allegiant®

January 28, 2016

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building
Washington D.C. 20510

Dear Senator Markey,

We are in receipt of your December 2, 2015 letter wherein you requested information pertaining to Allegiant's cyber-security practices and policies. As you know, cyber-security is a critical component of our industry and Allegiant takes every precaution to ensure our aircraft and company servers remain uncompromised.

As technology and cyber-defense systems continue to advance, so too advances the sophistication of existing and emerging cyber-security threats. Consequently, Allegiant invests, and will continue to invest, significant resources to protect and defend our critical and non-critical cyber-systems.

Of course, many aspects of Allegiant's cyber-security systems are confidential and proprietary. Therefore, we respectfully request that you hold and keep this letter, and all information contained herein, confidential. In that light, please find below the questions posited in your letter, followed by Allegiant's response.

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?

Cyber-attacks and cyber-security intrusions pose virtually no threat to Allegiant aircraft. The computers on Allegiant's aircraft are hard programmed and not connected to any outside system or network. Any attempts to physically download software that includes malware or a virus would be rejected by the target computer as the software would not match the embedded data. Consequently, the physical download would fail.

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?

No. None of our planes have in-flight wireless services available to passengers and we have no plans to add anything that would make such services available.

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 the changes in cybersecurity resulting from this transition?

Allegiant utilizes extensive levels of cyber-security protection to protect core and non-core Allegiant information systems. Firewalls, malware protection, intrusion prevention systems, and continuous monitoring, among other things, keep critical and non-critical systems operating and free from malware, viruses, and other threats. As our aircraft are not equipped with inflight entertainment systems or Wi-Fi, accessing any systems via these mediums is not possible. We will continue to employ detective, protective, and preventative controls, and modify these controls as needed to protect against emerging threats and changing environments.

4) Do you conduct cyber-security tests on your planes' computer systems? If no, why not?
   a. If yes, how often so these tests occur?
   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 and found cybersecurity vulnerabilities?

As our aircraft computer systems are not connected to any network, there is no need to conduct such tests. However, we have taken steps to ensure that physical downloads of malware or viruses to aircraft computer systems would be rejected.

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?

Allegiant maintenance staff installs and maintains aircraft computer software. All Allegiant personnel are subject to an extensive background check, including a criminal history review and verification of prior employment. Maintenance personnel undergo a fingerprint-based criminal history records check as required by federal law. (*See* 49 CFR § 1542.209 Fingerprint-based criminal history records checks (CHRC)). In the event it is necessary to have a third party, such as the original equipment manufacturer (OEM), perform software-related work on an aircraft, all such contracted vendors are subject to prior approval. The approval process requires a vendor to show that they are certified as an aircraft repair entity pursuant to 14 CFR §145, which includes the background screening requirements of 49 CFR § 1542.209, meaning their personnel are subjected to the same background screening requirements.

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.

Attacks and probing attempts to infiltrate internet facing systems are an ongoing, daily event. These types of attacks are not out of the ordinary for a significant e-commerce platform similar to the type that Allegiant operates. However, despite the frequency of the attempts, there have been no successful infiltrations, whether intentional or inadvertent.

7) What protections does your airline currently have in place to protect flight customer fate 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?

c. For example, do you encrypt customer data? If yes, please explain how. If no, why not?
d. Do you make efforts to remove certain personal identifying information?
e. For what length of time is this data stored?
f. Do you share this date 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?

Allegiant stores customer data on company-owned servers for a period of ten (10) years. Customer data is protected via firewalls, malware protection, intrusion prevention systems and continuous monitoring. Further, Allegiant utilizes encryption and tokenization as an additional safeguard. We do not share this data with third parties.

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?

Yes. We have collaborated with the FBI on several occasions – specifically through the InfraGard program, in addition to other similar programs. Additionally, we have collaborated with other industry stakeholders, including both passenger and cargo airlines, regarding best practices, as well as emerging threats. We expect these conversations with our industry peers and government agencies will continue.

Again, thank you for raising awareness regarding this critical issue. We trust you will find the foregoing responsive to the questions posited in your letter. However, should you require any additional information, please do not hesitate to contact me.

Sincerely,

Keith Hansen
Director, Airports & Government Affairs
702.830.8446