

Fort George G. Meade

National Security Exposure Assessment

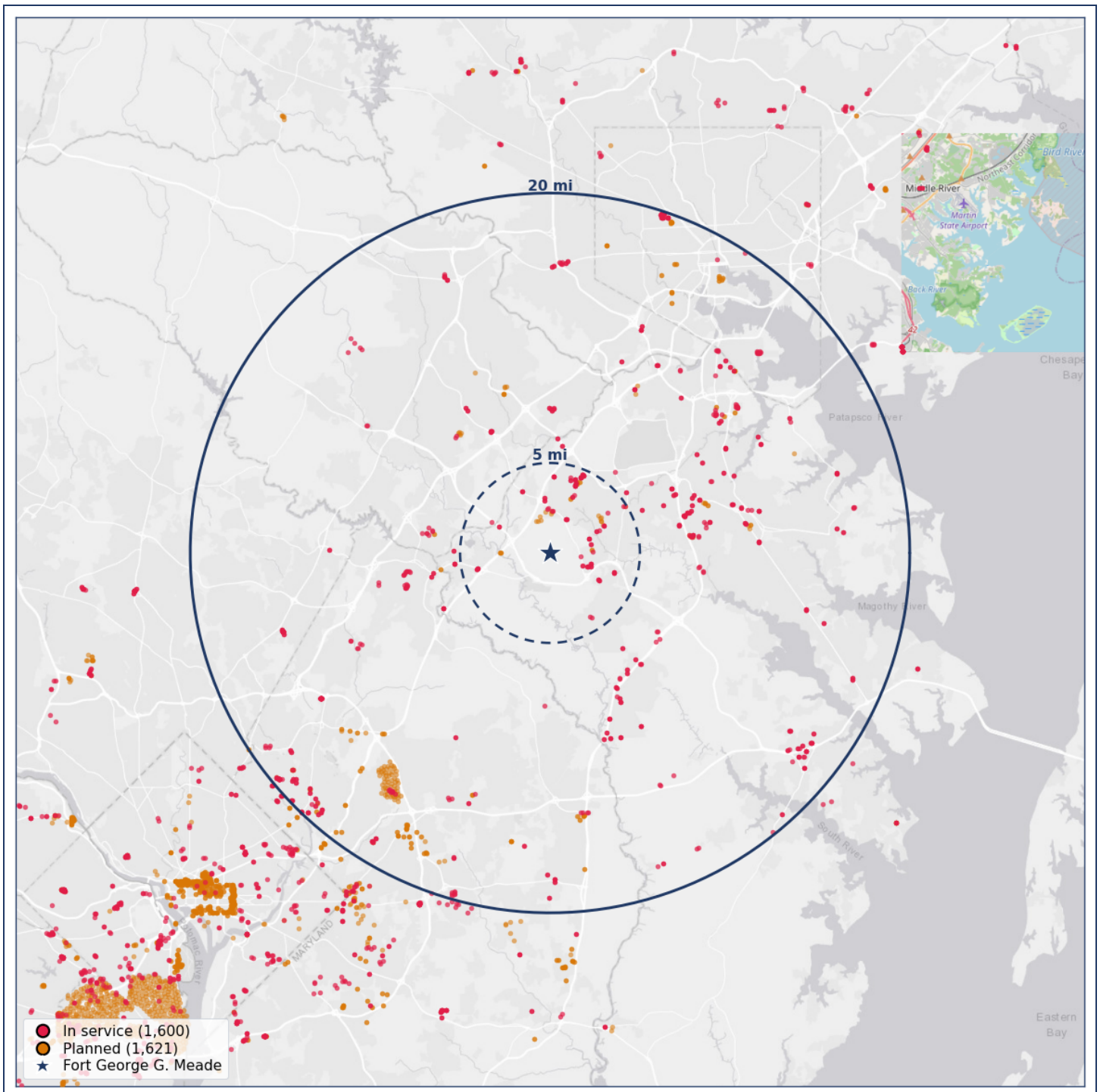
Joshua Michael

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

Fort Meade is the country's main hub for intelligence, information, and cyber operations — U.S. Cyber Command, DISA, and NSA all sit on or next to this post. An after-hours surge among cyber, intelligence, and contractor traffic could warn that the United States had just detected or started answering a major cyber event.

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 50.3% of those modeled trips pass a camera. Another 5.0% might pass one, 34.8% avoid them, and 9.9% could not be determined. Even at 5 miles, about 80.4% 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



- **50.3%** **Passes a camera**
A confirmed camera sits on every plausible road to a gate.
- **5.0%** **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.
- **34.8%** **Avoids all cameras**
No confirmed camera on any plausible road.
- **9.9%** **Couldn't determine**
The model could not finish a legal round trip for these draws.

