

The Adjacent-Launch Seam:

Counter-UAS Authority Gaps in the National Capital Region

Three legal regimes govern the airspace and property around protected sites in the NCR, and each was built for a different purpose: CFIUS real-estate review (31 C.F.R.

DOCUMENT	VERSION	DATE
WP-2026-D3	V1.6	2026-10-01
AUTHOR	ORGANIZATION	SERIES
COLLIN GEORGE	SANCTIR LLC	PAPER III OF THREE

UNCLASSIFIED // OPEN SOURCE · NOT OFFICIAL U.S. GOVERNMENT ANALYSIS

Paper record

SERIES	DRONE THREATS TO POLITICAL LEADERSHIP: CAPABILITY, DEFENSE, AND AUTHORITY
AUTHOR	Collin George, Founder, Sanctir LLC ¹
PAPER	Paper III of three — The Adjacent-Launch Seam
DOCUMENT	WP-2026-D3 · v1.6 · 2026-10-01
SCOPE	Adequacy of the U.S. legal and regulatory framework for National Capital Region leadership protection after the SAFER SKIES Act.
SOURCES	Open source only. Bluebook (21st ed.) citations; 39 footnotes.
CONFIDENCE STANDARD	ICD 203. Confidence is stated separately from likelihood.
COMPANION PAPERS	Paper I, <i>Not Science Fiction</i> ; Paper II, <i>The Terminal Residual</i>
CLASSIFICATION	Unclassified // Open source

Abstract

Commercially available small unmanned aircraft systems (sUAS) place a precision, close-access strike capability within reach of a lone actor operating from a privately controlled structure adjacent to a protected site. This paper — the third in a series on drone threats to political leadership — assesses the adequacy of the U.S. legal and regulatory framework for protecting senior leadership in the National Capital Region (NCR) against that threat. It argues that the principal advances of the SAFER SKIES Act, enacted within the FY2026 National Defense Authorization Act, materially narrowed the headline authority gap that dominated oversight from 2018 to 2025, yet left the specific vector of an adjacent-structure launch in the seam between three legal regimes that were each designed for a different purpose: CFIUS real-estate review (foreign investment), the National Capital Region airspace rules (cooperative operators), and 6 U.S.C. § 124n counter-UAS authority (active mitigation by authorized government actors). Only the last is aimed at the threat, and its operation against a non-cooperative drone launched close-in from a private adjacent structure is limited by sensing coverage, coordination, and a decision loop the launch geometry can out-time. The paper identifies six residual seams — implementation lag, the absence of private-adjacency authority, privately owned airspace coordination, a terminal-engagement timeline that may fall below the lawful decision loop, the absence of any protective-sightline screening regime, and a prevention layer that is voluntary and eroding — and evaluates constitutionally compatible oversight and legislative options to address the achievable ones. The analysis

¹. Collin George, Founder, Sanctir LLC. This is a working paper and does not constitute, and should not be cited as, official U.S. Government analysis. It is Paper III in the series *Drone Threats to Political Leadership: Capability, Defense, and Authority*. All sources are open-source; citations follow *The Bluebook: A Uniform System of Citation* (21st ed.). The author welcomes correspondence.

draws exclusively on open-source primary materials and is offered as scholarship, not as official analysis or operational guidance.

IF YOU READ NOTHING ELSE

Central Judgment: The three legal regimes touching the NCR — CFIUS real-estate review, the SFRA/FRZ/P-56 airspace regime, and § 124n C-UAS authority — each address a different axis (foreign investment, cooperative-operator compliance, active mitigation). Only § 124n is aimed at a non-cooperative drone, and against a close-in launch from a privately controlled adjacent structure it is limited by sensing coverage, coordination, and a decision loop the geometry can out-time.

Proximity and elevation — a private structure with a direct sightline onto a protected site — is the decisive geometry, minimizing warning time and placing the launch outside the federal access-controlled footprint.

No mitigation authority, and no authority to detect by legally restricted means, extends to private owners or occupants of the adjacent structures that provide the decisive sightline — the best launch position is the least-covered location.

1. Introduction

Commercially available small unmanned aircraft systems (sUAS) place a precision, close-access strike capability within reach of a lone actor operating from a privately controlled structure adjacent to a protected site. The threat to a protected person in the National Capital Region (NCR) is no longer bounded principally by the sophistication required to build a weapon; it is bounded by the defender's ability to detect, classify, decide, and lawfully mitigate within an engagement window that a short-range terminal profile can compress to seconds. That capability is mature and proliferating rather than speculative — a premise developed at length in the first paper of this series² and summarized in Part 4 below.

This paper does not argue that federal counter-UAS (C-UAS) authority is absent. Federal § 124n authority lapsed on 1 October 2025 and was restored on 12 November 2025, when a continuing resolution extended it through 30 January 2026. The SAFER SKIES Act, enacted as part of the FY2026 National Defense Authorization Act on 18 December 2025, then extended the core 6 U.S.C. § 124n authorities — federal authority to 30 September 2031 and the new state, local, tribal, and territorial (SLTT) authority to 31 December 2031 — and, for the first time, created a statutory pathway for SLTT law enforcement to mitigate drone threats.³ The headline authority gap that dominated oversight from 2018 to 2025 has substantially narrowed. The argument here is that the narrowing left intact the one vector that matters most for leadership protection.

2. Collin George, *Not Science Fiction: The Maturation of Small-UAS as a Precision Weapon* (Drone Threats to Political Leadership: Capability, Defense, and Authority, Paper I) (forthcoming 2026) (developing the capability-maturity premise summarized in Part 4).

3. 6 U.S.C. § 124n, as amended by the SAFER SKIES Act, Pub. L. No. 119–60, div. H, tit. LXXXVI, §§ 8601–8607, 139 Stat. 718, 1938–45 (2025). Federal authority terminates Sept. 30, 2031; the SLTT authority added at § 124n(a)(2) terminates Dec. 31, 2031 (sunset codified at § 124n(j)(2)). Federal authority lapsed Oct. 1–Nov. 11, 2025, and was restored through Jan. 30, 2026 by Pub. L. No. 119–37, div. A, § 145 (Nov. 12, 2025), before the SAFER SKIES amendments superseded that extension.

