United States Senate
WASHINGTON, DC 20510

December 2, 2015

Mr. W. Douglas Parker
Chairman and Chief Executive Officer
American Airlines Group Inc. & American Airlines Inc.
P.O. Box 619616, MD 5675
DFW Airport, TX 75261

Dear Mr. Parker:

I write to request information regarding your airline's protections and protocols against the threat of cyber-attacks in relation to the integration of new technologies onboard your company's aircraft. I also write to inquire into your airline's storage and processing of passenger data, and how your company protects against threats of cyber-hacking and unwarranted invasions of privacy.

As new technologies continue to enhance all aspects of the airline industry, airplanes and airline operations have become increasingly interconnected. With these technological advancements come great benefits, including improved flight navigation, greater communications abilities, and greater operational efficiency. However, as we have witnessed recently in the automobile industry,[1] I am concerned that these technologies may also pose great threats to our security, privacy, and economy.

Multiple airline carriers have already experienced problems with their computer systems, causing substantial delays and the grounding of thousands of flights across the nation.[2] One airline's computer system was reportedly breached, and hackers stole sensitive flight and personal information on millions of airline passengers.[3] Further, a passenger earlier this year allegedly hacked into the inflight entertainment system from onboard a plane, potentially gaining access to the critical flight systems that control the movement of the aircraft.[4] Finally, the Government Accountability Office (GAO) issued an April 2015 report addressing the increasing

---

[1] Edward J. Markey, Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk, A report written by the staff of Senator Edward J. Markey (D-Mass.), (February 2015), *available at* http://www.markey.senate.gov/news/press-releases/markey-report-reveals-automobile-security-and-privacy-vulnerabilities.

[2] *See, e.g.*, Michael Sasso and Lauren Thomas, *United Computer Failure Spanned Multiple Systems as Woes Persist*, July 8, 2015, *available at* http://www.bloomberg.com/news/articles/2015-07-08/united-computer-failure-spanned-multiple-systems-as-woes-persist.

[3] *See* Michael Riley and Jordan Robertson, *China-Tied Hackers that Hit U.S. Said to Breach United Airlines*, July 29, 2015, *available at* http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines.

[4] *See* Justin Wm. Moyer, *Hacker Chris Roberts Told FBI he Took Control of United Plane, FBI Claims*, May 18, 2015, *available at* https://www.washingtonpost.com/news/morning-mix/wp/2015/05/18/hacker-chris-roberts-told-fbi-he-took-control-of-united-plane-fbi-claims/.

connectedness of modern aircraft, raising important concerns about possible unauthorized access to aircraft avionics systems.[5]

These recent examples highlight just some of the potential vulnerabilities airlines already face. As technology rapidly continues to advance, we must all work to ensure that the airline industry remains vigilant in protecting its aircraft and systems from cybersecurity breaches and attacks.

As a member of the Committee on Commerce, Science, and Transportation and Subcommittee on Aviation Operations, Safety, and Security, I write to ask you the following questions:

1) What protections does your company currently have in place to protect your company's planes from cyberattack?
    a. What protections exist for your planes' onboard flight-critical systems (e.g., auto-pilot, engine, steering, thrust management)?
    b. What types of defenses are in place to protect your planes' computer systems from viruses, malware, and other third-party infiltrations?
    c. Are your onboard computer systems capable of detecting, isolating, and recovering from intentional or inadvertent unauthorized cybersecurity intrusions?

2) Have you already installed, or do you plan to install on aircraft, communications systems that will allow passengers to use in-flight wireless services? If yes, please explain.

3) Onboard flight-critical systems, onboard non-flight-critical systems, and maintenance/ground-support systems often interact with each other to successfully perform their intended functions. How does your company ensure that cyber-threats in a non-critical system do not penetrate or compromise the onboard flight-critical system?
    a. Could a passenger gain access to the onboard flight-critical system through a hard-wire connection to the inflight entertainment system? If yes, please explain how. If no, please describe the measures used to prevent this type of infiltration.
    b. Could a passenger wirelessly gain access to the onboard flight-critical system from aboard a plane through a Wi-Fi network? If yes, please explain how. If no, please describe the measures used to prevent this type of infiltration.
    c. Could a person on the ground gain access to the onboard flight-critical system (e.g., through a cellular network, non-flight-critical onboard systems, or aircraft maintenance or ground support systems)? If yes, please explain how. If no, please describe the measures used to prevent this type of infiltration.
    d. As the industry transitions to NextGen, will this change your company's current assessment of cyber-threats? If yes, how do you plan to deal with changes in cybersecurity resulting from this transition?

4) Do you conduct cybersecurity tests on your planes' computer systems? If no, why not?
    a. If yes, how often do these tests occur? If no, why not?

---

[5] U.S. Government Accountability Office; *AIR TRAFFIC CONTROL: FAA needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen;* GAO-15-370: Published: Apr 14, 2015. Publicly Released: Apr 14, 2015.

b. If yes, who conducts these tests? For example, are the tests conducted internally within your company, or are they also conducted by independent third parties?
c. If yes, what countermeasures does your company take to remedy any found cybersecurity vulnerabilities?

5) Who installs and updates your planes' computer software?
   a. Are software installations and updates conducted solely by personnel employed by the airline? If yes, do you require security background checks of those employees? If no, why not?
   b. If third parties conduct or are involved in updating and installing software, for whom do those third parties work? Do you require security background checks of those third parties? If no, why not?

6) For *each* of the past five years, please list and fully describe all instances in which your company was made aware of an infiltration to any of your company's systems or aircraft systems, including but not limited to onboard flight-critical systems, onboard non-flight-critical systems, maintenance/ground support systems, or airline reservation systems. Please describe any:
   a. Alleged intentional efforts to infiltrate one of your company's systems;
   b. Inadvertent infiltrations of one of your company's systems;
   c. Intentional or inadvertent introduction of malicious code into one of your company's systems.

   For each instance, please indicate the model and year of the aircraft involved (if applicable), the date on which the instance occurred, any personal injury or property damage alleged to have occurred as a result of the instance, any information or data taken, whether the instance was reported to federal authorities, and what changes, if any, were made to your planes or systems to protect against similar vulnerabilities from being exploited in the future.

7) What protections does your airline currently have in place to protect flight customer data processed and held by your company's computer systems and servers, including flight itinerary information and other sensitive information?
   a. Does your company store this data on company-owned servers, in the cloud, or both?
   b. What policies does your company have in place for the storage of this data? For example, do you encrypt customer data? If yes, please explain how. If no, why not?
   c. Do you make efforts to remove certain personal identifying information?
   d. For what length of time is this data stored?
   e. Do you share this data with third parties?
      i. If yes, with whom and for what purpose? For example, do you share this data with marketers or data brokers?
      ii. If yes, what is the process for releasing the information?

8) Have you collaborated with the Department of Transportation, Department of Homeland Security, Transportation Security Administration, Federal Air Marshals, the Federal Bureau of Investigation, or other agencies to gather their input on these concerns and possible mitigations of cyber-threats?
    a. If yes, please provide a summary of the agencies contacted and their feedback. If no, why not?
    b. Similarly, have you collaborated with other airline industry stakeholders and cybersecurity experts on these matters? If yes, with whom? If yes, what have the collaboration efforts involved and do you plan to continue these efforts in the future? If no, why not?

Thank you for your attention to this important matter. Please provide written responses to these questions no later than January 11, 2016. If you have any questions, please have a member of your staff contact Joseph Wender or Michal Freedhoff at 202-224-2742.

Sincerely,

Edward J. Markey

Edward J. Markey