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 Transportation and Infrastructure, Subcommittee on Aviation

Counter-Unmanned Aircraft Systems

February 6, 2025

Chairman Nehls, Ranking Member Cohen, Chairman Graves, Ranking Member Larsen, and Members of the Subcommittee on Aviation, 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) and one of the top UAS research programs in the country. ACUASI leads of one of the seven FAA designated UAS Test Sites, heads one of the eight BEYOND 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 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 C-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, improve cargo delivery to remote areas, deliver medical supplies quickly, provide broadband communications to remote areas, improve maritime domain awareness, facilitate Search and Rescue, assist law enforcement, monitor infrastructure, and a host of other positive use cases. However, it has been demonstrated that UAS also can be used to cause fear, conduct war, disrupt airports, interfere with commerce and transportation, support terrorism, and conduct other nefarious acts. Therefore, the U.S. needs to develop, test, and implement safe C-UAS technologies that will allow the discrimination between authorized UAS, unauthorized UAS, and manned aircraft, allow the safe removal of rogue UAS from the NAS by authorized individuals, and provide a sense of safety to the U.S. population.

Any discussion of C-UAS technologies has to start with the definition of a UAS. 49 U.S.C. Section 44801 states:

(11) UNMANNED AIRCRAFT.-The term "unmanned aircraft" means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.

(12) UNMANNED AIRCRAFT SYSTEM.-The term "unmanned aircraft system" means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system.

This means that UAS are the same as any other aircraft according to the law, and the statutes related to aircraft apply. This makes it harder to legally remove rogue UAS from the airspace.

Also, according to 49 U.S.C. Section 44801:

(5) Counter-UAS system.-The term "counter-UAS system" means a system or device capable of lawfully and safely disabling, disrupting, or seizing control of an unmanned aircraft or unmanned aircraft system.

There are multiple types of C-UAS mitigation (a.k.a., removal from the atmosphere) technologies, but they predominantly fall in to two categories: kinetic and non-kinetic solutions (https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS-Detection-Mitigation-Systems-ARC_Final-Report_02052024.pdf). Kinetic solutions cause direct physical damage to the UAS. Examples of kinetic solutions include: nets, collisions with other UAS, projectiles, and lasers, among others. Non-kinetic solutions use techniques that do not directly damage the UAS, such as disrupting or disabling the UAS's communications, internal processing, or navigation. Examples of non-kinetic solutions include: hacking, jamming, or spoofing Radio frequencies (RF), WiFi, or GPS signals, among others.

There are also systems that are capable of detecting, tracking, and identifying (DTI) UAS in the atmosphere. These detection systems often use one or more RF, radar, acoustic, electro-optical, or infrared sensors to determine where a UAS, and potentially its operator, are located. These systems can be used in a stand-alone manner or as the basis for a mitigation system to locate its target.

One of the challenges of conducting C-UAS activities is that the UAS is, as shown above, an aircraft, so interfering with its flight violates Title 18 U.S.C. (the Aircraft Sabotage Act) and/or 49 U.S.C. (Aircraft Piracy). Additionally, tapping into the communications between the UAS and its operator potential violates several sections of Title 18 U.S.C including the Pen/Trap Statute, the Wiretap Act, the Aircraft Sabotage Act, the Computer Fraud and Abuse Act, and others designed to protect the privacy of U.S. citizens. Therefore, anyone conducting C-UAS activities must receive relief from these statutes or face imprisonment. Additionally, several types of DTI activities run afoul of Title 18, so the operators of those systems must be granted relief as well.

Another challenge of implementing C-UAS technologies is that have the potential to adversely impact authorized UAS, manned aircraft, people or property on the ground, and/or safety systems in the NAS. If a C-UAS system operator disables or destroys a UAS, the UAS, or fragments of the UAS, will fall on whatever is below them or is located wherever they finally crash. This could cause human injuries or fatalities, property damage, risk to other systems (e.g., debris on a runway that could get sucked into the engine of a fighter jet or a damaged UAS hitting a manned aircraft), etc. The person operating the C-UAS system may have no idea what is below the UAS when they mitigate it, so the choice to do so must be made carefully and in coordination with all the stakeholders. Another example of the challenge is that if the C-UAS system jams communications

or navigation systems, other systems operating on those frequencies also will be jammed. This could impact other aircraft in the airspace or systems on the ground. Additionally, even DTI systems can cause problems. Radar systems can produce side nodes and frequencies that are not expected that can interfere with safety systems or communications. The result is that C-UAS, and DTI, systems must be tested for unexpected impacts and used only when the removal of the UAS greatly outweighs the risk of the removal.