CENTRAL JUDGMENT

Three legal regimes govern the airspace and property around protected sites in the NCR, and each was built for a different purpose: CFIUS real-estate review (31 C.F.R. pt. 802) screens *foreign investment*; the DC Special Flight Rules Area, Flight Restricted Zone, Prohibited Area P-56, and the FAA's UAS security notice for the Flight Restricted Zone regulate cooperative operators; and 6 U.S.C. § 124n governs *active mitigation by authorized government actors*. Only § 124n is aimed at a non-cooperative drone, and against a close-in launch from a privately controlled adjacent structure its operation is limited by sensing coverage, coordination, and a lawful decision loop that the launch geometry can out-time; the other two regimes neither detect nor interdict it. That specific vector therefore falls in the seam among all three regimes (high confidence).

The significance of that seam is heightened by a finding developed in the second paper of this series: terminal defense against this class of threat is not merely a U.S. problem but a structural gap common to states across regime types, including those that have adopted far more intrusive prevention and authority measures than the U.S. Constitution permits.⁴ If terminal interdiction cannot be relied upon anywhere, the achievable share of the risk must be managed through authority, coordination, and pre-launch measures — which is where the U.S. seams analyzed here become decisive. Paper II's finding also identifies the variable that matters: terminal defense succeeds when the defender has warning time and fails when it does not, and the adjacent launch is the case that removes it.

The paper proceeds as follows. Part 2 states scope, method, and sources. Part 3 positions the contribution relative to the existing C-UAS legal literature. Part 4 summarizes the threat to the extent necessary for the legal analysis to stand alone. Part 5 sets out the post-SAFER SKIES authority structure and its six residual seams. Part 6 consolidates the findings. Part 7 evaluates oversight and legislative options. Parts 8 and 9 state limitations and conclude.

2. Scope, Method, and Sources

Scope. This paper assesses the threat posed by small UAS employed as a close-access strike system against protected persons in the NCR and evaluates the adequacy of the post-SAFER SKIES C-UAS authority framework to counter it. It is a legal and policy analysis; the technical and comparative dimensions are treated in the companion papers.

Threat model. The series addresses one threat class — small unmanned aircraft operating at low altitude and short standoff against protected persons and sites. Paper I establishes the capability as it exists globally; Paper II addresses the defender's problem against low, slow, small platforms over populated areas; and this paper addresses the lone domestic actor launching close-in from private property near a protected site in the NCR. The variable that joins them is warning time: Paper I shows that the capability

4. Collin George, *The Terminal Residual: Warning Time and the Structural Limits of Small-UAS Defense* (Drone Threats to Political Leadership: Capability, Defense, and Authority, Paper II) (forthcoming 2026) (developing the finding that terminal defense against this threat is a structural gap across regime types).

compresses it, Paper II shows that terminal defense fails when it collapses, and this paper shows where U.S. law leaves it collapsed.

Deliberate exclusions. The paper contains no operational method: no airframe or payload specifications, no flight-planning or navigation tradecraft, no concealment or evidence-defeat techniques, and no concept of operations for defeating a protective detail. Threat characterization is presented only at the level of generalized capability necessary to size the legal problem. Where the mechanics of an attack are relevant, they are described solely as constraints on the defender's detection and engagement timeline. Content that would provide operational uplift is out of scope irrespective of framing.

Sources. The analysis rests exclusively on open-source primary materials — statutory text, the enrolled public law, agency rulemakings in the Federal Register, GAO products, congressional hearing records, and Department of Justice charging announcements. It incorporates no classified information and no non-public human sourcing. Citations follow The Bluebook.

Estimative language. Confidence levels (high / moderate / low) and estimative terms follow the Intelligence Community analytic-standards convention under ICD 203.⁵ Analyst confidence and likelihood are stated separately and are not combined within a single expression.

Status of underlying law. The SLTT framework is governed by an interim final rule whose comment period closed 4 September 2026; the rule may change on finalization. Statutory citations reflect the U.S. Code as amended through Pub. L. No. 119–60. Alleged criminal conduct described herein derives from charging instruments and is not adjudicated.

3. Prior Literature and Contribution

The legal literature on domestic counter-UAS authority has developed largely in response to the recurring, short-horizon reauthorizations of the Preventing Emerging Threats Act of 2018 and the associated Congressional Research Service and Government Accountability Office reporting on the detection-to-mitigation gap.⁶ That body of work is framed predominantly around the adequacy of federal mitigation authority in the abstract and around the mass-gathering and critical-infrastructure use cases emphasized in agency testimony. It has not, to date, isolated the adjacent-structure launch vector against protected persons as a distinct doctrinal problem, nor analyzed how the post–SAFER SKIES authority structure interacts with the three separate legal regimes — foreign-investment screening, airspace regulation, and counter-UAS mitigation — that together govern the airspace and property around leadership sites.

This paper's contribution is to reframe the question from the adequacy of any single authority to the seam among all three regimes, and to show that the residual risk is concentrated where those regimes fail to meet. To the author's knowledge, no prior scholarship analyzes the adjacent-structure launch vector as a seam among the CFIUS real-estate, National Capital Region airspace, and § 124n counter-UAS regimes, and none has examined the post–SAFER SKIES authority structure in this respect. Legal analysis of

⁵. Intelligence Community Directive 203, Analytic Standards (ODNI, Jan. 2, 2015). Likelihood (probability of occurrence) and analyst confidence (source quality/quantity) are distinct and are not combined within a single expression.

domestic counter-UAS authority has appeared chiefly in Congressional Research Service products, practitioner and academic commentary, and congressional testimony; sustained law-review treatment remains limited. In doing so it connects a homeland-security-law analysis to the technology-maturity and comparative-effectiveness findings developed in the companion papers, situating a U.S.-specific statutory problem within a threat that is demonstrably real and structurally difficult to defend against.

4. The Threat in Brief

The adjacent-elevated-structure vector is the analytically hardest case for a protective service precisely because it inverts the core assumptions the defense is built on. Perimeter security assumes the threat approaches from outside a controlled footprint; this vector originates within a structure the government does not control and never crosses the perimeter. Airspace defense assumes warning time proportional to standoff distance; this vector collapses that distance to a few hundred meters, compressing the detect-classify-decide-engage sequence below what a lawful decision loop can reliably execute over a populated area. Attribution assumes evidence at or near the scene; an autonomous platform leaves an operator nowhere near it. The incident record confirms the pattern is not hypothetical: drones have reached the White House grounds, the Kremlin's dome, a fortified Baghdad compound, the Israeli Prime Minister's residence, and a head of state mid-speech in Caracas — incidents documented in Papers I and II of this series. The vulnerability is not a failure of any single agency's competence; it is the predictable result of a threat geometry that no current authority structure was designed to cover.

