A D D E N D U M

to

DEFENDING AGAINST DRONES: SETTING SAFEGUARDS FOR COUNTER UNMANNED AIRCRAFT SYSTEMS AUTHORITIES

This Addendum is available at:

https://www.govinfo.gov/content/pkg/CHRG-119shrg61982/pdf/CHRG-119shrg61982-add1.pdf

Submitted by Chair Grassley:

Submitted by Ranking Member Durbin:

Submitted by Senator Schmitt:

Statement for the Record On Importance of Protecting Civil Liberties and Providing Accountability For C-UAS Authorities

The American Civil Liberties Union, Center for Democracy & Technology, Electronic Frontier Foundation, and Electronic Privacy Information Center jointly submit this Statement For The Record regarding counter unmanned aerial system ("C-UAS") authorities.

We recognize that the government has a genuine need for counter-drone monitoring and mitigation powers and support the development of policies that responsibly achieve this goal. However, given the expanding use of drones by the public—notably by journalists and activists—it is critical that those powers are carefully tailored, and that checks and oversight mechanisms exist to prevent misuse and allow ordinary, law-abiding individuals to exercise their rights.

Unfortunately, as we and many other civil society advocates have highlighted, past proposals have failed to give due consideration to these needs.[1] Congress should produce well-balanced rules that address all these priorities, not grant de facto authority to law enforcement to take down drone flights whenever they want. Ultimately, Congress must decide whether drones will be a technology that mainly serves government agencies and big companies, or whether it might also empower individuals.

To make progress in stabilizing C-UAS authorities and addressing emerging issues, Congress should adopt a more comprehensive approach that accounts for the full range of risks and implements proper safeguards. We recommend future C-UAS legislation include the following priorities, which are essential to protecting civil liberties and providing accountability:

Strong and explicit safeguards for First Amendment-protected activities: Protection of First Amendment rights is essential as drones have become a valuable tool for journalists, as well as activists recording demonstrations both to spread awareness and document potential police mistreatment of protesters. Law enforcement has already, on numerous occasions, abused their authority to block drone flights purely to stop journalists from recording the behavior of police;[2] Congress must not allow C-UAS powers to be misused in this nefarious manner. It is unacceptable that an investigative reporter or protester might have a drone they are using in a lawful and Constitutionally-protected manner abruptly taken out of the air due to overbroad or unclear rules. Any legislation extending C-UAS authorities should guard against this risk by providing strict protections for journalism and other Constitutionally-protected activities.

[1] See, 2023 Letter From Civil Society Organizations to Senators Peters, Paul, Durbin, and Graham on C-UAS Legislation, July 25, 2023, available at https://cdt.org/wp-content/uploads/2023/07/Civil-Society-Letter-on-C-UAS-Bill.pdf; see also, 2022 Letter From Civil Society Organizations to Senators Peters, Portman, Durbin, and Grassley on C-UAS Legislation, July 13, 2022, available at https://cdt.org/wp-content/uploads/2022/07/Counter-UAV-Privacy-Civil-Liberties-Letter.pdf.

[2] See, Jack Gillum, Associated Press, "AP Exclusive: Ferguson no-fly zone aimed at media," November 2, 2014, available at https://apnews.com/article/674886091e344ffa95e92eb482e02be1; see also, Jason Koebler and Sarah Emerson, Vice, "FOIA: How Police Convinced the FAA to Put a No Fly Zone Over Standing Rock," September 27, 2017, available at https://www.vice.com/en/article/foia-how-police-convinced-the-faa-to-put-a-no-fly-zone-over-standing-rock/; see also, Meerah Powell, OPB, "Temporary flight restrictions around Portland may be related to protests, federal agencies," July 21, 2020, available at https://www.opb.org/news/article/portland-protest-flight-restrictions-drones/.

Ensure transparency and require detailed reporting: Strong transparency measures and reporting requirements for C-UAS activities are essential to guard against abuse, as well as to ensure efficacy given rapid evolution in how drones are used and uncertainty over what C-UAS measures will most effectively mitigate threats. Legislation extending or expanding C-UAS powers should require any entity exercising those powers to provide annual public reporting that includes 1) the number of times mitigation measures were deployed, 2) a summary of any incidents in which aircraft were seized, disabled, damaged, or destroyed pursuant to C-UAS authority, 3) a description of any non-compliance events, and 4) a description of any C-UAS actions that disrupted unmanned aircraft engaged in Constitutionally-protected activities. Required reporting on these important metrics would not compromise methods and techniques, yet would protect against abuse, and provide the public and policymakers useful information on how counter-drone systems might be improved in the future.

Furthermore, if C-UAS powers are extended to state and local law enforcement, state open record laws and other transparency rules should be applied to their use of this authority. States and localities—and most importantly, the residents of those localities—must not be inhibited from assessing how their law enforcement personnel deploy new powers granted by the federal government.

Provide due process and recourse for improper counter-drone activities: C-UAS authorities—especially actions that result in the damage or seizure of private property—should be subject to reasonable due process and redress measures to account for impropriety. Individuals, including both drone operators and bystanders, must have reasonable means of contesting whether harmful C-UAS actions were within the bounds of the law, and seeking redress for any improper damage that does occur. Problematic practices that undermine due process rights such as asset forfeiture should not be considered.

Require C-UAS mitigation to involve least-invasive methods: Necessary counter-drone measures can range significantly depending on the situation. Most of the time, simply identifying the owner of a drone, checking whether a drone is on an authorized "whitelist" to fly in a sensitive area, or notifying its operator that it has veered into a restricted airspace is sufficient to remedy a threat. When these and other low-risk countermeasures are reasonably available, authorizing more extreme actions such as a kinetic response or otherwise downing a drone is both unnecessary and dangerous. C-UAS authorities should empower personnel to take only the least-intrusive measures reasonably necessary to mitigate a potential threat, and promote the development of guidelines on how to evaluate threats and necessary responses across various situations. Congress should also stipulate that no mitigation measures may be applied to drones unless they are actually flying within a prohibited or restricted area.