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. Additionally, the details of most C-UAS technologies themselves, and especially in conjunction with their effectiveness at a specific facility, are classified due to their value to national security. These agencies must protect our most critical infrastructure, such as military bases, nuclear power plants, large airport hubs, etc. These agencies must establish policies and procedures to better coordinate quickly and effectively between themselves during the C-UAS mitigation decision process to ensure privacy, security, and safety. It would be useful for these agencies to have their authorities renewed for longer periods of time; this challenge is not going to go away quickly and these agencies need to conduct long term planning secure in their authorities.

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 (https://www.faa.gov/newsroom/dhs-fbi-faa-dod-joint-statement-ongoing-response-reported-drone-sightings), highlighted the fact that there is not a consensus on who should have C-UAS authority. 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 a 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. 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. I do not want a local or state official to have the ability to take down a UAS without doing a risk/benefit analysis that includes identifying what is under it, whether it is an FAA-approved UAS operation, whether it is a UAS or a plane, what they can legally do to build a case against the operator, etc. A study (https://assureuas.org/wp-content/uploads/2021/06/A46-Final-Report.pdf) 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. 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. I, personally, want the C-UAS operator to be very cognizant of the risks of the activity, to be sure of the identity of the aircraft (e.g., not a manned aircraft or approved UAS), to know if it is a security operation that would not appear on publicly available sites, to understand the risks to people and property below the UAS, etc. Lastly, I would like the agency making the decision must communicate clearly and early with the public during any 'unauthorized drone' events to assuage the public's fear.

In contrast, I would be very comfortable with granting state and local authorities permission to use DTI systems that had been tested to ensure no adverse side effects to their use. Some of these systems allow the DTI system operator to determine the location of the UAS operator. Law Enforcement Officers would be able to intercept the operator of the UAS and educate them about proper drone use if they are careless or clueless or arrest them if they are being criminal.

Remote ID, a legal requirement that the UAS broadcast its location and identification during operation (https://www.faa.gov/uas/getting_started/remote_id) will increase C-UAS technology's effectiveness by providing information on the locations of all authorized UAS in an area. This will allow security officials to separate authorized UAS from unauthorized UAS. Most rogue 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. If they are not obeying the Remote ID law, then their right to fly in the national airspace should be revoked.

The number of companies able to test C-UAS, and some DTI, technologies is limited because it requires the participation of one of the entities listed above to exercise their authorities to mitigate an aircraft, even the company's own aircraft. This is driving companies to test their technologies in other countries. Ukraine, in particular, has been a hotbed of C-UAS testing due to the needs of the soldiers on the battlefield and the quickly evolving UAS environment. The U.S. should be facilitating the availability of testing locations in the U.S. to enable C-UAS and DTI technology providers to test their systems under a wide range of environmental conditions at a much faster pace. U.S. C-UAS system developers need to be able to move at the speed of UAS technology around the world while maintaining the safety of the U.S. airspace. This includes purchasing and testing new UAS from around the world, including 'covered UAS' that are made, have critical components from, use a ground control systems or operating software from, or use network connectivity or data storage located in the People's Republic of China, the Russian Federation, the Islamic Republic of Iran and the Democratic People's Republic of Korea (https://www.diu.mil/blue-uas-policy). The FAA Reauthorization Act of 2024 (Public Law 118-63) took the first step toward addressing these problems by including language allowing the seven FAA UAS Test Sites to support C-UAS testing and authorizing them to purchase 'covered UAS' for the purpose of providing representative aircraft for C-UAS testing. The FAA and other agencies need to use this avenue for testing C-UAS systems. The FAA UAS Test Sites have strong safety records and operate in a wide variety of environmental conditions, so they can conduct representative tests of the real-world operation of C-UAS systems in climates from hot deserts to maritime locations to humid forests to the Arctic.

ACUASI, as an FAA UAS Test Site, BEYOND site, ASSURE member, etc., has yet to test mitigation systems due to our not having the authority to do so. However, we have conducted DTI testing and we are partnering with organizations possessing the authorities to mitigate UAS in order to test the effectiveness of these systems. We need to test these technologies in Alaska due to our extremely harsh environment, large number of General Aviation and commercial aircraft that could be adversely affected by a C-UAS system, our proximity to Russia, the operation of Chinese vessels and aircraft near our shores, and the number of unauthorized UAS operations over critical military infrastructure.

The U.S. needs to be a leader in C-UAS technology. We cannot afford to be behind our enemies in the testing and implementation of this technology. Our military forces are already under the threat of UAS attack overseas and is only a matter of time until we have a serious UAS attack on U.S. soil. We need our Federal agencies equipped and trained to work together to make the best decision on how to address any UAS attack with minimal impact to the people and property in the area.

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

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.