The threat is developed in full in Paper I; it is summarized here only to the extent the legal analysis requires. Three points suffice. **First, the capability is mature.** Commercial platforms now combine autonomous or pre-programmed waypoint navigation with low size, weight, and power, so that a lone actor can field a drone that flies a fixed profile to a fixed point without emitting the command-and-control signature on which most radio-frequency detection and mitigation depend. Two of the most mature C-UAS sensing modalities — RF detection of the control link and RF or GNSS disruption of it — degrade against a platform that neither listens nor transmits during its terminal phase.

Second, proximity and elevation define the hardest variant. A launch point on or within a structure that holds a direct line of sight onto a protected site minimizes the slant distance the platform must traverse,

and therefore the time available to detect and engage it; places the launch below or outside the coverage geometry optimized for perimeter and airspace approaches; and removes the actor from the protected site's access-controlled footprint entirely. The decisive terrain feature is a private structure with an unobstructed sightline — not the government-controlled fence line.

Third, the vector is corroborated, not hypothetical. In the July 2024 Butler attack on former President Trump, then a candidate, the shooter fired from the rooftop of a building adjacent to the rally site — the adjacent-structure geometry in its plainest form — and had flown a drone over the site roughly two hours earlier, a flight the Secret Service never detected;⁷ in 2026 the Department of Justice charged a group of men — eight defendants by a July 2026 federal grand-jury indictment — in an alleged plot, disrupted at the planning stage, to deploy explosive-laden drones to force an evacuation at a White House-grounds event and then engage the fleeing crowd with snipers⁸; a September 2026 Government Accountability Office report found a multi-year lag in protective-policy adaptation to drone incidents.⁹ Two other 2026 matters — a charged attempt to assassinate the President at the White House Correspondents' Dinner and a May 2026 shooting at Secret Service agents near the Washington Monument — involved no drone and are noted only as context for the protective environment, not as corroboration of the vector.¹⁰ These are

6. The component literatures exist separately. On § 124n and domestic C-UAS authority: Cong. Rsch. Serv., R48477, Department of Defense Counter-Unmanned Aircraft Systems: Background and Issues for Congress (2025), and CRS IF13279 (July 29, 2026) (SLTT C-UAS regulation), IN12661 (Feb. 27, 2026), and IN12476 (Jan. 3, 2025); and, on the SAFER SKIES structure, Lawfare analyses including “The Counter-UAS Certification Bottleneck” (Philip W. Rohlffing, June 23, 2026), “Closing the Title 32 Gap in Domestic Counter-UAS Authority” (Philip W. Rohlffing, June 15, 2026), “Are Domestic Drone Shoot-Downs Lawful?” (Ashley Deeks & Madison Rinder, Feb. 5, 2025), and “Drone Threats Are Evolving; Data Retention Rules Are Not” (Philip W. Rohlffing, May 6, 2026); and Defending Against Drones: Setting Safeguards for Counter Unmanned Aircraft Systems Authorities, Hearing Before the S. Comm. on the Judiciary, 119th Cong. (May 20, 2025) (statement of Laura K. Donohue, Georgetown Univ. Law Ctr.). On CFIUS real estate: 31 C.F.R. pt. 802 and the Nov. 7, 2024 final rule (89 Fed. Reg. 88128), framed around foreign intelligence collection and espionage — see Richard A. Newman, ArentFox Schiff, “CFIUS 2.0: Real Estate as a Platform for Foreign Espionage Against the US Government?” (Sept. 12, 2019) (2019 background analysis, predating the 2026 events) — not a kinetic launch-platform vector. On the close-in launch record: DHS Off. of Inspector Gen., OIG-26-13 (June 30, 2026) (finding the Secret Service never detected the Butler drone flight; the counter-drone system was staffed by a single under-trained operator and was inoperable during the flight), contrasted with Don Rassler, “Going the Distance: The Emergence of Long-Range Stand-Off Terrorism,” CTC Sentinel 17:2 (Feb. 2024). Press reporting in August 2026 on a commercial-property acquisition near the White House indicates that the adjacent-structure concern has entered public discourse; consistent with Part 5.6, this paper does not identify the property or the parties. See also GAO-22-105705 (2022).

7. U.S. Dep't of Homeland Sec., Off. of Inspector Gen., OIG-26-13 (June 30, 2026) (the Secret Service “never detected Crooks’ drone flight, its location, or his location”; the counter-UAS system was staffed by a single operator with roughly 20 minutes of informal training and was inoperable during Crooks’ flight because of a technical fault, with the operator awaiting technical support); Testimony of FBI Director Christopher Wray before the H. Comm. on the Judiciary (July 24, 2024) (drone flown about 200 yards from the stage for about 11 minutes, roughly two hours before the rally). OIG-26-13 describes a flight of almost nine minutes beginning at 3:51 p.m.; the sources differ on duration, not on the fact of non-detection.

8. Press Release, U.S. Dep't of Justice, Five Men Arrested and Charged in Plot to Attack and Kill Government Officials and Others Attending the Ultimate Fighting Championship at White House (June 16, 2026), superseded by a federal grand-jury indictment returned July 9, 2026 in the Southern District of Ohio charging eight defendants with conspiracy to provide material support to terrorists and conspiracy to commit murder on federal government territory (a ninth individual was indicted separately in the Eastern District of California on Aug. 27, 2026 on firearm-possession and records-destruction charges, not the conspiracy counts). Allegations in charging instruments; the plot was disrupted at the planning stage; not adjudicated.

9. U.S. Gov't Accountability Office, Secret Service: Protection Policies Should Be Consistently Updated to Better Ensure Protectee Safety, GAO-26-108455 (Sept. 3, 2026) (of 83 security incidents FY2015–FY2025, policies were updated after 25; the report identifies drone incidents from 2015 to 2021 that produced no policy change before the July 2024 Butler attack).

