PREPARED STATEMENT OF BRIAN WYNNE
PRESIDENT AND CEO, ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

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, thank you very much for the opportunity to participate in today's hearing. I'm speaking on behalf of the Association for Unmanned Vehicle Systems International, the world's largest non-profit organization devoted exclusively to advancing the unmanned systems and robotics community. AUVSI has been the voice of unmanned systems in all domains for more than 40 years, including unmanned aircraft systems (UAS).

On August 29, 2016, the FAA implemented the small UAS rule, also known as Part 107. The rule was the result of years of collaboration between government and industry that established a flexible, risk-based approach to regulating UAS. This new regulatory framework helped reduce many barriers to low-risk civil and commercial UAS operations, allowing businesses and innovators to harness the tremendous potential of UAS and unlock the many economic and societal benefits the technology offers.

Since Part 107 was implemented, the demand for UAS has grown exponentially and the United States UAS market has become stronger and more robust. It is the largest national market in the world for UAS and likely to remain so for the foreseeable future. According to the AUVSI Unmanned Systems and Robotics Database, which documents the introduction of UAS as well as unmanned systems in other domains, the United States has developed more unique UAS platforms than any other country; and nearly twice as many as the second-largest UAS producing country. It also has more than triple the number of manufacturers in comparison, with 44 states having at least one UAS manufacturer.

From examining pipelines and newsgathering to helping first responders conduct search and rescue operations, UAS help save time, save money and, most importantly, save lives. It is no wonder why thousands of businesses – small and large – have embraced this technology, and many more are considering integrating UAS into their future operations. As of last month, more than 1.4 million drones

had been registered with the FAA, more than 400,000 of which are registered for commercial operations. While the vast majority of UAS operators follow the appropriate rules, occasionally bad actors threaten to undermine the great progress we have made. Careless and clueless operators can pose safety risks and paint responsible, legal UAS operations in a negative light, while criminal behavior can jeopardize the security of our airspace. As the number of UAS in our nation's airspace continues to grow, it is vital our regulatory framework around UAS evolve to address these potential security challenges and ensure technologies are put in place to detect, identify and mitigate UAS which may pose a threat.

Congress took a positive step when it granted additional authorities to the Department of Homeland Security and the Department of Justice as part of the FAA Reauthorization Act of 2018, including the authority to deploy appropriate countermeasures against UAS that threaten security. Congress also gave limited authorities to the Departments of Defense and Energy in the 2017 National Defense Authorization Acts. In addition, Section 2209 of the FAA Extension, Safety and Security Act, which was also adopted in the FAA Reauthorization Act, created a process through which state and local government entities can petition the FAA to prohibit or restrict the operation of a UAS in close proximity to a fixed-site facility, such as critical infrastructure.

As we consider what more needs to be done, it is critical that we approach UAS security from an overall airspace management perspective. That is, we need to address the issue in the context of the complete solution, rather than focusing solely on how to interdict an errant drone. We must meet three conditions in order for this approach to be successful. First, we need to develop a holistic framework for detecting, tracking, identifying, and mitigating UAS. Second, we need to secure UAS command and control connections and the data UAS collect. Finally, we need to put in place well-defined procedures for how to respond to potential security threats, which includes clarity about who has the authority to engage.

Let me first discuss detection, tracking and identification (DTI) technologies as well as mitigation technologies. A critical component for the future of DTI technologies is remote identification. It will enhance the security of the national airspace and allow law enforcement officials to quickly identify, track and apprehend operators acting carelessly, recklessly, maliciously or illegally. A comprehensive remote ID system would serve as a firewall of sorts. It would allow recreational and commercial operators flying in compliance with the appropriate rules to continue to do so unabated while providing law enforcement with the means to identify, and subsequently mitigate, the careless, clueless or potentially criminal operators.

The implementation of a remote identification system would not just alleviate security concerns; it would also serve as the linchpin needed to advance the UAS industry beyond what is currently possible. It is vital for the realization of a UAS Traffic Management (UTM) system, which would work alongside the existing air traffic control system to reduce barriers to innovation and improve security of the national airspace. It is also critical for the ultimate realization of expanded operations, including flights over people or beyond line of sight. That will help make operations like package delivery – and even autonomous air taxi service – a reality in the coming years.

As for mitigation technologies, also known as counter-UAS technologies, these will provide a way to interdict UAS that may pose a threat. According to MITRE, there are two primary types of mitigation technology: electronic, such as jamming the radio frequency or GPS signal from the UAS; and kinetic, such as capturing the UAS with a net or use of powerful lasers.

The UAS industry has been hard at work developing remote ID systems as well as other DTI and mitigation technologies. The FAA, in collaboration with industry, is developing the rulemaking process that will one day codify remote ID standards. Meanwhile, industry is refining those standards and looking for ways to voluntarily provide remote ID on a tactical basis for certain situations. It is my hope that these efforts by the industry will help to accelerate the rulemaking process. What is more, there may be the need to clarify or expand authorities to deploy appropriate countermeasures against UAS that are deemed a threat. Currently, UAS mitigation authority is limited to the Department of Defense, Department of Energy, Department of Homeland Security and the Department of Justice.

Recent incursions around airports including Gatwick Airport in the United Kingdom and Newark Liberty International Airport in the United States demonstrate that more needs to be done and at a faster pace than the regulatory process allows. If remote identification standards were in place, the operators responsible for those incidents could have been identified and tracked within a matter of minutes, mitigating the safety threat and potentially avoiding disruptive airport closures. Additionally, authorities could have used electronic countermeasures that take command and control of an errant platform to help mitigate the threat. These solutions exist, but here in the United States, the framework to deploy them remains in development.

