MEDIA STATEMENT

For Immediate Release
Contact: media@a-isac.com
Twitter: @AviationISAC

Aviation Industry Affirms the Safety of Commercial Aviation

Aviation Information Sharing and Analysis Center sets the Record Straight on Safety and Security of Aircraft

9 August 2018—The Aviation Information Sharing and Analysis Center (A-ISAC) affirmed today there is no risk to commercial aviation and passenger flight safety following statements delivered in a briefing by IO Active at today's Black Hat 2018, a cyber security conference. Though the brief highlighted the aviation industry's outstanding work to address safety and security issues, the industry is concerned about technical errors presented in the talk.

The aviation industry designs, builds, and operates its systems with safety as the core requirement. The industry continuously performs rigorous safety testing on its equipment and infrastructure, and multiple levels of encryption and protection exist for all aviation systems.

In fact, years ahead of this paper, the aviation industry theorized the attack and manipulation scenarios concerning WiFi systems and impact of radio frequency (RF) antennas installed on planes. Physical, digital, and process controls were designed, implemented and tested to prevent any negative outcome.

In the month preceding Black Hat, the Aviation ISAC worked with its trusted community partners to research IOActive's claims and recreate IO Active's tests on equipment used on board commercial airplanes. Working together, industry partners disproved the ability to execute any scenarios impacting safety of flight. Similarly, the industry disproved that a manipulation of antenna systems would not lead to an event of any consequence.

Despite ending their presentation with affirmation that flight safety was not at risk and that RF attacks could not be made using antennas on planes, the presentation included technical errors. For example, the physical design of the equipment prevents downward trajectory of RF beams and other physical engineering controls and process controls would trigger the system in-operable if used to emit RF waves beyond the designed strength. The configurations and capabilities described in the talk do not reflect deployed systems.

-- continued --

The Aviation ISAC worked with the Federal Aviation Administration (FAA), European Aviation Safety Agency (EASA) and Department of Homeland Security (DHS) in the analysis of this presentation.

The Aviation ISAC supports the work of researchers working to find security issues which would improve the resiliency of the entire aviation eco-system. Researchers can contact the Aviation ISAC at a-isac.ops@a-isac.com.

Jeffrey Troy, Executive Director of the A-ISAC concluded: “The Aviation ISAC and its member companies are committed to the responsible and ethical disclosure of potential risks to the aviation and the satellite communication industries. We are obligated to set the record straight in that there are significant controls built into satellite equipment which neuter the ability of the equipment to be used maliciously as proposed.

-- 30 --

About the Aviation ISAC

The Aviation ISAC (A-ISAC) was founded in 2014 by seven international aviation companies to help protect global aviation businesses, operations and services. Our vision is a safe, secure, efficient, and resilient global air transportation system. The A-ISAC analyzes and shares timely, relevant and actionable cyber security information as it pertains to threats, vulnerabilities, and incidents. The A-ISAC enables its members to share threats in real time, understand how to tactically combat threats and implement mitigation strategies, enhance association sector knowledge and implement best practices. A non-profit organization, A-ISAC membership is open to trusted private sector aviation companies in any part of the world. For more visit: www.a-isac.com.