10. Press Release, U.S. Dep't of Justice, Suspect in White House Correspondents' Dinner Shooting Charged with Attempt to Assassinate the President (Apr. 2026); and reporting on the May 4, 2026 incident in which a man fired at Secret Service agents near the Washington Monument and was shot by agents (CNN, May 4, 2026); the Washington Post later reported that he had walked along the path of the Vice President's motorcade (May 6, 2026). Allegations only; not adjudicated.

allegations or findings in the cited instruments and are treated as such. Attribution against an autonomous platform is inherently weak (unidentified drones operated intermittently over Langley Air Force Base for seventeen days in December 2023 without public attribution),¹¹ which shifts deterrence value left of the event, a point that reinforces the authority and pre-launch analysis below rather than the prospect of after-the-fact identification.

5. The Post–SAFER SKIES Authority Structure and Its Seams

5.1 Current authority baseline

Four authority layers bear on this threat in the NCR; three operate through § 124n. First, the core mitigation authority under 6 U.S.C. § 124n permits designated federal actors (principally DHS and DOJ components) to take mitigation actions against credible UAS threats to covered facilities and assets, notwithstanding a series of federal criminal prohibitions — aircraft-piracy, aircraft-destruction, computer-fraud, satellite-interference, Wiretap Act, and pen/trap statutes.¹² The FY2026 NDAA extended federal authority to 30 September 2031.¹³ Second, the U.S. Secret Service’s protective mission under 18 U.S.C. §§ 3056 and 3056A brings the White House complex, the Vice President’s residence, and designated National Special Security Events within the § 124n covered-facility definition; the mitigation authority itself flows from § 124n, while §§ 3056/3056A supply the protective mission that qualifies the site.¹⁴ Third, and newly, the SAFER SKIES Act amended § 124n to authorize SLTT law-enforcement and correctional agencies to detect, track, seize, disable, or destroy drones posing a credible threat, contingent on a DOJ/DHS training and certification regime and use of federally authorized equipment.¹⁵

The SLTT framework is governed by a joint DOJ/DHS interim final rule effective 1 July 2026 (published 6 July 2026), which establishes a two-tiered certification structure (a detection/warning tier and a more restrictive mitigation tier), mandates use of technologies and systems on federally maintained authorized lists, requires airspace and spectrum coordination, and imposes a 48-hour post-mitigation reporting requirement.¹⁶ The rule expressly notes that SAFER SKIES did not waive the Communications Act’s

¹¹. Pentagon officials confirmed the Langley incursions in October 2024 following Wall Street Journal reporting. See Pentagon confirms that unidentified drones flew over Langley Air Force Base over 17 days last December, *13NewsNow* (Oct. 2024).

¹². Statutes from which § 124n provides relief for authorized actors: 49 U.S.C. § 46502 (aircraft piracy); 18 U.S.C. § 32 (destruction of aircraft); § 1030 (computer fraud); § 1367 (interference with satellite operations); ch. 119 (Wiretap Act, §§ 2510 et seq.); ch. 206 (pen register/trap-and-trace, §§ 3121 et seq.).

¹³. Supra note 3 (6 U.S.C. § 124n(j)(1)).

¹⁴. 18 U.S.C. §§ 3056, 3056A (Secret Service protective mission); 6 U.S.C. § 124n(l)(3) (defining “covered facility or asset” to include USSS protection operations “pursuant to sections 3056(a) and 3056A(a) of title 18”). C-UAS mitigation authority itself derives from § 124n; §§ 3056/3056A supply the protective mission that renders a site a covered facility or asset.

¹⁵. SAFER SKIES Act § 8602 (extending mitigation authority to SLTT law-enforcement and correctional agencies, amending 6 U.S.C. § 124n); §§ 8603–8604 (UAS/C-UAS grant eligibility); § 8605 (enforcement — enhanced penalties for drone-facilitated offenses, codified at 6 U.S.C. § 124n-1(c), and a Sentencing Commission directive at § 8605(e); § 8605(f) civil penalty up to \$100,000 per violation, or suspension of authority, for knowingly taking counter-UAS action without required federal coordination; § 8605(g) civil action by the Attorney General to collect); § 8606 (rulemaking).

¹⁶. Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies, 91 Fed. Reg. 41466 (July 6, 2026) (interim final rule; effective July 1, 2026; codified at 6 C.F.R. pt. 124 and 28 C.F.R. pt. 124; comment period closed Sept. 4, 2026). Civil penalty implemented at 6 C.F.R. § 124.16 and 28 C.F.R. § 124.16; two-tiered certification (online detection/warning certification; resident mitigation training at the FBI National Counter-UAS Training Center); Authorized Technologies List and Authorized Systems List (§ 124.7); 48-hour post-mitigation report (§ 124.13).

spectrum provisions, so RF-based mitigation remains subject to FCC coordination. On 2 July 2026 five FCC bureaus and offices, acting jointly, granted a 180-day special temporary authority for SLTT counter-UAS operations that comply with the SAFER SKIES Act, and the Wireless Telecommunications Bureau issued a companion declaratory ruling that SLTT agencies operating in compliance with the Act are exempt from liability under 47 U.S.C. § 333; SLTT spectrum authority therefore rests, as of this writing, on a temporary instrument that expires in late December 2026 unless extended.¹⁷ The statute also imposes a civil penalty of up to \$100,000 per violation, or suspension of authority, for knowingly taking C-UAS action without the required federal coordination; the rule states that other violations do not give rise to civil penalties.¹⁸ These provisions are a deliberate governor on the proliferation of mitigation authority; they are also, for the adjacency scenario, part of the timeline problem analyzed below.

A fourth layer sits outside § 124n. The Department of Defense holds parallel counter-UAS authority for its own covered facilities and assets under 10 U.S.C. § 130i, which the FY2026 NDAA amended to authorize tracking by Remote ID broadcast and to require an annual public report, alongside a separate facility-protection pilot program; the section's relief from enumerated title 18 provisions and its forfeiture authority predate the amendment. Department-level policy has also moved: an 8 December 2025 memorandum, Updated Guidance for Countering Unmanned Aircraft Systems in the Homeland, consolidated roughly ten prior memoranda and extends defensive action beyond installation fence lines.¹⁹ Several § 130i-covered installations lie within the NCR, but the authority attaches to Defense facilities and missions, not to civilian protective sites, and because it runs to "members of the armed forces" it does not on its face reach National Guard personnel serving in Title 32 status — a gap identified in commentary rather than in express statutory text.²⁰ The Guard gap matters for the adjacency case because the Guard is a force likely to be physically present near protected sites without holding mitigation authority.

