Michael P. Delaney
Vice President
Engineering
Commercial Airplanes

The Boeing Company
P.O. Box 3707 MC 03-UC
Seattle, WA 98124-2207

January 11, 2016

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Markey,

On behalf of The Boeing Company, I write to address your inquiry on the integration of technology on commercial airplanes.

Through a collaborative partnership, the Federal Aviation Administration with stakeholders in the aviation industry continuously addresses safety standards. As you know, the aviation system is complex and constantly changing given the pace of emerging technologies, the introduction of new products and the increasing volume of air travel around the globe. Accordingly, it is imperative that all stakeholders in the aviation system work cooperatively to improve safety. Our collective efforts have produced a reliably safe system.

Your letter cites two examples I want to address head on: (1) the alleged hacking of an inflight entertainment (IFE) system from onboard a Boeing aircraft, and (2) the Government Accountability Office (GAO)'s April 2015 report entitled "Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen".

Firstly, your letter references a Washington Post article concerning an alleged IFE hacking onboard a Boeing aircraft. While it would be inappropriate to comment on an official investigation that was referenced in that article, Boeing's own investigation and analysis have concluded that the claims are patently false and that no vulnerability was found.

Secondly, the GAO report focused primarily on concerns with the Next Generation air traffic control system. That report contains key technical information that is factually incorrect. Accordingly, the report should not be considered as a definitive source on the systems architecture on board modern commercial airplanes. The Boeing Company has stated previously that it disagrees with elements of the report relating to how systems on board commercial airplanes are networked.

The Boeing Company's cybersecurity measures are subject to rigorous testing, including through the FAA's certification process. We consistently partner with regulators, our customers, subject matter experts and the aviation industry on security matters as a founding and active member of

The Boeing Company
P.O. Box 3707
Seattle, WA 98124-2207

the Aviation Information Sharing and Analysis Center (A-ISAC). For its part, The Boeing Company is committed to designing airplanes that are safe and secure and meet or exceed all applicable regulatory requirements for both physical and cyber security.

The Boeing Company is committed to the highest standards for the cybersecurity of its airplanes. Multiple layers of protection, including software, hardware, and network architecture features, ensure the security of all critical flight systems. Given the sensitivity of these issues, we would be happy to provide more information to you and your staff in a closed setting. The Boeing Company, the aviation industry and governments around the world share a vision for the safe and secure movement of people and commerce.

Sincerely,

Michael P. Delaney
Vice President, Engineering
Boeing Commercial Airplanes