These common sense rules would still permit counter-drone activities as needed in any given situation, while removing the danger of sloppy and overbearing mitigation measures, or even worse, abuse of C-UAS powers, such as disrupting journalists' drones based on the pretext of a threat. Limiting C-UAS mitigation powers to least-invasive methods is especially critical for any legislation that seeks to expand the personnel authorized to engage in counter-drone activities to include not just federal officials, but state and local law enforcement.

Maintain reasonable retention limits on data collection: Current law creates a 180-day retention limit for data collected via C-UAS activities, but also includes a broad exemption for whenever the government

deems necessary for an investigation or to support ongoing security operations.[3] The general retention period along with this exemption provides ample authority for preserving data to meet any legitimate security needs. Congress should maintain current retention rules, especially given that innovation in drone use could mean that in the future these aircraft contain new forms of sensitive data. Already today drones may contain personal video that would, in a cell phone or any other device, not be accessible to law enforcement without a warrant.

Maintain sunset for C-UAS powers as drone uses continue to evolve: Congress has been wise to place a sunset on C-UAS authorities. Drones are still a relatively new technology and are evolving in terms of their capabilities and uses to the public. Counter-drone techniques are evolving as well and involve even newer, more uncertain technologies. Periodic review ensures that rules created at this time do not improperly inhibit unforeseen future uses and do not grant authorities that prove needlessly broad or dangerous. Congress should continue to include a sunset on C-UAS authorities to protect civil liberties and promote efficacy.

We hope Congress will take effective action on this important issue. However, it must do so in a careful manner that protects privacy and civil liberties, as well as addressing public safety concerns. We urge you to only extend C-UAS authorities with the limits described above to help ensure that counter-drone authorities are wielded responsibly.

[3] 6 U.S.C. 124n(e)(3).

Statement for the Record
Association for Uncrewed Vehicle Systems International (AUVSI)

U.S. Senate
Committee on the Judiciary
Full Committee
"Defending Against Drones: Setting Safeguards for Counter Unmanned Aircraft Systems Authorities"

May 20, 2025
10:15 AM
Washington, DC

Chairman Grassley, Ranking Member Durbin, and Members of the Committee,

On behalf of the Association for Uncrewed Vehicle Systems International (AUVSI) and our members, we would like to express our gratitude for holding this important hearing on Counter-Unmanned Aircraft Systems (cUAS) and appropriate safeguards when considering expanded authorities. Recent reports of aircraft activity, including drones and crewed aircraft, over New Jersey and the Eastern U.S., regulatory developments related to beyond visual line of sight (BVLOS) drone operations, and continued inaction by Congress to expand cUAS authorities, this hearing is particularly timely.

AUVSI represents over four hundred corporations and 8,000 professionals across more than sixty countries in industry, government, and academia. Our members span the defense, civil, and commercial sector and multiple transportation domains, inclusive of hardware and software companies. Our member companies design, build, and operate Uncrewed/Unmanned Aircraft Systems (UAS or drones), as well as cUAS systems for detecting and mitigating drones. We also represent leaders in advanced air mobility (AAM), including manufacturers, aircraft autonomy providers, component suppliers, and infrastructure developers.

Drones offer extraordinary benefits to society, including enhanced public safety, infrastructure inspection, and economic growth. Emergency response teams increasingly rely on drones to aid in search and rescue operations, deliver medical supplies, and assess disaster damage, saving lives and improving response times. With respect to infrastructure, drones allow for safe and cost-effective inspection of bridges, power lines, and pipelines, minimizing risks for workers and preventing costly failures. Moreover, the burgeoning industry is a powerful engine of job creation, fostering innovation and economic activity across sectors like agriculture, logistics, and entertainment.

However, the lack of adequate government investment in airspace awareness technology has left the nation ill-equipped to reliably distinguish between lawful drone operations, careless activity, and potential threats. This confusion not only undermines public safety but also risks stifling innovation in the commercial drone industry, which represents one of the most promising sectors of modern transportation.

The aforementioned recent events highlight the urgent need for the U.S. to modernize its approach to airspace monitoring and regulation. The lack of clear rules and sufficient airspace awareness has led to the many positive applications of drones being overshadowed by concerns of misuse and safety. Additionally, the rapid advancement and proliferation of drone technology necessitates a comprehensive and updated regulatory framework to ensure the safety and security of our national airspace system (NAS). This is especially true now that the BVLOS and Section 2209 draft safety rules have recently re-entered the Office of Information and Regulatory Affairs interagency review process. It is our hope that these rules will be finalized in the near term, making it critical that Congress closely consider expanding cUAS authorities in a way that ensures robust oversight and diligent training.

The current rules governing cUAS have not been updated by Congress since 2018. Considering the significant technological advancements and the evolving threat landscape, it is imperative that Congress take decisive action to modernize these regulations. We strongly advocate the following measures:

- **Expanded Authority**: Granting broader authority to relevant agencies to effectively manage and mitigate UAS threats, tightly overseen by the appropriate federal government agencies.
- **Pilot Programs**: Implementing pilot programs to test and refine cUAS technologies and strategies in real-world scenarios.
- **Increased Funding**: Allocating sufficient funding to support research, development, and deployment of advanced cUAS systems.
- **Rigorous Testing**: Establishing rigorous testing protocols to ensure the reliability and effectiveness of cUAS technologies.

We also want to highlight the significant work done by the Federal Aviation Administration's (FAA) UAS Detection and Mitigation Systems Aviation Rulemaking Committee (ARC), co-chaired by AUVSI President and CEO Michael Robbins. The ARC's final report, released to government stakeholders in February 2024, makes critical recommendations to enhance airspace safety and security through the expanded use of drone detection and mitigation technologies. These recommendations include establishing minimum performance standards, creating a scalable regulatory framework, and developing clear approval processes for detection and mitigation deployment at airports and other facilities. Importantly, one of the ARC's key elements is to treat UAS detection equipment and rules distinct from UAS mitigation equipment and rules. They are unique, have different risk profiles, and accordingly should have different pathways towards integration.

