IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Michael Lemmon, *et al.*, Plaintiffs, v. Donald J. Trump, *et al.*, Defendants.	No. 1:26-cv-00544

DECLARATION OF MARKWAYNE MULLIN

I, Markwayne Mullin, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. This declaration is based on my personal knowledge and information made available to me in the course of my official duties.
2. I am the Secretary of Homeland Security, and I have served in that position since March 2026. In this role, I am responsible for overseeing Department-wide strategy, technology investment, interoperability, and interagency coordination to address Unmanned Aircraft Systems (UAS) threats while enabling legitimate UAS integration.
3. The commercially available and recreational UAS market is experiencing rapid growth in the United States, with the commercial fleet alone projected to reach up to 1.015 million units by 2027. Import data suggests that current Federal Aviation Administration registration numbers significantly underestimate the true size of the recreational fleet, meaning the actual number of hobbyist drones in operation is likely much higher than official estimates.
4. This mass proliferation of UAS increases the presence of authorized and beneficial operations while simultaneously raising the risk of unauthorized or nefarious use within the federal National Capital Region (NCR). Securing this airspace is exceptionally difficult for the five federal agencies—namely, DHS, the Central Intelligence Agency (CIA), the Department of

Justice (DOJ), the Department of War (DOW), and the Department of Energy (DOE)—that possess the explicit statutory authority to lawfully conduct Counter-Unmanned Aircraft Systems (C-UAS) detection and mitigation operations.

5. These agencies face significant challenges in differentiating authorized UAS from potential threats in the NCR due to critical limitations in domain awareness, technology, and interagency coordination. Current detection technologies and their deployment must continually evolve to ensure detection of all UAS activity, a challenge expected to grow as advancements in autonomy, telecommunications, and physical design make these systems increasingly difficult to track. This detection challenge is further compounded by a lack of tracking infrastructure, such as Remote ID, and the absence of unified databases. Consequently, authorized agencies often have to make threat determinations independently, using varying definitions, independently gathered information, and undocumented criteria. This siloed approach prevents efficient information sharing and collaborative defense, forcing agencies to make critical security decisions with incomplete information.

6. Further exacerbating this detection challenge, the NCR's current airspace protection strategies were designed in the aftermath of September 11, 2001, and focus primarily on identifying and defending against large, fast-moving, manned aviation threats. These traditional point-defense strategies and geographic boundaries, such as the Washington, D.C. Flight Restricted Zone (FRZ), rely on speed and notification margins that do not readily translate to UAS, which are typically smaller, highly maneuverable, and capable of launching from almost anywhere. Therefore, small Unmanned Aircraft Systems (sUAS) specifically present a unique and concerning threat to the NCR, an electronically cluttered urban environment, based on their size and the incompatibility of our current airspace protection strategies.

7. The NCR security environment is uniquely complex, multi-domain, and continuously evolving, requiring a highly coordinated law enforcement and protective security posture. Within this prominent and high-visibility jurisdiction, critical infrastructure, federal personnel, and public venues face a sophisticated array of security challenges. These challenges include unauthorized or malicious sUAS that could, among other impacts, violate restricted airspace, engage in hostile surveillance and reconnaissance targeting of government facilities, effect physical intrusions, exploit vehicle-based security vulnerabilities, create or deliver explosive hazards, and further incidents of targeted violence.
8. Additionally, regional security partners must counter disruptive tactics such as cyber-enabled attacks on key networks, interference with public safety communications, and coordinated incidents designed to strain law enforcement capacity, divert emergency response resources, or disrupt essential government and public activities. These threats may originate from foreign intelligence actors, violent extremists, criminal elements, lone offenders, or individuals whose motivations remain unidentified. Protecting the NCR requires constant vigilance, rapid intelligence sharing, and seamless operational integration among DHS components, federal and regional law enforcement agencies, and private sector security partners to safeguard the community and secure critical assets.
9. Mitigation of nefarious and illicit UAS by the federal government as a whole is largely episodic in the NCR, where—outside of individual agency efforts to protect their individual facilities or assets in accordance with their statutory missions—capabilities are temporarily deployed only during National Special Security Events (NSSEs), Special Event Assessment Rating (SEAR) Events, or for responding to emergencies.
10. To counter these agile, rapidly evolving, and evasive threats, the region must shift from these

legacy detection and mitigation frameworks and methods towards a hybrid and more enduring model that blends air, area, and point-defense strategies to establish layered protection for sensitive facilities alongside a baseline level of security for the broader region.