The airspace layer has also moved. Drone operations in the Washington Flight Restricted Zone are governed by an FAA security notice issued under 14 C.F.R. § 99.7, which prohibits recreational operation inside the FRZ, permits it in the surrounding SFRA only under enumerated conditions, and requires FAA authorization for civil and commercial operations anywhere in the SFRA.²¹ Executive Order 14305 directed the FAA to accelerate the long-delayed rule implementing § 2209 of the FAA Extension, Safety,

¹⁷. Supra note 16. The IFR states that the SAFER SKIES Act did not waive the Communications Act's spectrum provisions; SLTT mitigation using RF-based systems therefore remains subject to FCC coordination. See Fed. Comm'n's Comm'n, Order, DA 26-656 (July 2, 2026) (Wireless Telecommunications Bureau, Office of Engineering and Technology, Public Safety and Homeland Security Bureau, Space Bureau, and Media Bureau, jointly granting 180-day special temporary authority for SLTT counter-UAS operations); DA 26-655 (July 2, 2026) (declaratory ruling on 47 U.S.C. § 333).

¹⁸. Supra note 15 (§ 8605(f)).

¹⁹. 10 U.S.C. § 130i, as amended by National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, § 1707 (2025) (adding "including through the use of remote identification broadcast or other means" to § 130i(b)(1)(B) and converting periodic briefings to an annual publicly posted report); see also id. § 1089 (pilot program for accelerating protection of certain facilities and assets from unmanned aircraft). Relief from 18 U.S.C. §§ 32, 1030, 1367 and chs. 119 and 206, and forfeiture authority under § 130i(c), predate the amendment. On the Dec. 8, 2025 guidance, see Dep't of Def. (styled Dep't of War), Fact Sheet: C-UAS Policy in the U.S. Homeland (Feb. 10, 2026). Executive-branch documents issued since late 2025 style the Department as the "Department of War"; statutory references remain to the Department of Defense.

²⁰. On the Title 32 gap, see Philip W. Rohlfing, Closing the Title 32 Gap in Domestic Counter-UAS Authority, *Lawfare* (June 15, 2026).

²¹. FAA, Notice to Air Missions FDC 4/1783 (UAS operations in the Washington, D.C. Special Flight Rules Area and Flight Restricted Zone) (issued under 49 U.S.C. § 40103(b)(3) and 14 C.F.R. § 99.7; cancelling FDC 9/1811). On criminal prohibitions reaching non-cooperative operators, see 49 U.S.C. § 46307; SAFER SKIES Act § 8605 (repeat § 46307 violations); 18 U.S.C. § 39B; 18 U.S.C. § 1752.

and Security Act of 2016, required agency access to Remote ID data, and ordered revision of the 2020 interagency advisory on detection and mitigation technology;²² the FAA proposed the § 2209 rule — a new 14 C.F.R. part 74 establishing standard and special flight restrictions over critical infrastructure and other sites — on May 6, 2026; the comment period, extended once, closed August 5, 2026.²³ Criminal law does reach the non-cooperative operator: knowing or willful violation of national defense airspace is an offense under 49 U.S.C. § 46307, which SAFER SKIES made a felony on repeat violation; unsafe operation of an unmanned aircraft is punishable under 18 U.S.C. § 39B; and an operator physically present on restricted grounds is punishable under 18 U.S.C. § 1752. These provisions punish after the fact; they neither detect nor interdict. Each of the instruments above therefore regulates, identifies, or deters operators; none changes the physics of a non-cooperative launch.

Mapped to the three defensive columns of Paper II, the seams below fall as follows: seams (b) and (c) and part of (a) lie chiefly in detection; seam (d) and the remainder of (a) lie in terminal mitigation; and seams (e) and (f) lie in prevention — the column Paper II identifies as the one in which national choices actually move risk.

5.2 Residual seam (a): implementation lag in the NCR

SLTT mitigation authority exists in statute but converts to fielded capability only through certification, equipment authorization, and coordination protocols that opened, at the earliest, in mid-2026; the interim final rule itself had not been finalized as of this writing. The operative question is empirical: which NCR-area jurisdictions have completed certification, hold authorized equipment, and have pre-coordinated engagement protocols with the Secret Service and DHS for a launch originating from private property adjacent to a protected site? Until that pipeline is demonstrably operational in the NCR, the newly granted authority does not yet reduce risk in the scenario of concern (**moderate confidence, pending oversight data**).

5.3 Residual seam (b): no authority for private adjacency

The FY2026 provisions governing critical-infrastructure and SLTT grant eligibility do not extend mitigation authority to private owners or occupants of adjacent structures.²⁴ An owner of the very building that provides the decisive sightline has no lawful authority to detect via restricted means or to mitigate, and remains exposed to the federal criminal prohibitions § 124n waives only for authorized government actors. The 2020 interagency advisory counsels that even detection technologies may implicate the Wiretap Act and the pen/trap statute depending on how they operate, and it has not been revised despite Executive Order 14305's direction; the Department of Justice's June 12, 2026 charging policy concerning defensive actions against UAS bears on how that exposure is exercised in practice and must be assessed against the adjacency case before any legislative option is framed.²⁵ The result is a coverage seam precisely where the threat geometry most favors an attacker: the private elevated structure is

²². Exec. Order No. 14305, Restoring American Airspace Sovereignty, 90 Fed. Reg. 24719 (June 11, 2025) (signed June 6, 2025).

²³. FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114–190, § 2209; Designation—Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility, 91 Fed. Reg. 24650 (proposed May 6, 2026) (Docket No. FAA-2026–4558; proposing 14 C.F.R. pt. 74); comment period extended from July 6 to Aug. 5, 2026, 91 Fed. Reg. 39568 (June 30, 2026).

²⁴. Supra note 15.

simultaneously the best launch position and the location least covered by any mitigation authority (**high confidence**).

5.4 Residual seam (c): privately owned airspace and structure coordination

Federal mitigation authority attaches to covered facilities and assets and to authorized actors; it does not resolve who is sensing, who is authorized to act, and on what timeline, when the threat originates from private property outside the federal protective perimeter but within terminal range of a protected person. The low-altitude airspace immediately above and around privately owned adjacent structures in the NCR is a jurisdictional and sensing seam: Secret Service coverage is optimized around the protected site, SLTT authority is new and geographically uneven, and no actor holds an unambiguous, pre-coordinated mandate to persistently sense and rapidly mitigate a threat emerging from that specific volume (**moderate-to-high confidence**).