The ARC's work underscores the importance of a collaborative approach involving government and industry stakeholders to ensure the safe and secure integration of UAS into our NAS. We urge the FAA to swiftly release its plan to implement the ARC's recommendations. A clearer, expanded regulatory framework for cUAS technologies is imperative to ensure companies can make informed business decisions, and to ensure that private capital continues to invest in these transformative technologies. The steps outlined in this statement are also necessary to ensure that the United States remains the gold standard in aviation and aviation safety. With commonsense action by Congress and the FAA, we will no longer cede our competitive edge in this space to other nations.

Lastly, AUVSI applauds members across multiple Committees in Congress for introducing various pieces of cUAS legislation over the last several years. We are optimistic that legislation will move forward in the near term. AUVSI strongly supports expansions of broad UAS detection authorities across both federal, state, local, and private entities and more limited UAS mitigation authorities, coupled with rigorous federally administered training programs, for federal, state, and local entities. The key here is progress, and we do not want to let the perfect be the enemy of the good.

We appreciate the Committee's commitment to addressing this critical issue and stand ready to collaborate with Congress to advance these necessary updates. Together, we can ensure that our NAS remains safe, secure, and conducive to innovation.

STATEMENT FOR THE HEARING RECORD
LISA ELLMAN
CHIEF EXECUTIVE OFFICER OF THE COMMERCIAL DRONE ALLIANCE

United States Senate Committee on the Judiciary

"Defending Against Drones: Setting Safeguards for Counter Unmanned Aircraft Systems Authorities"

May 20, 2025
10:15 AM
Room 226, Dirksen Senate Office Building

Submitted into the Record: May 23, 2025

Chairman Grassley, Ranking Member Durbin, and Members of the Committee:

On behalf of the Commercial Drone Alliance (CDA) and its members, thank you for the opportunity to submit a statement for the record on the subject of counter-unmanned aircraft systems (counter-UAS) technologies. The CDA is an independent non-profit organization made up of leading entrepreneurs and innovators in the commercial drone and Advanced Air Mobility (AAM) industries. The CDA brings together commercial drone end-users, manufacturers, service providers, advanced air mobility companies, drone security companies, and vertical markets including oil and gas, precision agriculture, construction, security, communications technology, infrastructure, newsgathering, filmmaking, and more. The CDA works with all levels of government to collaborate on policies for industry growth and educates the public on the safe and responsible use of commercial drones to achieve economic benefits and humanitarian gains.[1]

Drones have become increasingly commonplace in our country and around the world, enhancing safety and efficiency, reducing costs, and saving lives. Communities across the country

[1] The CDA Board is comprised of Amazon Prime Air, the Choctaw Nation of Oklahoma, DoorDash, Florida Power & Light, Hidden Level, Honeywell, NUAIR, Ondas, Percepto Robotics, Skydio, SkySafe, Southern Company, Wing Aviation LLC, and Zipline International. Learn more about the CDA at www.commercialdronealliance.org.

use this technology every day to fight wildfires, respond to natural disasters, inspect critical infrastructure, bring aid to remote places, and even deliver food and medicine. The drone industry is projected to contribute billions of dollars to the global economy over the next decade. Many of these economic benefits will flow directly to small businesses.

All technology can be used for good and for bad, and drones are no exception. As we have all seen in the news, careless, rogue, or unauthorized drones can present potential public safety and homeland security threats. The commercial drone industry shares the Congress' and the public's desire to ensure that drones are operated safely and in compliance with applicable laws and regulations. To that end, the commercial drone industry is committed to operating transparently in accordance with applicable law and to prevent confusion. Our goal is for the public to trust that commercial drones are being operated safely and to understand the significant value this technology brings to our country.

We therefore encourage policymakers to take two important steps to mitigate potential issues caused by rogue or unauthorized drones in the future: establish a regulatory foundation that supports safe and secure drone operations, and take the necessary actions to expand existing authorities for dealing with non-compliant drones. Together, these steps will support lawful operators, promote American industry, create transparency in the airspace, and provide authorities with appropriate tools to address potentially nefarious drone operators.

A FOUNDATION FOR SAFE AND SECURE DRONE OPERATIONS

Beginning in 2016, and in response to the strong demand from industry to use commercial drones, the Federal Aviation Administration (FAA) authorized limited commercial drone operations away from airports. As commercial operators demonstrated that these flights could be performed safely and securely, the FAA has expanded the scope of these approvals. For instance, certain drones are now permitted to operate over people[2] and to operate at night with appropriate lighting.[3]

Importantly, the expansion of these authorized operations (over people and at night) coincided with the FAA's Remote Identification (Remote ID) rule, which went into effect this past year.[4] Remote ID requires drones to be equipped with a digital drone license plate to provide identification and location information that can be received via broadcast signal (using Wi-Fi or Bluetooth technology). The public can now use several readily available smartphone apps (such as Drone Scanner) to identify a drone's license plate—much like we do with cars on the road.

[2] *See* 14 C.F.R. §§ 107.39, 107.100 *et seq.* (2021).

[3] *See* 14 C.F.R. § 107.29 (2021).

[4] *See* 14 C.F.R. § 89 *et seq.* (2021).

Remote ID helps both the public and public safety officials discern legitimate authorized drones from those that are not following the rules. In general, a drone broadcasting its digital license plate will be operating in accordance with FAA regulations.

The Remote ID requirement was an important step to increase transparency. Now, more work must be done to improve compliance with the rule. Additionally, more resources and information must be made available to the public and to state, local, tribal, and territorial governments to enhance the understanding of Remote ID technology. The CDA recognizes that we play a critical role in both efforts, and we are committed to helping improve compliance and public outreach. We also urge lawmakers and regulators alike to consider ideas to incentivize additional adoption of Remote ID. To truly harness the benefits of the Remote ID rule and increase the transparency in the airspace, we need a public education campaign to provide information on how to use Remote ID as an effective tool.