5 MILES OUT



■ **80.4%** Passes ■ **0.1%** Might pass ■ **12.8%** Avoids ■ **6.7%** Couldn't determine

Installation Context

Fort George G. Meade is publicly described as the nation's premier platform for intelligence, information, and cyber operations [E62]. Official sources identify U.S. Cyber Command headquarters and the Defense Information Systems Agency headquarters on the installation, while Fort Meade public directories also acknowledge the National Security Agency and other military and federal organizations [E63, E160-E163].

The Cyber National Mission Force is especially relevant to movement analysis. USCYBERCOM describes it as a joint military cyber force that supports national priorities, conducts full-spectrum operations, and has participated in or responded to major national crises [E161]. DISA headquarters and its joint operations functions add a separate communications and network-support population whose surge patterns may overlap with, but are not identical to, cyber mission activity [E162].

Those public facts do not allow a plate to be assigned to NSA, USCYBERCOM, DISA, a military service, or a contractor. They explain why aggregate workforce movement at Fort Meade can be unusually sensitive. The study did not identify any employee, agency, cyber team, household, operation, or watch schedule, and its one reviewed gate cannot be assumed to represent every tenant's commuting behavior.

Installation-Specific Intelligence Scenarios

The study demonstrates Tier A deployment and modeled route exposure only. Both scenarios below require Tier B historical time-stamped observations and Tier C identity or organizational enrichment that were not obtained.

Scenario 1: Detecting a USCYBERCOM or Cyber National Mission Force Crisis-Response Surge

Assume that a foreign service obtains historical plate observations around Fort Meade and gradually establishes a baseline for recurring military, civilian, contractor, and support traffic. The service would not need to distinguish every agency at first. It could begin by isolating vehicle clusters that repeatedly appear during public cyber exercises, major ransomware events, election-security periods, or announced international cyber incidents.

A high-value signal would be an abnormal convergence involving probable USCYBERCOM or Cyber National Mission Force personnel, DISA operations support, technical contractors, senior staff, and security or continuity functions. If those clusters begin arriving outside normal schedules and sustain activity through nights or weekends, the pattern could indicate that the United States has detected a serious cyber event, initiated a national-level response, or activated a deployable cyber element [E160-E162].

The adversary might not know the target network, planned operation, or responsible team. Early warning that U.S. cyber forces are responding can still be valuable. It may allow the responsible actor to abandon infrastructure, alter command-and-control patterns, destroy evidence, accelerate an operation, or warn partner services before the U.S. response becomes public.

The same archive could reveal return and recovery. A surge that ends abruptly, a subset of vehicles that disappears, or a returning cluster following an overseas cyber hunt could help estimate mission duration and identify the personnel most directly involved. Repetition across several public events would improve the adversary's model of which movement signatures correspond to routine exercises and which indicate real operations.

The GRU Unit 26165 campaign disclosed by the United States, United Kingdom, and partner governments provides a direct collection precedent. The advisory states that Russian military intelligence targeted internet-connected cameras near military installations and border crossings to monitor and track military aid movement [E148]. The target in that case was logistics rather than cyber personnel, but the method is the same: compromise distributed civilian sensors to learn military activity without penetrating the military's classified operational network.

This study does not show a Fort Meade cyber surge, identify a tenant organization, or establish access to historical plate records. The scenario requires Tier B longitudinal observations, Tier C identity or organizational enrichment, and a baseline capable of separating real activity from shift work, exercises, contractor schedules, and the installation's many unrelated missions.

Scenario 2: Identifying Cleared Intelligence and Cyber Personnel Across Agencies and Contractors

Fort Meade's second major risk is persistent personnel identification. A plate repeatedly associated with the installation does not reveal whether the driver works for NSA, USCYBERCOM, DISA, a military service, a defense contractor, or an unrelated tenant. Long-term association analysis can narrow that uncertainty.

An adversary could compare vehicle co-occurrence, arrival times, secondary destinations, contractor facilities, public professional histories, and deployment or travel absences. Vehicles that repeatedly bridge otherwise separate clusters may belong to liaisons, technical leaders, network defenders, acquisition personnel, or contractors supporting more than one organization. The result could be a probabilistic map of the people who connect Fort Meade's intelligence, cyber, communications, and industry communities.

