The Written Testimony of Dr. Catherine F. Cahill
Director, Alaska Center for Unmanned Aircraft Systems Integration (ACUASI) at the University of Alaska Fairbanks (UAF)

U.S. House of Representatives Committee on the Judiciary
Subcommittee on Crime and Federal Government Surveillance

Unmanned and Unchecked: Confronting the Rising Threat of Malicious Drone Use in America

September 16, 2025

Chairman Jordan, Ranking Member Raskin, Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee on Crime and Federal Government Surveillance, my name is Cathy Cahill, and I am the Director of the Alaska Center for Unmanned Aircraft Systems Integration (ACUASI) at the University of Alaska Fairbanks (UAF). ACUASI is the University of Alaska's Center of Excellence for Unmanned Aircraft Systems (UAS), also known as drones, and one of the top UAS research programs in the country. ACUASI leads of one of the seven Federal Aviation Administration (FAA) designated UAS Test Sites, heads one of the eight BEYOND Phase 2 sites, and is a core university in the FAA's UAS Center of Excellence (a.k.a. the Alliance for System Safety of UAS through Research Excellence – ASSURE). We also partner with the best and brightest commercial and governmental entities on the cutting-edge UAS and Counter-UAS (C-UAS) technologies required to safely integrate UAS into the National Airspace System (NAS). ACUASI's diverse portfolio, operational expertise, and academic standing allow us to demonstrate, observe, and evaluate the benefits and risks associated with UAS and C-UAS use in both military and civil environments. Combined, these facts uniquely position me to discuss the topic of the use of malicious UAS. This written testimony is provided to you through my personal capacity as a private citizen and based on my professional experience; it does not necessarily represent the views of the University of Alaska.

Unmanned Aircraft Systems (also known as UAS, UAVs, Remotely Piloted Aircraft Systems [RPAS], or drones) have a tremendous potential to increase aviation safety by doing the dirty, dull, and dangerous flights that currently put pilots of manned aircraft at risk. They also can improve public safety and quality of life through delivering cargo to remote areas, accelerating medical supplies deliveries, providing broadband communications to remote areas, improving maritime domain awareness, facilitating Search and Rescue, assisting law enforcement operations, monitoring infrastructure, and conducting a host of other positive uses. However, UAS also can be used to commit crimes, disrupt airports, interfere with commerce and transportation, conduct war, support terrorism, cause fear, and conduct other malicious acts. As a result, the U.S. needs to develop, test, and implement policies and procedures for use by law enforcement organizations and safe C-UAS technologies that will allow for the safe removal of malicious UAS from the skies by authorized individuals to ensure public safety. A key part of the mitigation of malicious UAS will be the training of all authorized operators about applicable laws governing UAS usage and the benefits and risks associated with using C-UAS technologies. This will allow law enforcement personnel to make educated decisions about how to engage with a malicious operator and their UAS.

As the malicious use of UAS spreads, state and local law enforcement officers will be on the front lines for combating the threats from the rogue drones. Therefore, state and local law enforcement officials need to be educated about what laws are applicable when they encounter a UAS operator conducting careless, clueless, or criminal activities and how to safely resolve the situation whether through engagement with the operator or the use of C-UAS technology to mitigate (e.g., stop the UAS activity or remove it from the air). In my opinion H.R. 5061 Counter-UAS Authority Security, Safety, and Reauthorization Act is a good first step towards safely implementing these technologies in the U.S.

Watching the news or conducting a cursory Google search will result in multiple articles describing the malicious use of UAS. Airports have had near-collisions and stoppages due to UAS being flown over and around the airport[1]. UAS are interfering with wildfire fighting and medical evacuation operations[2]. UAS are being used to bring contraband into prisons[3]. UAS are bringing drugs over the U.S. border[4]. UAS are being used to surveille or damage critical infrastructure[5]. UAS are being flown by drunk operators, over people without the proper safety equipment, to ensure security guards are not near a location, etc.

I live in Alaska, but even in this remote location, our team and partners have seen the malicious use of UAS. We have seen flights of unauthorized UAS in the flight path of Ted Stevens International Airport in Anchorage, one of the top five cargo airports in the world, and near other critical infrastructure. Criminals have used UAS to drop contraband at correctional facilities. We have had wildfire fighting and medical evacuations stopped due to UAS violating the Temporary Flight Restriction (TFR) over the fire. One of our team members was cut by a piece of a UAS flown by a drunk operator that hit power lines and broke apart as it crashed. All of these examples show that malicious UAS activities are widespread and that we need policies, procedures, training, and technologies to allow law enforcement to stop these activities without creating a hazard to people and property.

