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. Senate Committee on Commerce, Science, and Transportation, Subcommittee on Security

Drone Security: Enhancing Innovation and Mitigating Supply Chain Risks

June 18, 2019

Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee, 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 UAS and one of the top UAS research programs in the country. ACUASI is unique in that it has multifaceted roles as lead of one of the seven FAA designated UAS Test Sites, is one of the nine UAS Integration Pilot Program (IPP) 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). As a result, our team is engaged with the best and brightest commercial and governmental entities on cutting-edge UAS technologies, helping FAA collect and analyze the data needed to support the safe integration of UAS into the National Airspace System (NAS), and educating the engineers, scientists, pilots and other future UAS users and providers. Our diverse portfolio and academic standing allow us to demonstrate, observe, and evaluate the risks associated with UAS use in military and civil environments. This written testimony is provided to you through my personal capacity as a private citizen and based on my professional experience; however, it does not necessarily represent the views of the University of Alaska.

Counter-UAS (C-UAS) and Detect and Avoid (DAA) technologies are two of the hottest areas for UAS technology development. C-UAS technology identifies potentially hazardous, unauthorized UAS and removes them from the airspace. It is required by DOD, DOE, DHS, DOJ, and the FAA to maintain the highest levels of safety while protecting critical infrastructure and special events and fulfilling other security requirements. DAA technology provides a UAS or its operator with the ability to spot another aircraft in the air and either autonomously avoid it or provide the remote pilot the information needed to avoid it. This technology appears to be one of the technologies that will enable safe UAS operations beyond visual line of sight of the Pilot in Command. Both technologies require the ability to detect UAS so that they can be either mitigated (C-UAS) or moved to avoid other aircraft (DAA). Remote Identification (Remote ID), the ability of a UAS to provide identification information to other parties during flight, could increase both technologies' effectiveness by providing information about the locations of all authorized UAS in an area, thereby allowing UAS users to avoid other UAS and allowing security officials to separate authorized UAS from unauthorized UAS. C-UAS and DAA systems can be based on similar technologies and requirements; however, the ability to test these systems is dramatically different due to their nature. Testing C-UAS technologies is limited due to their potential violation of sections in Title 18 United States Code including the Pen/Trap Statute, the Wiretap Act, the Aircraft Sabotage Act, the Computer Fraud and Abuse Act, and

others, and in 49 U.S.C., under Aircraft Piracy. Additionally, countermeasure technologies are frequently classified due to their value to national security. Therefore, the number of companies able to test C-UAS technologies is limited and requires the participation of one of the entities listed above to access restricted airspace and deploy the countermeasures. In contrast, DAA technologies are being driven by a large number of commercial entities who want to fly beyond visual line of sight for operations including package delivery, infrastructure monitoring, and a host of other missions. These technologies are unclassified; however, many include proprietary information. Even unclassified systems present risks and may violate Title 18 and other laws. Recent FAA studies and guidance[1] show that UAS detection technology deployed at airports has the potential to interfere with aircraft navigation and the control of air traffic. The nature of these systems means that many of the challenges of C-UAS are being solved by commercial entities which could make them easy for foreign entities to acquire. ACUASI, as a UAS Test Site, IPP site, ASSURE member, etc., has yet to test countermeasures because it is not yet legal for us to do so; however, we have direct experience in testing numerous DAA systems.

Unmanned aircraft systems, including their payloads such as infrared cameras, gas detectors, or other instruments carried by the aircraft, are targets for industrial espionage. Some universities and commercial entities focus on the positive impacts of the technology and do not consider the inherent danger or sensitive aspects of the technology. This, when combined with the nature of academic settings, leading-edge academic research, and student workers, makes universities susceptible to industrial espionage and the training of foreign assets in otherwise protected technologies if precautions are not taken. The ACUASI team takes International Traffic in Arms Regulations (ITAR) seriously; we have specially keyed offices, ITAR signage, U.S. citizenship/Permanent Resident requirements, and other security measures in place to protect ITAR controlled aircraft, payloads, and software. Going beyond what's required by law, we've had the FBI train our team in recognizing and preventing industrial espionage. These precautions, on occasion, conflict with academia's tradition of encouraging openness on campus. Because ITAR does not apply to information related to general scientific, mathematical or engineering principles that are commonly taught in college or information in the public domain, engineering departments teach classes in aerospace engineering to foreign students that include building UAS and payloads without consideration of ITAR. Many faculty I have spoken with do not realize that some of the Forward-Looking Infrared (FLIR) cameras used in academic research laboratories or in remote sensing classes are actually ITAR controlled and that allowing foreign students to take them apart, program them, etc. could violate ITAR. This makes universities susceptible for industrial espionage and training in sensitive technologies.

ACUASI works with and advises many public entities about UAS uses and capabilities. One of our challenges is that several of these entities, such as DOD and DOI, have had a prohibition against using foreign-made UAS due to security concerns related to data being sent to other countries. For example, DJI, the Chinese company that dominates the small, commercial UAS market, is the most cost-effective system available for many uses, including law enforcement, but data from DJI UAS was automatically being sent back to the manufacturer in China. DJI claims they now have new settings that the user can use to prevent that from happening. Given the recent reports about Chinese companies being required to provide intelligence to their

[1] https://www.faa.gov/airports/airport_safety/media/Updated-Information-UAS-Detection-Countermeasures-Technology-Airports-20190507.pdf

government upon request, we at ACUASI are hesitant to use any DJI system for any important research or approved flights over critical infrastructure. I confess we fly a small DJI system for public relations footage because it is quiet and produces good quality video, but we take actions to ensure the system is unable to communicate when not in use. The dominance of foreign products in the small UAS realm limits the number of potential U.S.-built platforms we can recommend to our partners and many are cost-prohibitive. ACUASI has partnered with U.S.-based small UAS companies, such as Skyfront, and we are working with them to get their aircraft FAA type certified, meaning designated by the FAA as airworthy, so they will have a competitive advantage over foreign, non-type certified UAS. This effort is being conducted under the IPP. Another way we are working to address the potential security risk of foreign made systems is to modify foreign built systems to operate using an open-source autopilot. For example, we have a DJI S-1000 frame, but it is not running DJI software. Some good news on the viability of the U.S. UAS market is that in the large UAS arena, U.S. manufacturers are producing highly competitive products. ACUASI is moving towards larger, U.S.-built UAS, like our Griffon Aerospace Outlaw SeaHunter, built in Madison, Alabama, to meet industry needs for cargo delivery, long-distance infrastructure monitoring, and other larger-scale UAS uses of special importance to Alaska and other remote areas of the U.S.

Unmanned aircraft systems have a tremendous potential to increase aviation safety by doing the dirty, dull, and dangerous flights that currently put pilots at risk, improve cargo delivery to remote areas, deliver packages quickly, effectively and economically; provide broad-band 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 can also be used to disrupt airports, commerce and transportation, support terrorism, and conduct other nefarious acts. The U.S. needs to ensure that it does not give up security, intellectual property, and UAS manufacturing capacity during this rush to advance the positive aspects of UAS technologies at the lowest cost possible. Our ability to innovate sets the U.S. UAS industry apart from other countries' UAS industries and the U.S. must protect the resulting technology if it wants to continue as a world leader in UAS while maintaining aviation safety and security.

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

About Dr. Cahill:

Dr. Catherine 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 for her Postdoc. 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.