Once probable identities are assigned, historical observations may expose residences, family vehicles, recurring off-base meetings, schools, medical locations, and periods of absence. That information can support tailored phishing, recruitment, surveillance, device theft, coercion, or collection against family members. The intelligence service need not identify every employee. Reducing a workforce of tens of thousands to a small set of probable mission-relevant specialists already has substantial value.

The 2015 Office of Personnel Management breach is a direct precedent for state collection against the cleared U.S. workforce. GAO reported that the breach affected 21.5 million people and included sensitive background-investigation information, while the FBI has publicly attributed the theft of OPM data to Chinese actors [E149, E150]. That system did not provide road movements, but it supplied the identity and vulnerability context an intelligence service would want to combine with longitudinal location records.

ALPR history would add what OPM records did not: current movement, recurring associations, household vehicles, and operational absence. Conversely, compromised personnel records could turn an otherwise anonymous plate cluster into a list of named intelligence and cyber targets. The combination is more dangerous than either dataset by itself.

The present research did not obtain OPM records, a Fort Meade roster, plate identities, or personal movement histories. It demonstrates Tier A route exposure only. The scenario is intended to show why broad retention and cross-system enrichment around an intelligence and cyber campus create a counterintelligence risk even when individual plate scans remain unclassified.

Combined Significance

Scenario 1 concerns operational warning: movement changes could signal that a national cyber response is underway. Scenario 2 concerns counterintelligence targeting: repeated observations could identify the cleared people and contractor relationships that make the response possible. Together they show how a surveillance layer outside Fort Meade's perimeter can reveal both mission tempo and the human network behind 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 (4 caveats)	Modeled estimate (4 caveats)
Headline channel	robust_lattice	robust_lattice
Primary H0 U/C/P/R	13.4%/82.1%/0.0%/4.5%	39.4%/52.3%/5.1%/3.3%

Field	5-mile near-base	20-mile primary
Robust H0/H1/H2 U/C/P/R	12.8%/80.4%/0.1%/6.7%	34.8%/50.3%/5.0%/9.9%
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 **+26.0** percentage points; separate robust H0/H1/H2 lattice **+22.0** percentage points. These channels answer different questions and are not averaged. [L41]

Legislative Significance

Fort Meade warrants designation as a heightened-risk intelligence and cyber site. Legislation should require strict vendor and subcontractor access controls, short non-hit retention, narrow historical-query predicates, limits on nationwide sharing, immutable auditing, and rapid notification to installation, USCYBERCOM, NSA, DISA, and appropriate counterintelligence authorities when plate or camera systems covering the area are compromised. Public policy should avoid disclosing precise gaps or routes while still requiring independent security review.

Neither recommendation depends on a claim that a current operator acted improperly. The policy issue is whether a longitudinal commercial movement archive surrounding a sensitive national-security site should be retained, broadly shared, or exposed through vendor and subcontractor systems without controls proportionate to the intelligence value of the aggregate record.

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

Finding	Observed condition	Evidence boundary	Disclosure and remediation status	Source(s)
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
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 Fort George G. Meade 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 a person assigned to Fort George G. Meade 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 Fort George G. Meade 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 Fort George G. Meade 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 `fort_george_g_meade`. It binds cohort `reachability-v7-audit-92bd2e6a45c3a7c6`, pair `fort_george_g_meade-4f7ddf34d612c73f`, seed `2575594657`, index SHA-256 `3d0755cb6fcc7dd165c6b9dd53ade8bfe5402773231904ea3807d1f17dc3b96b`, five-mile summary SHA-256 `a0f8b57a2a424ded3c49e5aa95007c090f09a737b52a84581e83f2cc585ead83`, and twenty-mile summary SHA-256 `6d757296f9cef904cdaf461d885903fb03098d939d1e7d05437ae3b1b6d0bc52`. [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 (4 caveats)	Modeled estimate (4 caveats)
V7 cohort	<code>reachability-v7-audit-92bd2e6a45c3a7c6</code>	<code>reachability-v7-audit-92bd2e6a45c3a7c6</code>
Pair ID	<code>fort_george_g_meade-4f7ddf34d612c73f</code>	<code>fort_george_g_meade-4f7ddf34d612c73f</code>
Pair seed	<code>2575594657</code>	<code>2575594657</code>
Generated at	<code>2026-08-12T10:35:24.105837+00:00</code>	<code>2026-08-12T10:35:24.105837+00:00</code>
Summary SHA-256	<code>a0f8b57a2a424ded3c49e5aa95007c090f09a737b52a84581e83f2cc585ead83</code>	<code>6d757296f9cef904cdaf461d885903fb03098d939d1e7d05437ae3b1b6d0bc52</code>