In addition to Remote ID, two new rules currently in development would contribute significantly to enhancing airspace transparency and preventing drones from flying where they should not. The first is a rule to enable beyond visual line-of-sight (BVLOS), and the second is a rule focused on drone security around critical infrastructure and sensitive airspace (commonly referred to as the "2209 rule"). The FAA Reauthorization Act of 2024 recognized the importance of these rules and established timelines for both.[5] We expect the BVLOS rule will improve electronic conspicuity for everyone in the airspace, and provide a framework for third parties to provide services that help the government more effectively link drones in flight to responsible parties on the ground. We expect the 2209 rule, which is approaching almost a decade of delay given that Congress first mandated the process in 2016, will enable critical infrastructure proprietors and other sensitive fixed-site operators to request that drone operations be restricted over their facilities.

Unfortunately, despite calls for action by the House Committee on Transportation and Infrastructure,[6] congressionally mandated deadlines for both rules have been ignored at the expense of the drone industry and the American public. We therefore urge this Administration to publish these draft rules as soon as possible, and hope that Congress will continue to hold the FAA and other agencies accountable for finishing this critical regulatory work. The CDA sent a letter

[5] FAA Reauthorization Act of 2024, Pub. L. No. 118-63, §§ 929, 930, 138 Stat. 1025, 1365–66 (2024).

[6] Letter from Chair of House Committee on Transportation and Infrastructure Sam Graves (R-MO), Ranking Member Rick Larsen (D-WA), and other members of the Committee to Secretary of Transportation Pete Buttigieg and Federal Aviation Administration Administrator Michael Whitaker, Oct. 21, 2024 (noting concern that a "failure to comply with statutory instructions may result in the delay of a final [BVLOS] rule" and stating that "[t]he DOT and the FAA must work in a safe and expeditious manner to issue this critical rulemaking.") (found at https://transportation.house.gov/uploadedfiles/2024-10-21_--_bvlos_letter_to_dot_faa.pdf).

to Secretary Duffy earlier this year urging swift action on these new rules that will enable this industry to scale.

Finally, to establish a foundation of security and as recommended by the Counter-UAS ARC, the CDA supports incorporation of a "verified operator" program for drones, similar to other "verified" or "known" operator or user programs such as the Transportation Security Administration's (TSA) Pre-Check, Known Shipper, and Transportation Worker Identification Credential programs. The commercial drone industry would willingly participate in such a program to enable the government to maintain a database of authorized commercial UAS operations and help relevant agencies and public safety officials with threat discrimination. This framework could allow registered and legitimate drone operators to fly their aircraft with streamlined approval processes for purposes that benefit society, including package delivery, infrastructure inspections, and agriculture operations.

EXPANDING EXISTING COUNTER-UAS AUTHORITIES

The CDA has worked for years with federal government officials, industry stakeholders, and others to promote technology solutions that enable the safe and secure integration of UAS into our National Airspace System (NAS). The CDA was honored to help lead a working group of the FAA's UAS Detection and Mitigation Aviation Rulemaking Committee (known as the "Counter-UAS" ARC). As the Counter-UAS ARC recognized, drone security policy has lagged behind the pace of technology.[7] Current laws prevent the use of helpful technology that can increase transparency[8]—for example, if there is a rogue drone in the air, even just using the necessary technology to detect it can violate laws meant to prevent hacking landline telephones or hijacking an aircraft. This stagnation has impacted the health of domestic drone security, risking both public safety and national security.

To address these challenges, we offer recommendations, in line with the spirit of the Counter-UAS ARC Final Report, to further enable the safe and transparent use of counter-UAS technology while also preventing unnecessary burdens on legitimate drone activities. The CDA recognizes that there are a variety of different counter-UAS technologies and systems available to authorized users. Different circumstances and environments may warrant different types of solutions, and policymakers should give operators the flexibility, with appropriate guardrails, to

[7] *See generally* Federal Aviation Administration, *Unmanned Aircraft Systems Detection And Mitigation Systems Aviation Rulemaking Committee Final Report* (Jan. 9, 2024), https://www.faa.gov/sites/faa.gov/files/UAS-Detection-Mitigation-Systems-ARC_Final-Report_02052024.pdf.

[8] *See generally* Federal Aviation Administration, Department of Justice, Federal Communications Commission, and Department of Homeland Security, *Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems* (Aug. 2020), https://www.dhs.gov/sites/default/files/publications/20_0817_ogc_interagency-legal-advisory-uas-detection-mitigation-technologies.pdf.

leverage the technology that works in their circumstances by being technology agnostic in their policy.

In addition to the suggestions offered below, the CDA urges both the executive and legislative branches to consider the various programs and initiatives that will be necessary to effectively and efficiently implement such legislation. Some areas of work, such as operator training, system testing, and standards development, can be started in advance of expanded authorities, and will need to be in place prior to use. We therefore urge executive branch officials to begin these critical efforts now to avoid implementation delays after legislation is enacted. We also urge Congress to ensure these agencies are appropriately resourced to implement any legislation once it is enacted.

Expand Advanced Detection Capabilities

The CDA supports the view of the Counter-UAS ARC that it is important to have direct, low-cost access to accurate information regarding low-altitude aviation within the vicinity of sensitive or highly vulnerable ground sites, including critical infrastructure, mass gatherings, active public safety, and emergency response incident scenes, as well as other locations that may require enhanced protection. With the implementation of the FAA's Remote ID rule, the vast majority of UAS are now required to broadcast their location. Additionally, use of built-in geofencing functions that help prevent careless or clueless drone flights is decreasing. These two factors combined make enabling broad use of detection technology more critical than ever. This authority should be expanded not only to state, local, tribal, or territorial (SLTT) law enforcement agencies, but also to certain appropriately trained private sector entities, such as critical infrastructure operators, in order to reduce the burden on law enforcement agencies.