5.5 Residual seam (d): the engagement timeline may fall below the decision loop

This is the most consequential seam and the one least addressed by any current authority. Lawful mitigation presumes a sequence: detect, classify, confirm a credible threat, identify the authorized actor, and execute mitigation consistent with coordination and safety constraints in a dense urban environment where kinetic options are heavily constrained by the presence of people and structures — and, for SLTT actors, subject to FCC spectrum coordination and post-action reporting.²⁶ A terminal profile flown from an adjacent elevated structure can compress the interval between first detectability and effect below the time that sequence realistically requires. Authority to mitigate is necessary but not sufficient; if the lawful decision loop is slower than the threat's terminal timeline, the authority cannot be exercised in time (**moderate confidence**). The burden shifts onto pre-launch detection and pre-delegated, pre-coordinated engagement authority — neither of which the current framework guarantees for the adjacency case. Consistent with Paper II, measures directed at this seam reduce decision latency within a column that cannot be closed; they are not a terminal solution.

5.6 Residual seam (e): no screening regime for sightline properties

No systematic physical-security regime screens the acquisition, lease, or occupancy of structures holding direct sightlines onto protected persons and facilities in the NCR. CFIUS holds real-estate jurisdiction under FIRRMA and 31 C.F.R. pt. 802 over certain transactions near enumerated sensitive facilities, and Treasury expanded that coverage in November 2024 by adding 59 installations.²⁷ No leadership site is among the covered sites: Appendix A to part 802 lists no entry for the White House, the Eisenhower Executive Office Building, the Naval Observatory, or the Capitol, and its District of Columbia entries are

²⁵. U.S. Dep't of Justice, Fed. Aviation Admin., Fed. Comm'n's Comm'n & U.S. Dep't of Homeland Sec., Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems (Aug. 17, 2020); U.S. Dep't of Justice, Charging Policy Concerning Defensive Actions Against Unmanned Aircraft Systems (June 12, 2026).

²⁶. Supra notes 15–16 (post-mitigation reporting under 6 U.S.C. § 124n(d)(2)(C)(i); FCC spectrum coordination).

²⁷. Provisions Pertaining to Certain Transactions by Foreign Persons Involving Real Estate in the United States, 89 Fed. Reg. 88128 (Nov. 7, 2024) (effective Dec. 9, 2024) (adding 59 military installations to 31 C.F.R. pt. 802 app. A — 40 at the one-mile radius, 19 at the 100-mile radius — moving 8 existing installations from Part 1 (one-mile) to Part 2 (100-mile) coverage, and removing 3; Treasury stated no aggregate total).

Defense installations. But that jurisdiction is transaction-triggered, proximity-based, and foreign-nexus specific, and was designed to screen foreign-investment risk — not to serve as a protective-sightline screen.²⁸ The consequence is a counterintelligence and physical-security seam: acquisition or occupancy of an elevated adjacent structure — by a foreign-nexus or a domestic actor — is not systematically evaluated as a protective-security risk factor (**moderate confidence**). This paper treats the concern as an abstracted vulnerability pattern; it identifies no property or party and makes no allegation regarding any individual or transaction.

5.7 Residual seam (f): the prevention layer is voluntary and eroding

Paper II concludes that prevention is the column in which national choices move risk and that its transferable elements are constitutionally compatible.²⁹ In the NCR that column rests substantially on measures that are voluntary, dated, or in transition. Manufacturer geofencing, long a significant passive barrier around Washington, is no longer enforced: DJI converted its U.S. restricted zones to advisory warnings in January 2025 and extended the change to all remaining international markets in November 2025.³⁰ The Federal Communications Commission's December 2025 addition of all foreign-produced UAS and critical components to its Covered List bars new equipment authorizations but leaves the installed fleet — the platforms most available to a lone actor — in place; January 2026 exemptions for Blue UAS and qualifying domestic products, a conditional-approval path, and DJI's February 2026 challenge to its designation have since qualified, not reversed, that action.³¹ Remote ID has been enforceable since March 2024, but it identifies only compliant operators, and a non-compliant platform is precisely the one of concern.³² And the § 2209 site-restriction rule remains a proposal. The prevention measures that Paper II identifies as the achievable share of the risk are, in the NCR, largely unmandated (moderate-to-high confidence).

^{28.} 31 C.F.R. pt. 802, implementing FIRRMA and § 721 of the Defense Production Act, 50 U.S.C. § 4565. Appendix A includes NCR-region entries (e.g., Adelphi Laboratory Center, Adelphi, MD; Air Force Office of Scientific Research, Arlington, VA); the District of Columbia entries are Joint Base Anacostia–Bolling and the Naval Research Laboratory. Appendix A lists no leadership site (the White House, the Eisenhower Executive Office Building, the Naval Observatory, or the Capitol).

^{29.} Supra note 4.

^{30.} DJI, DJI Expands GEO System Update to Remaining International Markets (Nov. 17, 2025) (following the Jan. 13, 2025 U.S. change from Restricted Zones to Enhanced Warning Zones).

^{31.} Fed. Comm'n's Comm'n, Public Notice (Dec. 22, 2025) (adding foreign-produced UAS and UAS critical components to the Covered List following a national-security determination under the FY2025 NDAA); previously authorized models are not affected. See also FCC PSHSB Public Notice DA 26–22 (Jan. 7, 2026) (exemptions for Blue UAS Cleared List items and qualifying domestic end products through Jan. 1, 2027; conditional-approval path); DJI's Feb. 2026 challenges before the Commission and in federal court are reported in trade and law-firm commentary.

^{32.} 14 C.F.R. pt. 89; Press Release, FAA, FAA Ends Discretionary Enforcement Policy for Drone Remote Identification (Mar. 2024) (enforcement from Mar. 16, 2024).