Field	5-mile near-base	20-mile primary
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	134/821/0/45	541/1328/54/77
Primary H0 U/C/P/R	13.4%/82.1%/0.0%/4.5%	39.4%/52.3%/5.1%/3.3%
Robust H0/H1/H2 U/C/P/R counts	128/804/1/67	487/1291/54/168
Robust H0/H1/H2 U/C/P/R	12.8%/80.4%/0.1%/6.7%	34.8%/50.3%/5.0%/9.9%
Direction H0 interval	13.4% to 17.9%	39.4% to 47.7%
Fixed-gate access interval	12.8% to 19.6%	34.8% to 45.3%
Joint interval	12.8% to 19.6%	34.8% to 49.7%
Spatial H0 interval	12.6% to 15.8%	38.8% to 41.7%
Gate reselection diagnostic	fixed 13.4%; reselected 13.4%; absolute difference 0.0 pp	fixed 38.0%; reselected 38.0%; 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: 13.6%/81.9%/0.0%/4.5%; 150ft: 13.4%/82.1%/0.0%/4.5%; 250ft: 13.4%/82.1%/0.0%/4.5%	75ft: 44.3%/52.2%/0.2%/3.3%; 150ft: 39.4%/52.3%/5.1%/3.3%; 250ft: 38.6%/52.5%/5.6%/3.3%
H0 direction sensitivity U/C/P/R	25deg: 13.4%/82.1%/0.0%/4.5%; 30deg: 13.4%/82.1%/0.0%/4.5%; 35deg: 13.4%/82.1%/0.0%/4.5%; 40deg: 13.4%/82.1%/0.0%/4.5%; 45deg: 13.4%/82.1%/0.0%/4.5%; 60deg: 7.1%/82.1%/6.3%/4.5%	25deg: 41.5%/52.3%/2.9%/3.3%; 30deg: 41.5%/52.3%/2.9%/3.3%; 35deg: 39.4%/52.3%/5.1%/3.3%; 40deg: 39.4%/52.3%/5.1%/3.3%; 45deg: 39.4%/52.3%/5.1%/3.3%; 60deg: 29.0%/52.3%/15.5%/3.3%
Deployment-status sensitivity U/C/P/R	declared_policy: 13.4%/82.1%/0.0%/4.5%; in_service_only: 13.6%/81.9%/0.0%/4.5%	declared_policy: 39.4%/52.3%/5.1%/3.3%; in_service_only: 46.8%/49.7%/0.3%/3.3%
Physical-camera-cluster influence	maximum removal shift 3.7 pp; 0 material clusters	maximum removal shift 4.3 pp; 0 material clusters
H0 validation	single-reviewer check	single-reviewer check

Field	5-mile near-base	20-mile primary
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 4.500%3. fixed-gate access-policy interval spans 6.800 pp4. direction-tolerance sensitivity exceeds materiality limit	1. corridor routing is a single-reviewer accuracy check (~89.5%; see the report's Appendix O)2. primary H0 unresolved weight is 3.264%3. fixed-gate access-policy interval spans 10.507 pp4. direction-tolerance sensitivity exceeds materiality limit
QA and artifact warnings	None	None

20-mile minus 5-mile weighted unobserved-rate difference: primary conditional H0 **+26.0** percentage points; separate robust H0/H1/H2 lattice **+22.0** percentage points. These channels answer different questions and are not averaged. [L41]

Reachability Results

Five-Mile Near-Base Scope

Publication state: Modeled estimate (4 caveats).

The 5-mile primary H0 channel contains 1,000 draws on the full in-frame sampled denominator: 134 unobserved (13.4%), 821 confirmed exposure (82.1%), 0 possible exposure (0.0%), 45 unresolved model (4.5%). The separate robust H0/H1/H2 lattice reports 128 unobserved (12.8%), 804 confirmed exposure (80.4%), 1 possible exposure (0.1%), 67 unresolved model (6.7%). Neither channel drops or renormalizes unresolved-model weight.

