United States Senate
WASHINGTON, DC 20510

December 2, 2015

Mr. Allan McArtor
Chairman and Chief Executive Officer
Airbus Group Inc.
2550 Wasser Terrace, Suite 9100
Herndon, VA 20171

Dear Mr. McArtor:

I write to request information regarding your company's protections and protocols against the threat of cyber-attacks in relation to the integration of new technologies onboard the aircraft designed and manufactured by your company.

As new technologies continue to enhance all aspects of the aircraft 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.

The airline industry, including airplane manufacturers, has recently come under scrutiny over the need to keep airplanes secure from cyber-threats. The Government Accountability Office (GAO) issued an April 2015 report addressing the increasing connectedness of modern aircraft, raising important concerns about possible unauthorized access to aircraft avionics systems.[2] 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.[3]

These recent examples underscore just some of the potential vulnerabilities today's aircraft already face. As technology rapidly continues to advance, we must all work to ensure that the airplane manufacturing 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] 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] 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.

[3] *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/.

1) What protections does your company currently have in place to protect planes your company manufacturers from cyber-attack?
    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, or other third-party infiltrations?
    c. Are your onboard computer systems capable of detecting, isolating, and recovering from intentional or inadvertent unauthorized cybersecurity intrusions?

2) Does your company install 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 design and manufacture planes to 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 the 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) After a plane manufactured by your company is purchased, does your company continue to test and monitor the plane's computer systems for cybersecurity vulnerabilities? If no, why not?
    a. If yes, how often do these tests occur? If no, why not?
    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) For *each* of the past five years, please list and fully describe all instances in which your company was made aware of:
    a. An alleged intentional effort to infiltrate the computer systems of a plane manufactured by your company;
    b. An inadvertent infiltration of one of the plane's computer systems;

c. The intentional or inadvertent introduction of malicious code into one of the plane's computer systems.

For each instance, please indicate the model and year of the aircraft involved, the date on which the instance occurred, how your company was notified about the infiltration (e.g., by an airline operating the aircraft), 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 to protect against similar vulnerabilities from being exploited in the future.

6) Has your company 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/aircraft 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