6. Consolidated Findings

NO.	FINDING / JUDGMENT	ANALYST CONFIDENCE
CJ	Central Judgment: The three legal regimes touching the NCR — CFIUS real-estate review, the SFRA/FRZ/P-56 airspace regime, and § 124n C-UAS authority — each address a different axis (foreign investment, cooperative-operator compliance, active mitigation). Only § 124n is aimed at a non-cooperative drone, and against a close-in launch from a privately controlled adjacent structure it is limited by sensing coverage, coordination, and a decision loop the geometry can out-time.	High
F-1	Commercial sUAS with autonomous navigation and low signatures place a precision close-access strike capability within reach of a lone actor; RF-dependent detection and mitigation degrade against a platform with no active control link in its terminal phase.	High
F-2	Proximity and elevation — a private structure with a direct sightline onto a protected site — is the decisive geometry, minimizing warning time and placing the launch outside the federal access-controlled footprint.	High
F-3	Post-incident attribution is inherently weak against autonomous platforms; deterrence value shifts to pre-launch detection and to reducing the population of viable launch positions.	Moderate
F-4	Recent events (July 2024 Butler adjacent-rooftop attack and undetected pre-attack drone flight; 2026 charged White House-grounds plot; GAO-26-108455 adaptation-lag findings) corroborate the close-access thesis as a demonstrated pattern.	High (pattern); matters adjudicated
F-5	SAFER SKIES materially narrowed the headline authority gap, but SLTT mitigation capability in the NCR is limited by an implementation lag between statutory grant and fielded, coordinated capability.	Moderate*
F-6	No mitigation authority, and no authority to detect by legally restricted means, extends to private owners or occupants of the adjacent structures that provide the decisive sightline — the best launch position is the least-covered location.	High
F-7	No actor holds an unambiguous, pre-coordinated mandate to persistently sense and rapidly mitigate a threat emerging from the low-altitude airspace above and around privately owned adjacent structures; Secret Service coverage is optimized around the protected site, and SLTT authority is new and geographically uneven.	Moderate-High
F-8	The lawful detect-classify-decide-mitigate loop may be slower than the terminal timeline of a short-range launch from an adjacent structure; authority to mitigate cannot be exercised if the decision loop is out-timed.	Moderate
F-9	No systematic physical-security regime screens acquisition or occupancy of protective-sightline properties; CFIUS real-estate jurisdiction is transaction- and foreign-nexus specific and not designed for this purpose.	Moderate

NO.	FINDING / JUDGMENT	ANALYST CONFIDENCE
F-10	The NCR prevention layer — manufacturer geofencing, Remote ID, site-restriction rules — is voluntary, eroding, or not yet in force; the column Paper II identifies as the achievable share of risk is largely unmandated.	Moderate-High

** Confidence pending oversight data on NCR-jurisdiction certification and coordination status. Confidence levels reflect source quality under ICD 203 (supra note 5) and are stated separately from any likelihood judgment.*

7. Policy Implications and Legislative Options

The options below are ranked. Three legislative measures are priority recommendations and lead Part 7.2; the remainder are supporting measures. Each targets a specific seam identified in Part 5 and a finding in Part 6.

7.1 Oversight and executive-branch inquiry

- A classified briefing from the Secret Service, DHS, and DOJ on C-UAS coverage of privately owned airspace and structures adjacent to protected sites in the NCR, and specifically on the engagement timeline against a terminal profile launched from an adjacent elevated structure (addresses CJ, F-2, F-7, F-8).
- Certification and coordination status for NCR-area SLTT agencies under the SAFER SKIES interim final rule, including whether pre-coordinated engagement protocols exist for the adjacency case and whether FCC spectrum-coordination requirements introduce latency in a compressed timeline (addresses F-5, F-8).³³
- An interagency view on whether the 48-hour reporting and federal-coordination requirements are compatible with a terminal timeline measured in seconds, and whether pre-delegated engagement authority for designated high-risk zones is warranted (addresses F-8).
- The DHS/USSS response to GAO-26–108455 on drone-incident policy adaptation, and whether adjacent-structure launch is addressed in current protective doctrine (addresses F-4).³⁴
- The status of the revision of the 2020 interagency advisory directed by Executive Order 14305, and the application of the Department of Justice’s June 12, 2026 charging policy to detection by owners and occupants of adjacent structures (addresses F-6).

7.2 Legislative options

- Priority 1. A statutory geo-awareness requirement for UAS sold or operated in the United States covering a defined national-security site list, converting into a mandate the manufacturer geofencing that was withdrawn voluntarily in 2025 (addresses F-10).

³³. Supra note 16.

³⁴. Supra note 9.

- Priority 2. Direction to the FAA to finalize the § 2209 rule with an express designation pathway for leadership protective sites in the NCR, and to publish those restrictions in machine-readable form for manufacturer geo-awareness, as Executive Order 14305 contemplates (addresses F-10).
- Priority 3. A pre-coordinated mitigation and persistent-sensing framework for designated high-risk protective zones in the NCR that expressly covers privately owned adjacent airspace and structures, with civil-liberties and airspace-safety safeguards, framed as a reduction in decision latency rather than a terminal solution (addresses CJ, F-2, F-6, F-7, F-8).
- A limited, safeguarded pathway for authorized detection (not mitigation) by private critical-infrastructure and adjacent-structure owners in designated zones, tied to information-sharing with the Secret Service and DHS (addresses F-6).
- A study — by GAO or a federally funded research and development center — of a protective-sightline screening regime for acquisition, lease, or occupancy of structures with direct sightlines onto protected sites, including whether CFIUS pt. 802 covered-site coverage should be extended or a separate physical-security mechanism established (addresses CJ, F-9).³⁵
- Prioritization of appropriations and authorities toward left-of-launch detection and forensic-attribution capability rather than post-incident mitigation hardware alone (addresses F-1, F-3).
- Resourcing for Remote ID enforcement and receiver coverage within the SFRA and FRZ, with protective-agency access to Remote ID data under Executive Order 14305 (addresses F-3, F-10).
- Monitoring of H.R. 5061 (Counter-UAS Authority Security, Safety, and Reauthorization Act) as a potential vehicle for adjacency-specific reforms; the core § 124n authorities were already extended by the SAFER SKIES Act in the FY2026 NDAA, and because H.R. 5061's central SLTT policy was enacted through SAFER SKIES, its value as a vehicle is now limited to residual provisions (addresses framework gaps generally).³⁶

8. Limitations and Scope Conditions

- **Regulatory currency.** The SLTT framework rests on an interim final rule whose comment period closed 4 September 2026; section-level requirements may change on finalization.³⁷
- **Unadjudicated matters.** The 2026 plots and attempts cited are allegations in charging instruments, not convictions, and are characterized as such.³⁸

^{35.} Supra note 27.