Expand the Counter-UAS Pilot Program

The CDA supports the Counter-UAS ARC recommendation to more broadly enable the testing of detection and mitigation technologies in real-world environments. To that end, the CDA supports implementing a robust Counter-UAS Pilot Program to enable more SLTT law enforcement agencies to leverage approved mitigation technologies at a broad variety of sites. An expansive pilot program is critical to collecting enough data from a diversity of circumstances and geographies to inform future policy. Additionally, we support limiting the program to areas with a flight restriction, as legitimate operators already know to avoid operating in those areas. In addition, the federal government should be specific at the outset to define what a successful program will look like by providing clear metrics to measure success and enable future appropriate expansion.

Streamline Interagency Approval Processes

The CDA supports a requirement for advanced detection and mitigation technologies to be approved by federal agencies prior to use, and also supports the use of training requirements for technology operators. The CDA also urges policymakers to streamline the implementation of requirements through appropriate legislative accountability mechanisms to ensure progress and avoid delay due to inaction.

Maximize Future Certainty for Government and Industry

The CDA believes that any comprehensive counter-UAS legislation must include a multi-year extension and enhancement of counter-UAS authorities to allow federal agencies, as well as SLTT governments, to appropriately plan and budget their counter-UAS activities. This certainty also will allow for industry stakeholders to invest in the future, which will foster innovation and competitiveness currently lacking in the marketplace. For the same reasons, it is important for the federal agencies implementing these authorities and approving the technology use to be appropriately resourced.

CONCLUSION

Our collective goal is to enable compliant, careful, commercial drone operators while addressing the challenges posed by careless, clueless, or criminal actors. As recent events have shown, there is more that policymakers can do to enable transparency and beneficial uses of counter-UAS technology to prevent misuse of drones. The commercial drone industry fully supports taking the steps outlined above—establishing a framework for safe and secure drone operations, and expanding existing counter-UAS authorities—to update our domestic drone security policy for the safety and security of all Americans. We appreciate the opportunity to inform the committee's exploration of the safe and responsible use of counter-UAS technologies in the United States, and look forward to continuing to collaborate with you and your staff on enacting this important legislation.

May 20, 2025

The Hon. Charles E. Grassley
Chairman
U.S. Senate Committee on the Judiciary
Washington, D.C. 20510

The Hon. Dick Durbin
Ranking Member
U.S. Senate Committee on the Judiciary
Washington, D.C. 20510

Statement of DJ Smith, Deputy Director for DroneResponders Global Public Safety UAS Alliance

Chairman Grassley and Ranking Member Durbin, thank you for the opportunity to offer a statement into the record for the full committee hearing titled "Defending Against Drones: Setting Safeguards for Counter Unmanned Aircraft Systems Authorities." My name is DJ Smith, and I am the Deputy Director for DroneResponders Global Public Safety UAS Alliance, which currently has a membership roll of 1681 US public safety agencies and 1818 public safety agencies worldwide. In my fulltime job I work as a Senior Technical Surveillance Agent as well as serving as Virginia's statewide Unmanned Aerial & Counter UAS Systems Program Coordinator for the Virginia State Police. I have been flying drones for over 14 years and have been working in the Counter UAS space for over 9 years. I previously served on the FAA CUAS Aviation Rulemaking Committee and in addition to that I currently serve on several working groups such as the Commercial Drone Alliance, the US Chamber Working Group, Alliance for Drone Safety and Security, and serve in an advisory role for several other Federal, State, & International CUAS working groups. With Richmond, VA designated by DHS S&T as the urban test site for CUAS, the Virginia State Police was a participating stakeholder in the Bradford I urban CUAS test in downtown Richmond in July of 2022 and most recently the Bradford II test in August of 2024 as a preparation run-up for FIFA 2026.

We can learn from this moment similar to other points in history. The Federal-Aid Highway Act of 1956 was signed into law on June 29, 1956, which started the process of building out the Interstate Highway System (IHS) and was intended to address a number of issues, including:

- **Safety**: Nearly 40,000 people died and 1.3 million were injured annually in traffic accidents.
- **Congestion**: Detours and jams wasted billions of hours and dollars.
- **Courts**: Traffic-related civil suits cluttered the courts.
- **Economy**: Inefficient road transportation made it harder to produce goods.
- **Defense**: The IHS could be used to transport troops and evacuate cities in case of nuclear attack.

The IHS was built to address the mass proliferation of automobiles across the United States. As we witness the mass proliferation of small unmanned aerial systems into the national airspace, we are now dealing with similar pain points which need to be addressed in a similar fashion.

When looking at airspace security for the Homeland as it relates to Small Unmanned Aerial Systems (sUAS), Beyond Visual Line of Sight flights, Drone as a First Responder programs, and Advanced Air Mobility projects, the largest challenge we face is our inability to create a common operating picture of the airspace in a specific geographic area (or, as it is commonly referred to in the current federal vernacular, a "Shared Situational View" of the airspace) across the U.S.. Underlying all of these vulnerabilities is the need to quantify the airspace across the country so we can better define all objects aloft for deconfliction purposes. Foundationally, Detect, Track & Identify (DTI) Counter UAS technology is essential in addition to mitigation tools when the need arises to remove a public safety threat from the airspace. If we do this and look at the larger airspace picture by defining & securing the low-mid level airspace, we not only address the now realized security threat from sUAS, but we also create the foundational piece for the multitude of Advanced Air Mobility projects to flourish. This in and of itself can expand things like Drones as a First Responder (DFR), and Beyond Visual Line of Sight (BVLOS) flights to enable medical deliveries, to address congestion at our maritime ports by moving goods, and a number of other opportunities. All of that will result in creating new business ventures around the use of unmanned aerial vehicles, jobs, and increased tax revenues for our communities. My focus in this document will be on what is needed to address our security vulnerabilities at the SLTT level involving sUAS, but more importantly how we should create a pathway to address these pain points through legislation, implementation, and action. Furthermore, these pathways will positively impact the shared situational view of the Homeland with the state, local, tribal, and territorial (SLTT) law enforcement community becoming a needed force multiplier in securing the Homeland overall.