The first question I always get when I talk to the public about the issue of malicious UAS use is, "why can't we shoot them." The answer is not as straightforward as it would seem. First of all, according to the United States Code (U.S.C.) Section 49 defines UAS as aircraft and all of the laws codified for traditional manned aircraft apply to them. Therefore, shooting a UAS is a Federal offense with applicable jail time and fines. Only five Federal agencies (DOD, DOE, DHS, DOJ, and the FAA) have relief from the U.S.C. sections applicable to shooting down or jamming/hacking UAS, so most law enforcement operators dealing with unauthorized UAS do not have the legal authority to do so. Second, unlike shooting a firearm at a target where you can see what your bullet might hit if you miss the target, if you shoot at a UAS, you usually cannot see what is under the aircraft and might get hit by the falling aircraft or its pieces. Third, basic physics says that what goes up must come down, so the bullet you fired into the air could come down on a person or property. Fourth, you may not be looking at a nearby UAS, but a more distant manned aircraft. A study conducted by the FAA Center of Excellence for UAS Research (ASSURE) shows that even trained observers can have trouble telling how far a manned aircraft is from them[6]. This means it is even more difficult to determine the distance of a small UAS from the observer. Additionally, night complicates the whole situation by making the aircraft and UAS more difficult to see. Fifth, you do not know if the UAS you see is authorized to be flying in that location. You would not want to be liable for shooting down an authorized UAS that could be carrying hundreds

of thousands of dollars' worth of camera or sensor equipment. These factors and multiple others mean that a private citizen shooting at a UAS is a very bad idea.

The recent New Jersey 'unauthorized drones' scare, when FAA-approved UAS, distant planes, and other lights in the sky caused citizens to have concerns about terrorist drones, highlighted the fact that there is not a consensus on who should have C-UAS authority[7]. State and local officials and legislators, and many members of the public, wanted state or local entities to be able to use C-UAS to shoot the 'drones'. In my opinion, the risk of unintended consequences from a mitigation attempt by an untrained state or local entity is too high. The primary job of the state or local official will most likely not be C-UAS operations, and they may not have all of the information about the operation of the UAS of concern and the risks of the mitigation attempt.

The good news is that authorized and trained Federal personnel have multiple types of C-UAS mitigation technologies either in use or under development for their use[8]. Due to the physical and privacy risks associated with conducting C-UAS operations, the authority for conducting C-UAS activities has been limited to five agencies (i.e., DOD, DOE, DHS, DOJ, and the FAA). This ensures the highest level of training, oversight, safety, and security while protecting the public, UAS operators, and others from potential collection and misuse of personally identifiable information or adverse impacts from uninformed mitigation decisions. These agency personnel must determine if the risks due to the rogue UAS outweigh the risks associated with the removal of the UAS. In my opinion, some of the mitigation techniques, such as those involving the physical damaging or destruction of the UAS, should remain with the trained agency personnel due to their risks to aviation and people and property on the ground. I am a little bit more comfortable with allowing the mitigation of UAS using non-destructive techniques, such as hacking and jamming, by state and local law enforcement officials, provided they have extensive training about the potential risks of these systems to First Responder communications, aviation navigation systems, and other critical systems. This will require giving the trained personnel relief from the parts of the United States Code pertaining to hacking and jamming systems (e.g. Title 18).

There are also systems that are capable of detecting, tracking, and identifying (DTI) UAS. The track data collected from the systems can be compiled into maps that show the most common launch and recovery points and flight tracks. Law enforcement officials can use this information to determine where to go to observe potential criminal UAS operations and to catch the perpetrators in the act. Some of these DTI systems allow the system's operator to determine the location of the UAS operator. Law enforcement personnel can use the systems to find the operator of the UAS and educate them about proper drone use if they are careless or clueless or arrest them if they are conducting criminal acts. I am very comfortable with granting state and local authorities permission to use DTI systems that have been tested to ensure no adverse side effects to their use.

Remote ID, a legal requirement that the UAS broadcast its location and identification during operation will allow security officials to separate authorized UAS from unauthorized UAS[9]. However most rogue and home built UAS probably will not be broadcasting RID signals or may be broadcasting false signatures, so other forms of DTI will be needed to determine the location of the rogue UAS and its operator. I would be comfortable with granting state and local governmental DTI operators Title 18 relief to get information about the UAS's operator from the UAS if they are not using Remote ID.