^{36.} H.R. 5061, 119th Cong. (2025), Counter-UAS Authority Security, Safety, and Reauthorization Act (introduced Aug. 29, 2025; ordered reported 60–0 by the House Committee on Transportation and Infrastructure, Sept. 3, 2025; no floor action as of this writing).

^{37.} Supra note 16.

^{38.} Supra note 8.

- **Open-source basis.** All capability claims derive from open sources and are pitched at the assessment level; any classified corroboration would be handled through appropriate channels and is outside this product.
- **Quantification.** The engagement-timeline finding (F-8) is qualitative by design; publishing operational parameters is out of scope.
- **CFIUS list volatility.** 31 C.F.R. pt. 802 Appendix A is updated at least annually; the covered-site figures reflect the November 2024 rule and should be reconfirmed before reliance.³⁹

9. Conclusion

The SAFER SKIES Act substantially narrowed the authority gap that oversight had identified since 2018, but it did not close the gap that matters most for leadership protection in the National Capital Region. The adjacent-structure launch vector remains in the seam among three legal regimes, only one of which is aimed at the threat, and that one cannot reliably be exercised in time, and the residual risk is concentrated precisely where an attacker's geometry is most favorable and the defender's authority least settled. Because the companion papers establish that the underlying capability is mature and that terminal defense against it is a structural gap across regime types, the policy question is not whether to acquire a decisive interdiction capability that does not exist, but how to allocate authority, coordination, and pre-launch measures to reduce the achievable share of the risk within constitutional constraints. The options set out above are directed to that end.

Appendix A. Authorities and Sources

Statutes and regulations

- 6 U.S.C. § 124n (as amended by the SAFER SKIES Act, Pub. L. No. 119–60, div. H, tit. LXXXVI, §§ 8601–8607 (2025)) — core C-UAS mitigation authority; federal sunset 30 Sep 2031; SLTT sunset 31 Dec 2031.
- SAFER SKIES Act §§ 8602 (SLTT authority), 8603–8604 (grant eligibility), 8605 (criminal & civil penalties), 8606 (rulemaking).
- Counter-UAS Authority for SLTT Law Enforcement and Correctional Agencies, 91 Fed. Reg. 41466 (July 6, 2026) (interim final rule; eff. July 1, 2026; 6 C.F.R. pt. 124; 28 C.F.R. pt. 124).
- 18 U.S.C. §§ 3056, 3056A (USSS protective mission); 6 U.S.C. § 124n(l)(3) (covered-facility definition).
- Relief statutes: 49 U.S.C. § 46502; 18 U.S.C. §§ 32, 1030, 1367; 18 U.S.C. ch. 119 (§§ 2510 et seq.); ch. 206 (§§ 3121 et seq.).
- FIRRMA; 31 C.F.R. pt. 802 (CFIUS real estate); 89 Fed. Reg. 88128 (Nov. 7, 2024) (adding 59 installations).
- 14 C.F.R. pt. 93, subpt. V (DC SFRA/FRZ); Prohibited Area P-56A/B.

³⁹. Supra note 27.

- 10 U.S.C. § 130i (as amended by Pub. L. No. 119–60, § 1707); FAA NOTAM FDC 4/1783 (14 C.F.R. § 99.7); 14 C.F.R. pt. 89 (Remote ID); Pub. L. No. 114–190, § 2209, and proposed 14 C.F.R. pt. 74, 91 Fed. Reg. 24650 (May 6, 2026), comment period extended, 91 Fed. Reg. 39568 (June 30, 2026); Exec. Order No. 14305, 90 Fed. Reg. 24719 (2025).
- DOJ/FAA/FCC/DHS Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate UAS (Aug. 17, 2020); DOJ Charging Policy Concerning Defensive Actions Against UAS (June 12, 2026); FCC Covered List action (Dec. 22, 2025).
- H.R. 5061, 119th Cong. (2025) — pending reauthorization/reform bill.

Reports, hearings, and charging announcements

- GAO-26–108455, Secret Service: Protection Policies Should Be Consistently Updated to Better Ensure Protectee Safety (Sept. 3, 2026).
- DHS Off. of Inspector Gen., OIG-26–13 (June 30, 2026) (Butler counter-UAS performance).
- Securing the Skies: Law Enforcement, Drones, and Public Safety, Hearing Before the S. Comm. on the Judiciary, 119th Cong. (July 22, 2025).
- U.S. Dep’t of Justice charging materials — June 16, 2026 complaint and July 9, 2026 eight-defendant indictment (S.D. Ohio) in the White House-grounds UFC drone plot; 2026 White House Correspondents’ Dinner and Washington Monument matters (no drone nexus; context only).

Analytic standards

- Intelligence Community Directive 203, Analytic Standards (ODNI, Jan. 2, 2015).

Companion papers in this series

- George, C. Not Science Fiction: The Maturation of Small-UAS as a Precision Weapon (Paper I, forthcoming 2026).
- George, C. The Terminal Residual: Warning Time and the Structural Limits of Small-UAS Defense (Paper II, forthcoming 2026).

DISCLOSURE

Author's Statement on Sources and Independence

This paper was prepared in the author’s personal capacity and is not official U.S. government analysis. It relies exclusively on publicly available sources, each cited. In the author’s assessment it contains no classified information, no Controlled Unclassified Information, and no technical data or technology controlled under the ITAR or EAR; operational method, targeting, and build detail are deliberately omitted. The work was self-initiated and self-funded. No client, government, or foreign principal requested, directed, funded, or reviewed it. Inquiries: <https://sanctir.com/contact/>

ABOUT THE AUTHOR

Collin George is the founder of Sanctir LLC, where he advises on national security, export control, and compliance. He holds the CISSP. Correspondence: <https://sanctir.com/contact/>.

ORCID 0009-0007-8162-6839

SUGGESTED CITATION

Collin George, *The Adjacent-Launch Seam: Counter-UAS Authority Gaps in the National Capital Region*, Sanctir Working Paper WP-2026-D3 (2026-10-01), *Drone Threats to Political Leadership: Capability, Defense, and Authority*, Paper III, v1.6.

Keywords: counter-UAS; C-UAS; unmanned aircraft systems; drones; National Capital Region; executive protection; SAFER SKIES Act; 6 U.S.C. § 124n; homeland security law; national security law; critical infrastructure protection; CFIUS.