H0 uncertainty intervals: direction-H0 13.4% to 17.9%; fixed-H0-gate access 12.8% to 19.6%; joint 12.8% to 19.6%; spatial/grade-H0 12.6% to 15.8%. 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":

"3f440354380ebe6df53cc505f7559ea547c5cd03c8c32205e86b1c0f3091d16a", "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": 409, "near": 1303, "outer": 28720, "proven_out_of_frame": 75356},

"per_leg_scope_rule": "outbound_and_return_each_lte_declared_scope_radius", "source_count":

105788, "source_weight": 1657134.9999999993, "weight_by_status": {"frame_unknown": 4987.5,

"near": 27018.416666666657, "outer": 519866.5833333332, "proven_out_of_frame":

1105262.4999999995}, "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": 27018.416666666144, "weight_by_status": {"artifact_error": 0.0,
"frame_unknown": 0.0, "in_frame": 27018.416666666144, "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 4.500% 3. fixed-gate access-policy interval spans 6.800 pp 4. direction-tolerance sensitivity exceeds materiality limit **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: 541 unobserved (39.4%), 1,328 confirmed exposure (52.3%), 54 possible exposure (5.1%), 77 unresolved model (3.3%). The separate robust H0/H1/H2 lattice reports 487 unobserved (34.8%), 1,291 confirmed exposure (50.3%), 54 possible exposure (5.0%), 168 unresolved model (9.9%). Neither channel drops or renormalizes unresolved-model weight.

H0 uncertainty intervals: direction-H0 39.4% to 47.7%; fixed-H0-gate access 34.8% to 45.3%; joint 34.8% to 49.7%; spatial/grade-H0 38.8% to 41.7%. 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":
"3f440354380ebe6df53cc505f7559ea547c5cd03c8c32205e86b1c0f3091d16a", "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": 409, "near": 1303, "outer": 28720, "proven_out_of_frame": 75356},
"per_leg_scope_rule": "outbound_and_return_each_lte_declared_scope_radius", "source_count":
105788, "source_weight": 1657134.9999999993, "weight_by_status": {"frame_unknown": 4987.5,
"near": 27018.416666666657, "outer": 519866.5833333332, "proven_out_of_frame":
1105262.4999999995}, "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": 546885.00000000065, "weight_by_status": {"artifact_error": 0.0, "frame_unknown": 0.0, "in_frame": 546885.00000000065, "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 3.264% 3. fixed-gate access-policy interval spans 10.507 pp 4. direction-tolerance sensitivity exceeds 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 +**26.0** percentage points; separate robust H0/H1/H2 lattice +**22.0** 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, <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.
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.

ID	Source and use in this report
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.
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.
E62	U.S. Army Garrison Fort George G. Meade, “Mission,” https://home.army.mil/meade/about/mission - Official description of Fort Meade as a platform for intelligence, information, and cyber operations and of the garrison’s readiness-support role. Accessed 2026-07-21.

ID	Source and use in this report
E63	U.S. Army Garrison Fort George G. Meade, "Col. Sapp takes command of U.S. Army Garrison Fort George G. Meade," https://home.army.mil/meade/about/Garrison/public-affairs/digital-meade/col-sapp-takes-command-us-army-garrison-fort-george-g-meade - Dated official context describing Fort Meade's multi-service and civilian workforce and installation population. Used only as public scale context, not as a current person-level census. Accessed 2026-07-21.
E148	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 logistics and transportation organizations and internet-connected cameras near military installations and border crossings to monitor and track aid shipments. Accessed 2026-08-08.
E149	U.S. Government Accountability Office, <i>Information Security: OPM Has Improved Controls, but Further Efforts Are Needed</i> (GAO-17-614), August 3, 2017, https://www.gao.gov/products/gao-17-614 - Official account that the 2015 OPM breaches affected 21.5 million individuals and involved sensitive personnel and security-clearance-investigation information. Accessed 2026-08-08.
E150	Federal Bureau of Investigation, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," July 7, 2020, https://www.fbi.gov/news/speeches-and-testimony/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states - FBI attribution and counterintelligence context for Chinese theft of OPM and other large U.S. personal-data repositories. Accessed 2026-08-08.
E160	U.S. Cyber Command, "Home," https://www.cybercom.mil/ - Official public mission and headquarters context for U.S. Cyber Command at Fort George G. Meade. Accessed 2026-08-08.

ID	Source and use in this report
E161	U.S. Cyber Command, "About the Cyber National Mission Forces," December 6, 2023, https://www.cybercom.mil/Media/News/Article/3610711/about-the-cyber-national-mission-forces/ - Official description of CNMF's crisis-response, defensive, disruptive, and globally deployable cyber mission. Accessed 2026-08-08.
E162	Defense Information Systems Agency, "Military," https://www.disa.mil/careers/military - Official confirmation that DISA headquarters is located at Fort George G. Meade. Accessed 2026-08-08.
E163	U.S. Army Garrison Fort George G. Meade, "Inspector General," https://home.army.mil/meade/about/Garrison/inspector-general - Official public directory acknowledging USCYBERCOM and NSA organizations on Fort Meade. Used only for public installation context. 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.json .

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].