The ACUASI team has been investigating the willingness of local law enforcement officers to engage with DTI systems. In Alaska, for example, we have had difficulty getting local and state law enforcement to address rogue UAS because they are overworked, understaffed, feel it is not their responsibility to do it, and do not know what they can legally do to build a case for the misuse of the UAS. Additionally, many of the law enforcement participants in our study are unsure as to what laws are applicable to malicious UAS use. This includes being unclear as to what is allowed under FAA regulations for recreational and commercial UAS use as well as other regulations, such as operating an aircraft while intoxicated. Our law enforcement/C-UAS project manager describes the situation as everyone standing in a circle and pointing at someone else in the circle as being the responsible party. However, we have found that once the officers see a situation in which the DTI system provides a benefit, they are more willing to engage with the system. One example of this was the recent glacial outburst flooding in Juneau, Alaska. The State of Alaska Department of Transportation and Public Facilities put up a TFR over the river so they could monitor the flooding using their UAS. A DTI system was deployed to monitor the TFR. The DTI system captured a UAS violating the TFR and nearly missing a DOT UAS. The system was able to track the UAS back to its launch point. Local law enforcement officers then went house to house in that area and were able to find and engage with the UAS operator. Another example was when a DTI system tracked a contraband drop into an Alaskan Correctional Facility. The facility, which had been skeptical about the use of a system, immediately requested that all of their personnel be trained as quickly as possible.

We cannot afford to allow criminals to use UAS maliciously or careless or clueless UAS operators to endanger U.S. airspace and people and property on the ground. The U.S. needs to invest in: 1) training law enforcement personnel in how to engage with malicious UAS operators, 2) establishing the requirements for a clear chain of custody for evidence of criminal UAS activities, 3) developing clear guidance for law enforcement about applicable laws, policies, and procedures, and 4) DTI and C-UAS technologies. This investment will help not only our law enforcement organizations here at home, but also our military overseas as they deal with malicious UAS. The U.S. should be the world leader in the development and deployment of these technologies; if we do not move fast enough the criminals and our enemies will win the UAS war.

This ends my prepared statement, and I would be happy to answer any questions you might have.

1.https://www.skysafe.io/blog/drones-and-airplanes-a-growing-threat-to-aviation-safety)

2.https://www.justice.gov/usao-cdca/pr/culver-city-man-agrees-plead-guilty-recklessly-crashing-drone-super-scooper

3.https://nij.ojp.gov/topics/articles/addressing-contraband-prisons-and-jails-threat-drone-deliveries-grows)

4.https://www.newsnationnow.com/us-news/immigration/border-coverage/border-patrol-expands-blimp-surveillance-to-combat-drone-threat/#/questions/5662210

5.https://dronelife.com/2021/11/08/drone-attack-on-u-s-power-grid-failed-this-time/

6. https://assureuas.org/wp-content/uploads/2021/06/A46-Final-Report.pdf

7.https://www.faa.gov/newsroom/dhs-fbi-faa-dod-joint-statement-ongoing-response-reported-drone-sightings

8.https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS-Detection-Mitigation-Systems-ARC_Final-Report_02052024.pdf

9. https://www.faa.gov/uas/getting_started/remote_id

About Dr. Cahill:

Dr. Catherine (Cathy) F. Cahill is the Director of the Alaska Center for Unmanned Aircraft Systems Integration (ACUASI) and a Full Professor of Atmospheric Chemistry at the University of Alaska Fairbanks (UAF). Her educational background includes earning degrees in Applied Physics (B.S.) and Atmospheric Sciences (M.S. and Ph.D.) and researching trans-Atlantic aerosol transport during a Fulbright Fellowship to Ireland that served as her Postdoctoral experience. For many years, her research focused on the sources, transport, transformation, and impacts of atmospheric aerosols, including the effects of atmospheric aerosols on the Warfighter in Iraq and Afghanistan and the long-range transport of pollution from China into the Arctic. To understand the altitudes at which pollution crosses the Pacific Ocean, Cathy needed to make vertical measurements of aerosols in the atmosphere. In 2006, this need led her to start designing aerosol samplers for unmanned aircraft. After a 2014-2015 sabbatical to Washington D.C. in which she served as a Congressional Fellow to the U.S. Senate Committee on Energy and Natural Resources, Cathy returned to UAF and became the Director of ACUASI. Since then, she has participated in the FAA's Beyond Visual Line of Sight Aviation Rulemaking Committee and served on the FAA's Drone Advisory Committee/Advanced Aviation Advisory Committee.