MITRE

COUNTERING UNMANNED AIRCRAFT SYSTEMS
SECURING THE HOMELAND AGAINST EVOLVING THREATS

Due to their proliferation and rapidly evolving capabilities, unmanned aircraft systems (UAS), commonly known as drones, pose an emerging threat to the safety and security of the Homeland when used illicitly. Confronting UAS threats and effectively safeguarding the Homeland requires presidential support for legislative expansion of counter-UAS (C-UAS) authorities and a holistic approach to airspace awareness and protection that preserves Americans' rights to access and use the airspace.

The Case for Action

The rise of recreational and commercial uses of UAS with increasingly advanced capabilities creates numerous economic opportunities for various domestic industries, including aerial photography, delivery services, and the agricultural sector. While UAS technology benefits commercial industries, UAS's relative low cost, growing presence in the airspace, and ease of use also make them an attractive tool for carrying out non-attributional, nefarious activities. UAS capabilities may be exploited to conduct hostile surveillance and smuggling activities, as well as to disrupt government missions and aviation operations. They may also be weaponized to carry out lethal attacks on mass gatherings. Due to the variety of potentially malicious applications of UAS, they are one of the most significant emerging threat vectors in the Homeland.

Preventing and confronting UAS threats demands extensive coordination and collaboration across multiple federal departments and agencies. Currently, four U.S. government departments—the Departments of Homeland Security (DHS), Justice (DOJ), Defense, and Energy—have the authority to conduct C-UAS activities under 6 U.S.C. § 124n, 10 U.S.C. § 130i, and 50 U.S.C. § 2661, respectively. The proposed Safeguarding the Homeland from Threats Posed by Unmanned Aircraft Systems Act of 2023 seeks to expand the C-UAS authorities granted to DHS and DOJ. For example, if passed, the Act would finally grant statutory authorization to DHS and DOJ for the protection of airports. It would also establish a pilot program to evaluate the potential benefits of state, local, tribal, and territorial (SLTT) law enforcement (LE) entities having the ability to detect and mitigate credible UAS threats. Presidential support for the passage of appropriate legislative expansions of C-UAS authority, such as those included in the Act, is critical to address and close the policy and legal gaps that currently impede departments, agencies, and other stakeholders from being able to effectively carry out their C-UAS missions.

To protect the Homeland from UAS threats and enable the counter-UAS mission, the Executive Office of the President should articulate, prioritize, and emphasize the national security need for expanded legal authorities and additional resources.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

To protect the Homeland from UAS threats and enable the C-UAS mission, the Executive Office of the President (EOP) should articulate, prioritize, and emphasize the national security need for expanded legal authorities and additional resources. Ensuring the mission success of safety and security partners will require addressing legal, regulatory, technological, and resource challenges, while also seizing relevant opportunities within the C-UAS landscape.

Key Challenges and Opportunities

UAS technology is rapidly evolving and proliferating across the United States, increasing potential threat vectors and outpacing the capabilities of current air domain awareness systems and countermeasures.

Technological advancements in areas such as imaging, construction, composition, speed, autonomy, and artificial intelligence, coupled with higher UAS proliferation due to factors such as increased affordability, private and public sector uses, 3-D printing, and do-it-yourself kits, make UAS more attractive as potential threat vectors for nefarious actors. These advancements also enable UAS to circumvent traditional countermeasures such as signal jamming. The federal government has opportunities to improve current air domain awareness and counter-capabilities and systems by adapting, modifying, and/or expanding existing acquisition and technology development approaches. These opportunities include exploring alternative types of equipment ownership, rental, or lease agreements, as well as incentivizing industry to rapidly develop innovative air domain awareness and countermeasure solutions.

Safely and securely integrating authorized UAS into the National Airspace System (NAS) is a multifaceted issue complicated by considerations related to airspace congestion, privacy, cybersecurity, and environmental impacts.

Akin to the current traffic infrastructure available on the nation's roads, UAS Traffic Management (UTM) solutions must be implemented for authorized UAS operations in the NAS. Although this is a complex and challenging endeavor, there are opportunities in this space for federal security partners to invest in, improve, and enforce the use of UAS Remote Identification, as well as to closely collaborate with safety partners to develop and deploy UTM solutions.

There is an overall lack of UAS and C-UAS protection-focused infrastructure across the United States.

Discriminating and countering UAS threats requires scalable, protection-focused planning, systems, processes, and infrastructure to address the growing presence and use of UAS in the NAS, while also minimizing current and anticipated homeland security risks. Protection constructs, technologies, and systems must be tailored for C-UAS purposes and supplemented, as needed, by additional security measures. Opportunities exist to foster public-private partnerships and to collaboratively develop infrastructure solutions to establish air domain awareness and enable UAS countermeasures.

Security partners lack the resources needed to effectively safeguard soft targets (STs) and crowded places (CPs) against UAS threats.

Increasing UAS activity heightens the risk that they will be used to cause harm at any one of the thousands of ST and CP events that take place annually across the United States. Potential UAS threats at STs and CPs may include deploying dangerous chemical, biological, or other substances over crowds or using the physical device to cause harm. Nationwide, federal and SLTT personnel should be trained, funded, and equipped to defend against UAS threats. The federal government has the opportunity to enhance the security of STs and CPs by advocating for additional personnel, equipment, and educational resources for federal and SLTT C-UAS protection efforts.

