Issued 6/11/18

Government: It is only a Matter of Time until a Commercial Airline is Hacked

Motherboard got its hands on a number of government documents via Freedom of Information Act request, which yielded internal presentations and risk assessments from DHS. The agency has been looking into potential vulnerabilities in commercial aircraft and found that most planes lack necessary cybersecurity protections, which is not reassuring. A portion of the documents come from a presentation put together by the Pacific Northwest National Laboratory (PNNL), a research group that is part of the Department of Energy. The lab conducted tests earlier this year in which it attempted hack an aircraft via its wifi internet service. The presentation, dated January 10, 2018, seems to suggest PNNL succeeded in part, noting that researchers were able to “establish actionable and unauthorized presence on one or more onboard systems.” What the research does make clear is the fact that they view a potential hack of an airplane as a viable threat and one that should be taken seriously. “Potential of catastrophic disaster is inherently greater in an airborne vehicle,” part of the presentation said. Another troubling part claims that it’s just “a matter of time before a cyber security breach on an airline occurs,” the document adds. While the PNNL documents come from earlier this year, DHS has been probing the possibility of a cyberattack against commercial airplanes for a while. A document from 2017 reported that “early testing indicates that viable attack vectors exist that could impact flight operations.” A team of researchers at the agency reportedly successfully hacked the electronics systems of a commercial aircraft last year, bolstering

concerns that malicious actors could make planes a target for attack. DHS stated in a 2016 presentation that “most commercial aircraft currently in use have little to no cyber protections in place.” Per the presentation, most current aircraft have about a 20-year or longer lifecycle, which means “15-20 years of higher cyber vulnerability.”