THE WALL STREET JOURNAL.

http://www.wsj.com/articles/panel-reaches-preliminary-agreement-on-airliner-cybersecurity-standards-1465848030

BUSINESS

Panel Reaches Preliminary Agreement on Airliner Cybersecurity Standards

Proposals include cockpit alerts in event that critical safety systems are hacked

Flight controls are seen inside the cockpit of an Airbus A350-900 aircraft. The preliminary agreement would include new in-flight warnings. *PHOTO: BLOOMBERG NEWS*

By **ANDY PASZTOR**

June 13, 2016 4:00 p.m. ET

A panel of government and aviation-industry experts has reached a preliminary agreement on proposed cybersecurity standards for airliners, including the concept of cockpit alerts in the event that critical safety systems are hacked, according to people familiar with the matter.

Some of the recommendations, these people said, incorporate work already under way to create an entirely new category of automated in-flight warnings—intended to directly notify pilots if navigation signals are jammed or corrupted. Such safeguards for ubiquitous Global Positioning System satellite broadcasts aren't widely available today, and regulators typically don't mandate them on any aircraft.

But the proposals envision that these and other provisions would be incorporated into a broad package of future cyberprotections and enhanced airworthiness requirements applying to both new and existing aircraft. Commercial and business planes certified during the past several years already feature some more-stringent cyberprotections, though the recommendations are expected to go further.

The coming report will be the most comprehensive move yet to lay the groundwork for global regulations combating potential cyberattacks against aviation.

The advisory group is expected to call for an array of changes affecting airliners, business jets and even small, private planes powered by propellers. Creating different levels of protection for each category, however, continues to be one of the most challenging goals, and last-minute disagreements could change the final outcome.

RELATED

- U.S., European Aviation Authorities at Odds Over Cybersecurity (http://www.wsj.com/articles/u-s-european-aviation-authorities-at-odds-over-cybersecurity-1450816124) (Dec. 22)
- Airline Trade Group Warns About Cybersecurity Threats (http://www.wsj.com/articles/airline-trade-group-warns-about-cybersecurity-threats-1436444810) (July 9, 2015)
- U.S. Panel Aims to Shield Planes From Cyberattack (http://www.wsj.com/articles/u-s-panel-aims-to-shield-planes-from-cyberattack-1435537440) (June 29, 2015)

Without spelling out specific security measures or technology, the recommendations are expected to urge tighter restrictions for accessing ground-based maintenance computers that routinely transfer data on and off aircraft, according to people familiar with the details.

Stepped-up controls would extend beyond determining who can log on to such networks. Experts are considering future additional safeguards for those maintenance computers connected to the internet, which pose greater intrusion risks.

In addition, the group favors enhanced efforts to ensure the integrity of software used in laptops, called electronic flight bags, increasingly used by pilots of commercial, business and private planes.

The U.S. Federal Aviation Administration kicked off the process last summer amid escalating concerns by plane makers, equipment suppliers and regulators world-wide about the industry's overall vulnerability to hackers. There has never been a verified in-flight incident of unauthorized access to airplane safety systems, but the topic of verifying incoming GPS signals is steadily attracting more attention.

"The FAA and aviators are worried, particularly in the past 12 months, about spoofing of GPS," which means sending fake signals to navigation and flight-control computers on board planes, according to Matt Desch, chief executive of Iridium Communications Inc., a commercial-satellite operator with aviation customers. The company recently introduced a service that "can be used to check a GPS signal or provide an alternative," he said.

The FAA has instructed panel members not to talk publicly about their deliberations before an expected progress report during a U.S.-European safety conference in Washington, D.C., that starts Tuesday. An FAA spokeswoman didn't respond to requests for comment.

The advisory group isn't expected to go beyond generic recommendations, stopping well short of prescribing specific technical fixes.

The recommendations are being drafted by a federally created committee with more than three dozen members and observers, ranging from Boeing Co. and Airbus Group SE to Honeywell International Inc. to air-safety regulators from Europe and Brazil.

Boeing, which co-chairs the advisory panel along with the trade association representing small-plane makers, has been blunt about potential threats.

Mike Delaney, Boeing's vice president of aircraft development, told an industry conference Monday: "You have to worry about the direct attack, you have to worry about the indirect attack" from ancillary operations.

Along with U.S. officials, Patrick Ky, Europe's top aviation-safety regulator, has emphasized the importance of ensuring that air-traffic-control systems don't become conduits for bogus information.

The findings are to be delivered to the FAA in late August, though translating sweeping, high-level recommendations into detailed technical standards is likely to take at least a year. Implementing them will take significantly longer.

—Jon Ostrower contributed to this article.

Write to Andy Pasztor at andy.pasztor@wsj.com