Data-Driven Recommendations

1. IDENTIFY AND PRIORITIZE AREAS IN THE UNITED STATES THAT MOST REQUIRE PROTECTION FROM UAS THREATS

Not all areas in the United States require the same level of protection from UAS threats. DHS and DOJ should lead an effort to identify, assess, and prioritize locations in the country to receive C-UAS protection. Locations may be selected based on factors such as population density, infrastructure, national or homeland security criticality, economic or financial value, aviation nexuses, and current levels of UAS activity.

2. DEVELOP DATA AND INFORMATION EXCHANGE STANDARDS FOR C-UAS SYSTEMS

The Office of Science and Technology Policy (OSTP) and the National Institute of Standards and Technology (NIST) should lead a coordinated, interagency effort with federal and SLTT partners, commercial industry

partners, and other relevant stakeholders to design, develop, and implement C-UAS data and information exchange standards. These standards will facilitate system interoperability and scalability, improve data and information quality and reporting, enhance air domain awareness, and enable timely decision making when federal and SLTT security partners are responding to UAS threats within and across different locations and jurisdictions.

3. ENACT STRONGER PENALTIES FOR UNAUTHORIZED UAS ACTIVITY AND FAILURE TO COMPLY WITH UAS OWNERSHIP AND FLIGHT RULES

To maintain a safe and secure NAS, the Federal Aviation Administration (FAA) should spearhead the enactment of stronger regulatory UAS operation rules and collaborate with federal and SLTT agencies, such as DOJ, to enforce penalties for airspace violations. The FAA should also work with DOJ to influence the development of tighter controls and restrictions on UAS ownership, registration, and compliance with Remote Identification standards, as well as impose more effective penalties for violations.

4. EMPOWER SLTT LE TO USE UAS FOR THE PUBLIC INTEREST AND TO SERVE AS C-UAS PROTECTION FORCE MULTIPLIERS

Many SLTT LE entities are not currently equipped with sufficient guidance, authority, or resources to use UAS effectively for the public good and protect the public from emergent UAS threats. At a minimum, the EOP should support granting legislative authorities to SLTT LE to conduct UAS detection-only activities to enable SLTT air domain awareness. In coordination with the Office of Management and Budget (OMB) and DOJ, SLTT entities should be given federal assistance to educate and train personnel in the tactics, techniques, and procedures needed to use UAS, as well as to respond to unauthorized or nefarious uses of UAS.

Implementation Considerations

FIRST 100 DAYS:

- Task federal security departments through the National Security Council (NSC) to coordinate and develop objective, interagency-supported location criteria to inform the selection of areas warranting C-UAS protection.
- Direct OSTP and NIST to identify and lead relevant federal agencies in designing, developing, and implementing C-UAS data and information exchange standards.
- Establish and task an NSC Interagency Policy Committee (IPC) to improve enforcement of existing rules and regulations governing UAS operations in the NAS, and to investigate options for imposing tighter controls and restrictions that require individuals to register their UAS with the FAA at the point of sale.
- Instruct the NSC IPC to engage SLTT LE partners to understand the challenges these entities encounter when confronting UAS threats.

FIRST SIX MONTHS:

- Commission DHS and DOJ to lead a coordinated effort to identify, evaluate, and prioritize an initial set of U.S. locations of concern warranting C-UAS protection using established objective criteria.
- Support through the EOP the passage of legislative expansions to current C-UAS authorities, such as the authority for the Transportation Security Administration or DOJ to conduct countermeasures at airports, to address policy and legal gaps that impede federal and SLTT security partners from protecting high-risk and potential target locations.

FIRST YEAR:

- Direct OSTP to begin piloting and testing with security stakeholders C-UAS data and information exchange standards across departments and agencies, federal and SLTT partners, commercial industry partners, and other relevant stakeholders.
- Task OSTP and OMB with establishing a federal interagency working group that will monitor UAS and C-UAS technology evolution; address subsequent protection gaps; and obtain the federal funding for necessary personnel, technology, and infrastructure resources.

MITRE Resources and Support

MITRE brings more than 50 years of multidisciplinary experience through mission-driven teams and public-private partnerships enabling tools, analytics, facilities, and training in UAS and C-UAS capabilities. Highlights include:

C. Ulsh and S. Major. MITRE National Range. 2024. MITRE. https://www.mitre.org/sites/default/files/2024-07/PR-24-2208-MITRE-National-Range.pdf

Autonomous Systems and Counter-Autonomy – Positioning the United States for Economic and Security Advantage. October 2024. MITRE. https://www.mitre.org/sites/default/files/2024-10/PR-24-01820-19-Positioning-United-States-Economic-Security-Advantage.pdf

A. Hebert. As Drones Become Weapons of Choice, a Back-to-Basics Way to Counter Them. September 2023. MITRE. https://www.mitre.org/news-insights/impact-story/drones-become-weapons-choice-back-basics-way-counter-them

About the Center for Data-Driven Policy

The Center for Data-Driven Policy, bolstered by the extensive expertise of MITRE's approximately 10,000 employees, provides impartial, evidence-based, and nonpartisan insights to inform government policy decisions. MITRE, which operates several federally funded research and development centers, is prohibited from lobbying. Furthermore, we do not develop products, have no owners or shareholders, and do not compete with industry. This unique position, combined with MITRE's unwavering commitment to scientific integrity and to work in the public interest, empowers the Center to conduct thorough policy analyses free from political or commercial pressures that could influence our decision-making process, technical findings, or policy recommendations. This ensures our approach and recommendations remain genuinely objective and data-driven.

Connect with us at policy@mitre.org.