000001666, "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. fixed-gate access-policy interval spans 9.900 pp**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: 978 unobserved (18.5%), 289 confirmed exposure (22.5%), 693 possible exposure (56.0%), 40 unresolved model (3.0%). The separate robust H0/H1/H2 lattice reports 892 unobserved (17.0%), 238 confirmed exposure (18.5%), 639 possible exposure (50.5%), 231 unresolved model (14.0%). Neither channel drops or renormalizes unresolved-model weight.

H0 uncertainty intervals: direction-H0 18.5% to 77.5%; fixed-H0-gate access 17.0% to 31.3%; joint 17.0% to 81.5%; spatial/grade-H0 17.9% to 20.5%. 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": "84c68c08cc9ea2f4f4ffacd9e11fd0ceed8433cd420c20e927a9a0fc6c7da980", "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": 460, "near": 4070, "outer": 53260, "proven_out_of_frame": 47753}, "per_leg_scope_rule": "outbound_and_return_each_lte_declared_scope_radius", "source_count": 105543, "source_weight": 1803160.00000000012, "weight_by_status": {"frame_unknown": 5299.5, "near": 63258.49999999999, "outer": 947039.4166666671, "proven_out_of_frame": 787562.5833333341}, "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": 1010297.9166666981, "weight_by_status": {"artifact_error": 0.0, "frame_unknown": 0.0, "in_frame": 1010297.9166666981, "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 3.050%3. fixed-gate access-policy interval spans 14.306 pp4. 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 **-65.2** percentage points; separate robust H0/H1/H2 lattice **-59.2** 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.

ID	Source and use in this report
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.
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.
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.
E116	Northrop Grumman, "Who We Are," https://www.northropgrumman.com/who-we-are - Official Falls Church headquarters, government and intelligence-community customer base, and public portfolio description. Accessed 2026-08-08.
E117	Northrop Grumman, "B-21 Raider," https://news.northropgrumman.com/b-21 - Official public information on Northrop Grumman's B-21 role and program progression. Accessed 2026-08-08.

ID	Source and use in this report
E118	Northrop Grumman, "Digital Engineering from the Ground Up," https://www.northropgrumman.com/what-we-do/advanced-weapons/sentinel/digital-engineering-from-the-ground-up - Official public description of the Sentinel strategic-deterrence program. Accessed 2026-08-08.
E119	The Guardian, "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 precedent for collection against external signatures of an advanced aviation capability. Accessed 2026-08-08.
E114	The Guardian, "Snowden cache reveals diplomats' hotel bookings being tracked by GCHQ," November 17, 2013, https://www.theguardian.com/world/2013/nov/17/edward-snowden-diplomats-hotel-bookings-documents - Reporting on Royal Concierge, used as precedent for mapping rare official travel and meeting overlaps. 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.

ID	Source and use in this report
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.
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.

ID	Source and use in this report
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.
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 reachability-v7-audit-92bd2e6a45c3a7c6 (index SHA-256 3d0755cb6fcc7dd165c6b9dd53ade8bfe5402773231904ea3807d1f17dc3b96b); 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 ../Supporting Tools and Docs/project_support/planning_and_qa/reachability_v7_audit_development_snapshot.js on .

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].