First, let's look at the primary homeland security vulnerability surrounding sUAS and arguably the most important: the need to Detect, Track, & Identify (DTI) what is aloft in the low-mid level airspace. If we can't Detect and Track things aloft through our airspace, we have no chance of stopping or removing a threat from the airspace when necessary. The other piece is the ability to identify it and essentially answer the questions: "What is it?" & "Where is it?" Basic detection is the ability to know something is aloft and that may be accomplished in a couple of ways. One of the most common is radar, which will let you know that something is aloft in your airspace but does not answer the crucial questions of "What is it" (it could be a drone, or a bird) and "Where is it". The "Where Is It" question is critical to enable law enforcement to interact with the pilot to determine the intent of the flight, and in most cases merely educate the pilot on what is required to safely and legally fly in the NAS. Next is where the much needed legislative "Decoding" piece becomes critical as we start to answer those crucial questions through the use of radio frequency ("RF") or command & control (C2) detection, electro-optical and infrared (EO/IR) cameras, or acoustic sensors. These methods are receiving the command & control signal between the aircraft & controller, noise from the propellers, or visual signature of the airframe. Then, it works through a complex comparative analysis, often through the use of advanced AI algorithms, of known cataloged frequencies or unique signatures of that airframe in real time to let you know what it is. Part of that "Decoded Signal" will also in most cases contain the GPS location of the pilot and airframe as it flies through the airspace. During this process, there is no Personal Identifiable Information (PII) being intercepted in this signal, reducing privacy concerns. Many of the newer advanced systems currently available can also now ingest a signal and analyze it in real time. Although it may not be able to give you the particulars of that specific airframe or controller, it will give you the ability to catalog what it does know so it can alert if the aircraft returns to your airspace.

The biggest issue for the State, Local, Tribal, & Territorial (SLTT) community currently is that we are legislatively limited to only passive detection, which is primarily limited to radar, limiting SLTTs to basic visibility that something is present in the airspace without essential information to evaluate the threat level or secure the airspace. For one small exception, the SLTT community can utilize the DJI Aeroscope or Dedrone's cyber sanitized version of the Aeroscope called an "Aerial Armor" which allows you to detect, track, & classify all DJI products in your airspace. These tools are limited to DJI drones, and only when DJI drone users voluntarily opt to share their data with DJI itself. Beyond that, the SLTT community does not have the legislative authority to perform advanced detection or to "Decode" signals from the airframe to determine the location of the controller, the flight path of the sUAS, and to classify "What it is". This information is essential to assess the threat an sUAS may pose. Title 18 of the federal code forbids any unlawful interception of "electronic signals" without the issuance of a search warrant. 6 U.S.C. 124n relieves certain federal law enforcement entities of this requirement when it comes to counter UAS functions, but not SLTTs. The ability to Detect, Track, & Identify all items aloft is the pivotal piece of the initial process and critical to airspace security and advanced air mobility.

Both chambers have proposed legislation that acknowledge the problem and that something needs to be done. Personally, I think there is legislation to be had if we can coalesce all these bills including the voice of the SLTT public safety community if it will result in legislation that provides a wholistic approach to this threat. I think that any comprehensive solution will need to be a wholistic approach including:

1. As proposed legislation is being discussed and crafted, SLTT stakeholders from around the country need to be a part of those discussions to produce better, more functional and comprehensive legislation. The SLTT public safety community has and will always be the first responder to drone incidents across the country, so crafting solutions that empower us to conduct advanced decoding operations (DTI) and equipping us with mitigation enables SLTTs to act as force multipliers to secure the Homeland and relieve pressure on already thinly spread federal resources. Any legislation that includes accomplishing this through a pilot program needs to ensure that the program is of sufficient implementation size that will move quickly but safely to make a difference because we are already behind in addressing this problem set.

2. A national reporting system for significant drone incursions or incidents is critical. This infrastructure is already in place at every state level with our state fusion or intelligence centers. These centers already have well established communication channels to push intelligence up from the state level to our federal partners as well as down to the local agencies within each state. Incidents reported into this database could be subject to threshold criteria, such as incidents involving sensitive sites like critical infrastructure, correctional facilities, or any incident involving the criminal or terroristic use of a sUAS; not the everyday general "educational" interactions with drone pilots who just do not know the rules, which happens every day at the SLTT level. We need to remember one of the hard lessons from the 911 report: we missed all the small intelligence pieces, and thus we missed the larger picture of the attack in real time. A database would allow us to recognize a potential or realized threat posed by an sUAS or operator by drawing a nexus to the criminal or terroristic use of a drone in real time. For example, if we interdict a drone operator hovering over one of Dominion energy's nuclear power plants here in Virginia and that same pilot, or maybe just that same drone operated by a different pilot is interdicted while

shooting video or mapping the area around a Georgia Nuclear power plant, there is currently no way to link those incidents together. Or perhaps during an investigation of a drone incident an SLTT public safety agency comes across a wing from an Iranian shahed-136 drone; without the national reporting database we could miss a vital piece of intelligence of the presence of a foreign actor or impending attack in real time. That is an intelligence gap that we can fix tomorrow with the current infrastructure in place.

3. Another area that needs to be addressed in this discussion involves the lack of education surrounding sUAS and CUAS across the country. Attached is an informational reference card we created for our sworn personnel at VSP outlining interaction with a drone pilot as well as the proper standard response to a drone incident. When purchasing a drone at point of sale, the purchaser does not get information on what is required prior to launching a drone into the National Airspace System (NAS). Currently, you can purchase a drone from a retailer, charge the batteries, and launch it into the air without knowing that as the pilot you must have a Part 107 or TRUST license, and that the airframe is required to be registered if it is above a certain weight. This group of people are typically referred to as the "careless and clueless" because they are unaware of the rules for safe and legal flight, and make-up 90% plus of the issues we currently deal with. To un-ring that bell there needs to be a robust national campaign to educate the public on what safe and legal flight is for drone operators. The "Remote ID" law went into effect on 09/16/23 with enforcement starting on 3/26/24. However, when you interact with most drone pilots they are completely unaware of the law. This national campaign needs to include education on what "Remote ID" (RID) is and what is required for their airframe to comply with that law. RID was a step in the right direction to help narrow the haystack and to add clarity for deconfliction purposes, which enables law enforcement to focus on the non-compliant drones aloft.

