Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

20 April 2015

Alert Number
150420-001

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov
Phone:
1-855-292-3937
Local Field Offices:
www.fbi.gov/contact-us/field

(U) FBI and TSA Analyzing Claims in Media Concerning Intrusion Vectors into Onboard Avionics

(U) The FBI and TSA are currently analyzing claims in recent media reports which included statements that critical in-flight networks on commercial aircraft may be vulnerable to remote intrusion. At this time, the FBI and TSA have no information to support these claims but continue to leverage public and private sector partnerships to evaluate potential threats posed by intrusions into a commercial aircraft's secure networks. The FBI and TSA also continuously monitor and analyze reporting on cyber and technical threats to proactively deter individuals from using remote intrusions to disrupt any portion of the aviation sector, including its business networks, critical navigation and air traffic control signals, and the onboard networks of commercial aircraft.

(U) Claims in the Media Suggest Vulnerability

(U) Statements in the media allege that an intrusion into a commercial aircraft's onboard avionics and wireless networks in the aircraft's cabins or through the aircraft's In Flight Entertainment (IFE) network poses a credible vulnerability. Specifically, the claims are that cyber actors could intrude into the onboard network systems and disrupt or disable the controls of an aircraft by exploiting vulnerabilities in the airplane's wireless network or the aircraft's IFE, and focus on Boeing and Airbus models: Boeing 757-200, Boeing 737-800, Boeing 737-900, and Airbus A-320.

(U) Monitoring of Cyber Threats to Aircraft

(U) FBI and TSA evaluate potential cyber or other technical threats to commercial aircraft's avionics networks. The FBI and TSA work with other government agencies and leverage private sector partnerships to prevent or deter individuals from attempting to use remote intrusions to disrupt any portion of the aviation sector, including its business networks, critical navigation and air traffic control signals, and the onboard networks of commercial aircraft and to decrease the likelihood of any malicious cyber intrusions into commercial aircraft.

(U) Airlines and Flight Crews Should Remain Vigilant To Avoid Intrusion Attempts into Airplanes

(U) Attempting to gain unauthorized access to the onboard networks of a commercial aircraft violates federal law. The FBI recommends that airline employees remain vigilant for intrusion attempts or similar activity. Although the media claims remain theoretical and unproven, the media publicity associated with these statements may encourage actors to use the described intrusion methods. The FBI advises its private partners to take the following steps to help mitigate the risks of potential cyber incidents aboard aircraft:

- (U) Report any suspicious activity involving travelers connecting unknown cables or wires to the IFE system or unusual parts of the airplane seat.

- (U) Report any evidence of suspicious behavior following a flight, such as IFE systems that show evidence of tampering or the forced removal of covers to network connection ports.

- (U) Report any evidence of suspicious behavior concerning aviation wireless signals, including social media messages with threatening references to Onboard Network Systems, ADS-B, ACARS, and Air Traffic Control networks.

(U) Review network logs from aircraft to ensure any suspicious activity, such as network scanning or intrusion attempts, is captured for further analysis.