11. Promptly addressing UAS threats is a highly complex endeavor that requires seamless coordination among the diverse security and safety partners operating throughout the NCR. Although entities like the National Capital Region Coordination Center (NCRCC) have successfully facilitated rapid, real-time situational awareness for manned aviation threats by physical co-location of agency representatives, they lack the specialized methods, processes, and tools required for continuous operation in the high-volume UAS environment of the NCR. Currently, there is no "shared situational view" (SSV) to enable the consistent distribution of tactical, operational, and strategic UAS information across different leadership levels and law enforcement agencies. Without system interoperability, automated domain awareness, and a unified SSV, the NCR's security posture remains fragmented, leaving security partners poorly positioned to address the evolving sophistication of modern UAS technology.

12. In the NCR, mission success depends entirely on seamless interagency coordination due to an incredibly dense and complex jurisdictional landscape. Within this single geographic area, authority is shared and divided among dozens of overlapping federal protective forces, state police departments, municipal agencies, and transit authority law enforcement. Because each of these agencies operates under distinct statutory mandates—ranging from executive protection and federal asset security to local community policing—their immediate operational priorities can easily compete or conflict during a crisis. A unified coordination framework will help minimize these fragmented environment risks that would otherwise lead to critical coverage gaps, operational friction, and resource duplication that adversaries can exploit.

13. To overcome these challenges, physical co-location and real-time information sharing are operational necessities between federal partners in the NCR. By placing personnel from diverse agencies side-by-side within regional fusion centers, joint operations centers, and other centralized entities or structures, the security apparatus builds immediate trust and bypasses slow, formal bureaucratic channels. This co-location ensures that localized, seemingly isolated intelligence—such as a suspicious physical intrusion or an unauthorized drone sighting—is immediately integrated with federal threat intelligence to create a single, comprehensive picture of the regional security posture. Ultimately, this unified approach will allow the region's diverse law enforcement entities to act as a single, responsive security network capable of protecting critical infrastructure and public safety. The Washington, DC-FRZ Interagency C-UAS Concept of Operations, issued in 2026, reflects the combined efforts of the Department and its interagency partners to develop a framework for strategic and operational coordination to address the UAS threat in the NCR.

14. As a means to attain such joint coordination, the implementation of a centralized and elevated infrastructure node at a key geographic location in the NCR would effectively bridge the NCR's fragmented jurisdictional boundaries and enhance homeland defense. A single, integrated joint operations center or similar facility operating from an elevated location would enhance regional coordination by establishing a common operating picture across agencies authorized to engage in C-UAS, maximizing line-of-sight advantages by enabling the placement of detection sensors and other C-UAS equipment above urban obstructions ubiquitous in the NCR and providing operational resilience for C-UAS support during emergencies.

15. According to information I have reviewed concerning the planned Triumphal Arch and Military Complex (the Arch), the Arch would be built at the western end of the Arlington

Memorial Bridge and stand approximately 166 feet tall; at that height, the Arch would be equipped with an observation deck and gilded figures, bringing the total height to approximately 250 feet. Based on that information, I believe the Arch—when equipped with the necessary technological capabilities and space to permit interagency co-location on C-UAS efforts—in that location would satisfy the requirements set forth above (i.e., an elevated, central location that permits enhanced domain awareness, interagency coordination, and information sharing).

16. The implementation of the capabilities discussed in this declaration would not require any structural modifications or alterations to the existing plans for the Arch. The security features will be fully integrated into the existing design.

17. As an agency with standalone C-UAS authority at 6 U.S.C. § 124n to detect, identify, monitor, track, and disrupt or mitigate UAS threats, DHS would benefit from the development and construction of a platform such as the planned Arch for C-UAS operations in the NCR.

18. The Arch would, when properly equipped, provide an opportunity to substantially expand UAS detection, and if necessary, disruption or mitigation, in the NCR, directly supporting DHS's mission. The Arch would also enhance overall DHS UAS awareness in the NCR.

19. The Arch would also support other DHS national security functions including providing security for senior U.S. Government officials through the United States Secret Service and protecting federal facilities through Federal Protective Service. The Arch could provide a forum to enhance overwatch, operational planning, monitoring, and execution, and interagency information sharing and coordination including in the protection and movement of U.S. Government protectees and the protection of federal facilities.

20. In addition, the planned location, at a strategic entrance and exit to the District of Columbia and

situated between multiple interagency partners responsible for the NCR, would—provided the Arch is equipped with the necessary space and equipment—provide DHS and its partners the opportunity for enhanced interagency coordination. As President Trump stated, the Arch is intended to incorporate a number of features that will support national security. The geographic location provides opportunities for increased capability for information-sharing and logistical coordination, increased sensor capabilities for domain awareness, and provides a strategic location for joint operational coordination capabilities.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Dated: October 27, 2026

Markwayne Mullin
Secretary of Homeland Security