In Virginia, we approach education in a four pronged "Education with Outreach":

1. We take the time to engage and educate our State and Congressional leaders which is extremely important for them to better understand the technology surrounding this issue and how it works. The threat and pain point we are currently dealing with at the SLTT level surrounding the nefarious & criminal use of unmanned aerial systems as well as exploring legislative action moves us closer to securing the NAS and Homeland overall. This hearing is a huge step in that direction, and I applaud the committee for stepping up to hear from the SLTT public safety community and do this.
2. The low-mid level airspace projects we are doing here in Virginia have been extremely important for legislative outreach to illustrate how many sUAS are in the airspaces across Virginia and why some of their flights pose a realized risk. This is extremely beneficial when explaining the vulnerabilities and necessary solutions to our legislators.
3. Outreach & Education across each state and down to the local communities on what is required to fly a drone safely and legally in the NAS.
4. Outreach & Education to the local prosecutors and judges helps them better understand drone technology and what Counter UAS technology is and what it is not. This will inevitably equip them to better prosecute cases where there may be a criminal or terrorist drone

nexus. We accomplish this by going to the annual judges and commonwealth attorneys conference to give presentations on the technology as well as have Q&A sessions.

Once we can create a common understanding across the country on what is required for safe and legal flight coupled with good legislation affording SLTT public safety agencies the carve-outs necessary to conduct meaningful Detect, Track, & Identify operations, we will be better equipped to secure the Homeland. I encourage each member of Congress to go back to your home states and talk to your SLTT public safety officials and listen to their concerns surrounding drones. You will find the pain points and needed solutions are the same in each state with the only difference being that the scope and amount of need will vary because each state's critical infrastructure & airspace are different. This approach will without a doubt result in better legislation with a wholistic approach that addresses the needs of your specific constituency.

Currently, drones weighing less than .55 pounds. are not required to be registered or possess and broadcast Remote ID. As we look to secure the airspace here in the Homeland, we need to see everything aloft to have the ability to completely deconflict the airspace. These smaller drones are at a price point where they are the ones significantly proliferating in the NAS currently. One common drone fitting this size category is the DJI Mavic Mini, which collided with a Canadian super scooper water tanker during the CA wildfires in January and took it out of commission, illustrating the need to have all things aloft compliant with the remote ID law. I would encourage Congress and the FAA to revisit the registration exception for small drones weighing less than .55 pounds.

I would like to personally thank you for allowing the State, Local, Tribal, & Territorial law enforcement voice to be heard on this emerging threat and to be a part of the discussions surrounding solutions in securing the Homeland.

Sincerely,
D.J. Smith
Deputy Director DroneResponders (CUAS)
Senior Technical Surveillance Agent
Unmanned Aerial & CUAS Program Coordinator
Virginia State Police

Right On CRIME

May 19, 2025

Honorable Charles E. Grassley
Chairman
U.S. Senate Judiciary Committee
Washington, D.C. 20510

Honorable Dick Durbin
Ranking Member
U.S. Senate Judiciary Committee
Washington, D.C. 20510

Chairman Grassley and Ranking Member Durbin:

Thank you for holding a hearing on why and how federal and state correctional facilities must defend against the increased infiltration of drones.

According to the U.S. Department of Justice (DOJ) National Institute of Justice, "[e]very day, correctional facilities face formidable threats from contraband such as illicit weapons, drugs, and cell phones."[1] Drones exacerbate this. Drone operators can carry larger payloads, fly faster and for longer distances, and operate more cheaply. It is therefore necessary to identify and support policies that enable correctional facilities – both at the federal and state levels – to prevent drones from infiltrating airspace and delivering dangerous contraband.

Drones pose a public safety risk in several ways.

First, they can transport and deliver dangerous contraband, most frequently drugs and cell phones. Drug use is prolific in Bureau of Prisons (BOP) facilities and increases violent incidences with staff and between inmates, decreases the health and well-being of prisoners and staff, and undermines rehabilitation. In fact, at a Senate Judiciary hearing last year, DOJ Inspector General Horowitz testified that contraband drugs are a contributing or sole factor in nearly 1/3 of inmate deaths.[2] Further, BOP inmates have used contraband cellphones to conduct illegal activities, including ordering hits on individuals outside of the prison walls, running illegal drug operations, facilitating sex trafficking, and organizing escapes.

The dangers of the contraband themselves cannot be understated. But beyond the overt security threats, drones wreak administrative havoc. When staff suspect a drone contraband drop, it often requires a lockdown, a thorough search, and staff moving to and from designated duties.[3] With the ongoing and well documented BOP staffing crisis, no other catalyst should fan the flames. Safety

[1] https://nij.ojp.gov/topics/articles/addressing-contraband-prisons-and-jails-threat-drone-deliveries-grows.
[2] https://www.judiciary.senate.gov/committee-activity/hearings/examining-and-preventing-deaths-of-incarcerated-individuals-in-federal-prisons.
[3] *See, e.g.*, https://advexure.com/blogs/news/inside-the-wire-how-correctional-facilities-are-combatting-drone-contraband?srsltid=AfmBOorP7Jp48tb57EJshBD8gNXVP0il3WDoZQRxoi62w7HeY5AraEwo.

concerns for both inmates and staff, therefore, are exacerbated by lower staffing numbers, increased augmentation, and staff limitations.

