Testimony of

Jeffrey L. Troy
Executive Director
Aviation Information Sharing and Analysis Center, Inc.

Before the
Committee on Homeland Security
U.S. House of Representatives

September 6, 2018

Good morning. My name is Jeffrey Troy. I am the Executive Director of the Aviation Information Sharing and Analysis Center. The Aviation ISAC is a global, member-driven, non-profit corporation. Our member companies are headquartered on 5 continents and represent a cross section of the many businesses making up the aviation industry ecosystem. They include the makers of aircraft, engines, airlines, airports, air traffic control, ground traffic control, satellite communication providers, and aviation services as well as their supply chains. The mission of the Aviation ISAC is to increase the cyber resiliency in aviation worldwide.

Safety comes first in every aspect of the aviation industry, and cybersecurity is no exception.

Each segment of our industry has numerous automated, computer-based processes, which contribute to the overall safety and efficiency of aviation. Each member of the Aviation ISAC has a Chief Information Security Officer (CISO) or someone comparable who assumes the responsibility of protecting computer networks and products performing the operations of the business from cyberattacks. The Aviation ISAC works with each CISO to understand their company's risk profile. We use this information to drive industry cooperation and collaboration on projects and programs to reduce cyber risk.

The Aviation ISAC builds communities of experts within each of the specialties supporting the CISO. These include Cyber Threat Analysts, Compliance Experts, Network Security Architects and Product Security Specialists. Each community leverages the combined experience and intelligence capabilities of the members to expedite the development of solutions and intelligence to reduce or eliminate risk.

We facilitate automated and in-person intelligence exchange, training, best practices, and table top exercises. We proactively hunt for threats, stolen network access, indicators of compromise and engage with threat researchers. Our focus is on finding information that can be used by the aviation industry to reduce cyber risk and increase operational resilience.

Every business and every industry, including aviation, can only succeed when the needs and concerns of their customers are met. This includes addressing misperceptions. Flying is the safest mode of transportation. However, there have been times over the past few years when persons incorrectly alleged they were able to impact flight safety by hacking a system on a plane.

The Aviation ISAC has addressed these issues head on. Working with industry and coordinating with government partners, we play a leading role in investigating alleged vulnerabilities, and conducting extensive testing to ferret out any vulnerabilities validated or invalidated. The Aviation ISAC recognizes the value of the work of cybersecurity researchers in finding cyber vulnerabilities, even if those vulnerabilities are minor, contained, and do not pose a risk to safety. The aviation industry will continue to investigate vulnerability claims and take swift action when required. As of today, none of the vulnerabilities that have been investigated by the Aviation ISAC or its members have impacted the safety of flight.

The Aviation ISAC also is pleased to have a strong and productive relationship with our government partners. Indeed, liaison with government was a founding idea behind the creation of the ISAC. We collaborate in many forums and on a wide scope of aviation, cybersecurity related projects. For example, in a recent engagement with a threat researcher who sensationalized a claim of being able to “hack a plane,” we kept both our industry members and government partners well apprised of our work to include the sharing of technical details. We engaged with the Department of Homeland Security, Transportation Security Administration, the Federal Aviation Administration and the European Aviation Safety Agency.

The aviation industry, like all industries with extensive digital integration, has not declared victory, but rather is constantly engaged in the battle.

As I said earlier, in aviation, safety comes first. Digital enhancements to processes are adopted at a deliberate pace to ensure no impact to safety. Security around the digital processes begins in the design stages and runs through the build, deploy, operate and continuously monitor phases. Airframers and their suppliers extensively test new technologies and design layered safety and security controls, both digital and physical, to ensure the highest level of assurance in flight safety.

We do not know what we do not know. Many vulnerabilities in computer systems were discovered years after the systems were designed and deployed. And new technologies are being added to existing platforms. As such, our industry is constantly red-teaming their systems and seeking to uncover issues before they become impactful.

We believe safety and security are significantly enhanced when companies and government agencies communicate on cyber threats and vulnerabilities. On behalf of all our members, I thank you for the opportunity to come before you today and answer your questions about cybersecurity and cyber resilience in the aviation industry.