In the interim, we cannot stand idly by. That is why AUVSI and the Airports Council International-North America recently commissioned a Blue Ribbon Task Force on UAS Mitigation at Airports. The Task Force, co-chaired by former FAA Administrator Michael Huerta and Los Angeles World Airports CEO

Deborah Flint, is studying the issue of UAS detection, tracking, identification, and mitigation in and around airports. The panel includes a cross-section of stakeholders representing the airport, UAS and manned aviation communities, and will provide recommendations to airports and the federal government to refine procedural practices in response to incursions and provide a policy framework to address this timely and critical issue. The Task Force also will consider comments from the public and meet with experts in government, national security, law enforcement, pilots, air traffic controllers and airline and airport leadership, to develop and release initial findings this summer.

While the purview of the Task Force is mitigation around airports, we are optimistic that its findings and recommendations could serve as a blueprint to inform future conversations about UAS security at other facilities, such as national landmarks, stadiums, prisons, military bases, and other critical infrastructure. As such, we plan to share any data the Task Force collects with the FAA to ensure that any solutions we identify will help inform future rulemakings and conversations about UAS mitigation across the national airspace. We will also make sure the Task Force's reports are shared with Chairman Sullivan, Ranking Member Markey, and members of the subcommittee.

The work of the Task Force is separate from, but complementary to, industry-government partnerships currently underway to develop effective UAS detection and mitigation solutions. Last year, AUVSI collected more than 40 white papers on remote identification solutions from industry stakeholders to help the FAA meet its congressional directive under the 2016 FAA reauthorization extension to develop consensus for such standards.

In addition, the Drone Advisory Committee (DAC), a federal advisory committee of which I am a member that provides the FAA with advice on key UAS integration issues, considers remote identification and UAS mitigation two of its top priorities. We discussed these topics at length in our meeting earlier this month, and we formed task groups to delve further into both remote identification and counter-UAS. Eventually, the DAC will provide consensus-based recommendations to the FAA to help inform its future rulemakings on these matters.

The FAA's UAS Integration Pilot Program is another important industry-government partnership. It brings together state, tribal and municipal governments with UAS industry leaders and academic institutions to collect data and conduct critical research. Nine projects across the country, from Alaska to Virginia, are currently conducting research that will not only help inform the federal UAS policy framework

for detection and mitigation, but also advance expanded operations such as flights beyond line of sight and even package delivery.

Importantly, the UAS Integration Pilot Program allows state and local entities to provide input without infringing upon the FAA's sovereignty over the U.S. airspace. Federal authority over the airspace has been a bedrock principle of aviation law for more than 70 years, and it is one of the reasons that the U.S. maintains an aviation safety record that is the envy of the rest of the world. AUVSI has been in discussions with our government partners responsible for national security, and we will continue to work with policymakers to ensure that government agencies have the authority to keep America's skies safe and secure while maintaining federal sovereignty over the U.S. airspace.

Security of the nation's airspace is paramount, but we must also ensure that the data collected, retained, transmitted or shared after UAS flights is also secure. In 2015, the National Telecommunications and Information Administration (NTIA) convened representatives from government, industry, and civil liberty groups to develop a set of best practices for UAS privacy, accountability, and transparency to ensure that UAS operators are flying responsibly. AUVSI participated in this process, and the resulting best practices include clear guidance for operators for how best to collect, store and secure data.

The industry is also working with government partners to develop data management and risk mitigation strategies. For example, since 2015, industry partners have been working collaboratively with the Department of the Interior (DOI) to define, understand, and address data management concerns. AUVSI appreciates that the solutions to challenges should come from those who understand, know, and use unmanned technologies. DOI has been a leader among the federal agencies in the use of UAS, and its work on this subject matches AUVSI's longstanding principle on cybersecurity calling for industry-driven consensus security standards, and cautioning against "[p]rescriptive regulation or government-imposed requirements."

Finally, we also cannot ignore the importance of education in deterring careless, clueless or criminal behavior. The legions of new UAS operators may not all be aware of the FAA regulations that determine where they can and cannot fly. AUVSI, the Academy of Model Aeronautics and the FAA partnered to launch the Know Before You Fly campaign in December 2014 to provide these new flyers with information about how to fly safely and in compliance with applicable rules and guidelines. In fact, the FAA recently issued new guidance for recreational operators, and new rules for recreational flyers are also under development. As the regulatory environment evolves, educating flyers and raising awareness

of new requirements can help increase compliance. Recognizing the continued importance of education, our organizations also recently signed a new memorandum of agreement that solidifies our commitment to expanding and improving Know Before You Fly over the next three years.

Much has been accomplished so far because government and industry have banded together to advance UAS. We share the same goals – supporting innovation while at the same time ensuring the security of the national airspace – which has made for a working relationship that is defined by both productivity and mutual respect. Thanks in part to our strong partnerships, the United States UAS market is stronger and more robust than any other country. To ensure domestic UAS companies continue to flourish, we need to accelerate the federal rulemakings.

The security of our airspace is a serious issue that should be addressed from an overall airspace management perspective. Only by working together can industry and government develop holistic policy solutions that give us the framework we need to keep the skies secure while still allowing the nascent UAS industry to truly take off. Thank you, again, for the opportunity to speak today. I look forward to answering any questions the committee might have.