The presence of drones can also hamper the effective implementation of hallmark criminal justice laws. For instance, the First Step Act, a bill shepherded by this Committee and signed into law by President Trump, focuses heavily on using evidence-based recidivism reduction programming in federal prisons to encourage inmate participation and promote public safety outcomes. To wit, such measures have succeeded. Prior to the First Step Act, the recidivism rate among federal offenders hovered around 50%.[4] However, since its passage, the rearrest rate has dropped significantly. In fact, according to the DOJ's 2024 First Step Act report to Congress, the average recidivism rate among the nearly 45,000 federal prisoners who benefitted from the First Step Act is only 9.7 %. It is a pro-public safety strategy to continue meeting the mandate of the First Step Act. That means, in part, ensuring consistent access to programming while in prison.

However, drones can largely inhibit this. In fact, a drone can completely shut down a correctional facility. This means that inmates cannot move around the facility because of ongoing recovery and investigations. So, education programs, treatment programs, and evidence-based recidivism reduction programs are shut down.[5] Simply put, a drone incursion can derail the necessary rehabilitative efforts of federal and state prisons. Preventing eligible inmates from accessing programming, substance use treatment, GED classes and work programs can stack the cards against them. Drones are a direct roadblock in promoting successful reentry. If you believe in strong programming opportunities that promote public safety – like those promoted by the First Step Act –, then addressing drones is necessary.[6] Increased availability and use of tools to defend against drones will promote public safety inside and outside carceral walls.

Today's hearing sheds light on an important issue and Right On Crime looks forward to continuing to work with both sides of the aisle on policies that promote public safety, rehabilitate offenders, and support victims.

Sincerely,

Brett Tolman
Executive Director
Right On Crime

Cc: Members of the U.S. Senate Committee on the Judiciary

[4] https://www.ussc.gov/sites/default/files/pdf/research-and-publications/researchpublications/2016/recidivism_overview.pdf.
[5] https://www.linkedin.com/events/contrabandcrisis-drones-intervi7285027357604626432/comments/ at 14:00.
[6] https://www.youtube.com/watch?v=jQiwoOfGlv0 at 5:00.

U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

May 19, 2025

The Honorable Chuck Grassley
Chair
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Dick Durbin
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Grassley and Ranking Member Durbin:

The U.S. Chamber of Commerce ("Chamber") respectfully submits the following statement for the record for the Senate Judiciary Committee's hearing titled "Defending Against Drones: Setting Safeguards for Counter Unmanned Aircraft Systems Authorities." We appreciate the Committee's ongoing efforts to address the public safety threats posed by illicit unmanned aircraft, or drones, to our nation's critical infrastructure, sporting and entertainment events, and airports.

Drones provide substantial economic, social, and national security benefits to the United States and it is crucial that we take a global lead in this innovative technology. However, the misuse and illicit use of drones presents substantial public safety, national security and economic concerns. These concerns include endangering the flying public, disrupting major sporting and entertainment events, enabling criminal and terrorism threats to public safety, and industrial espionage activities towards our most advanced critical infrastructure facilities. These risks are not hypothetical, given the number of unauthorized drone intrusions, close calls, and use of drones globally for malicious purposes.[1]

Presently, four federal agencies have the legal authority to utilize counter-drone detection and mitigation technologies to protect certain sensitive facilities and operations. While we support the missions of those federal agencies to use counter-drone technologies, those federal agencies do not have sufficient resources and

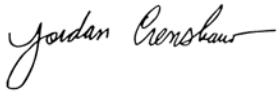
[1] Sara Ruberg, *Man Planned to Use Drone With Explosive to Attack Substation, U.S. Says*, THE NEW YORK TIMES (Nov. 4, 2024), https://www.nytimes.com/2024/11/04/us/columbia-energy-facility-weapon-mass-destruction.html; James Tutten, FBI *Investigates After Large Drones Seen Flying Near Military Base and Trump's Bedminster Golf Club*, WFTV9 (Dec. 4, 2024), https://www.wftv.com/news/local/fbi-investigates-after-large-drones-seen-flying-near-military-base-trumps-bedminster-golf-club/UU7NO62Y6VAZNCMIBN3GD7XYT4/; Gordon Lubold, Lara Seligman, and Aruna Viswanatha, *Mystery Drones Swarmed a U.S. Military Base for 17 Days. The Pentagon Is Stumped*, THE WALL STREET JOURNAL (Oct. 12, 2024), https://www.wsj.com/politics/national-security/drones-military-pentagon-defense-331871f4; *Russian Drones Attack Critical Infrastructure in Ukraine's West, Air Force Says*, REUTERS (Dec. 2, 2024), https://www.reuters.com/world/europe/russian-drone-attack-leaves-parts-ukraines-ternopil-without-power-military-says-2024-12-03/; UAS Sightings Report, Federal Aviation Administration (accessed Dec. 9, 2024), https://www.faa.gov/uas/resources/public_records/uas_sightings_report.

adequate legal authorities to adequately protect the full scope of sensitive facilities and operations affected by illicit drone operations. Congress can remedy this issue by responsibly expanding detection and mitigation authorities to other relevant federal government agencies and functions that currently do not possess these authorities, detection authorities for private sector entities, and limited mitigation authority for state and local enforcement through a pilot program. Expanding the aperture of entities that possess counter-drone authorities conserves limited federal resources and empowers federal agencies to prioritize protecting the most sensitive assets and operations.

We recognize the complexities presented by employing counter-drone technologies, and support placing reasonable and tailored guardrails on expanded counter-drone use to address important policy goals including protecting privacy and civil rights and liberties, ensuring aviation safety, addressing spectrum interference, continuing federal oversight of the national airspace, and allowing lawful commercial activity. However, policymakers should ensure that any counter-drone framework minimizes red tape for law enforcement and the private sector while also being practical to implement. Otherwise, the benefits of expanded detection and mitigation authorities will not be realized.

Ensuring public safety and the security of the national airspace is a priority for the U.S. Chamber, and a tailored, comprehensive counter-drone framework plays a significant role in achieving that objective. We urge you to act on this important issue.

Sincerely,



Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce


BIG SISTER
IS WATCHING
YOU