

Southwest Airlines Co.  
David Richardson, Esquire  
Director, Governmental Affairs  
919 18th Street, N.W. – Suite 600  
Washington, D.C. 20006  
(202) 263-6287 – Office  
(202) 263-6291 – Fax  
david.richardson@wnco.com



January 11, 2016

VIA EMAIL & HAND-DELIVERED

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

Dear Senator Markey:

On behalf of Southwest Airlines, I write in response to your December 5, 2015, letter concerning cybersecurity. Although Airlines for America (A4A), our industry trade association, submitted the attached response on behalf of its members, including Southwest Airlines, I write to further stress that the Safety of our Employees and Customers is Southwest's top priority – which has remained unchanged during our 45-year history. To be clear, the cyber threat is real, and we cannot stress enough how seriously we treat this threat.

Over the past several years, Southwest has devoted a tremendous amount of time and resources to upgrading and protecting our information systems. And these investments continue to grow each and every year, as we constantly monitor our operations and systems to identify existing and future risks, conduct thorough risk assessments, and take appropriate measures to manage or eliminate such risks.

Moreover, the sharing of cyber threat information in real-time is critical to ensuring our internal protections remain robust and up-to-date. We are very encouraged that, after many years of effort, Congress has finally adopted cybersecurity information sharing legislation in December 2015. While our Company has partnered with key federal agencies, as well as our equipment manufacturers, technology vendors, and various other subject matter experts – including via our active involvement with the Aviation Information Sharing and Analysis Center (A-ISAC), of which we are a founding member – the additional federal direction and protections should allow for greater cooperation and information sharing, especially when federal intelligence/security agencies know of potential threats to our systems.

Senator, we sincerely appreciate and respect your concerns about this extremely important issue. And, considering the sensitivities surrounding this issue, we would welcome the opportunity to more thoroughly address your questions and concerns via a private briefing. I am happy to work with your staff to schedule such a briefing with Southwest's Chief Technology Officer.

The Honorable Edward J. Markey

January 11, 2016

2

In general, if you or your staff has any questions or comments with respect to this issue, please contact me at (202) 263-6287 or [david.richardson@wnco.com](mailto:david.richardson@wnco.com).

Sincerely,

A handwritten signature in cursive script, reading "David Richardson".

David Richardson

Attachment

Copy to: Mr. Gary C. Kelly, Chairman, President & CEO  
Southwest Airlines Co.

Mr. Craig Maccubbin, Vice President & CTO  
Southwest Airlines Co.



## Airlines for America®

*We Connect the World*

David A. Berg  
Senior Vice President, General  
Counsel & Secretary

January 11, 2016

The Honorable Edward J. Markey  
United States Senate  
255 Dirksen Senate Office Building  
Washington, D.C. 20510-2107

Dear Senator Markey:

I am responding on behalf of the members of Airlines for America that received your recent letter concerning their respective programs to deter cyber-attacks against aircraft systems and to protect passenger data from such attacks. We very much appreciate your interest in these significant issues.

Cyber-attacks are malicious and potentially disruptive attacks on often critically important information systems. They can have grave consequences, both for the target and others affected. Cyber-attacks are associated with a variety of individuals or organizations, including state-related actors. These considerations mean that national policy must not only recognize the responsibilities of individual private-sector entities but also that a collaborative approach between government and the private sector is indispensable in dealing effectively with such attacks.

The U.S. commercial aviation industry—airlines, manufacturers and service providers—as well as federal agencies with aviation responsibilities, have understood for some time the importance of cybersecurity. Airlines have focused considerable attention and extensive resources on creating and upgrading information systems and practices to deter cyber-attacks. These are ongoing, continuous efforts. Cybersecurity demands that kind of attention and our members are committed to it.

A4A members defend against malicious cyber activity and maintain the integrity of their customers' personally identifiable information in a number of ways. This integrated effort includes:

- carefully investigating and monitoring identified and emerging cyber threats;
- developing and improving internal standards and controls, both with respect to deterring cyber-attacks, and by restricting access to and protecting passenger information;
- using and following established cross-industry standards and industry-standard best practices;
- complying with the guidance of equipment manufacturers and service providers;
- adhering to applicable regulatory guidance;
- employing industry-leading virus and malware protection;
- performing rigorous self-evaluations and audits;
- closely liaising with federal agencies with cyber-security responsibilities, such as the Federal Bureau of Investigation; and
- exchanging pertinent experience both within and outside of the aviation industry.



Airlines depend on a variety of third-party hardware, software and system providers that either manufacture or provide services for them. This, of course, includes the Federal Aviation Administration's air traffic control system. This reliance underscores the complexity of airline operations and the consequent need for collaboration in this area, something that airlines engage in diligently.

With respect to onboard systems, aircraft in-flight systems and entertainment systems are not connected to each other and as a result cannot be used to attack each. Consequently, they face different security threats. Likewise, flight control and other operations systems are well protected by imbedded manufacturer cyber-security systems against intentional or inadvertent malicious access. Such cyber-security systems employ established NIST and ISO standards and carefully crafted protocols. Entertainment systems do not enable access to onboard flight systems. To protect these systems, our members utilize elaborate, industry-leading virus and malware protections, including industry malware detection and removal standards. In performing these functions, our members remain in close contact with the manufacturers of the equipment to better respond to emerging threats.

In performing these threat-mitigation functions, airlines test, typically through internal resources, aircraft electronic systems. Identified anomalies are promptly addressed and, as needed, with the assistance of the manufacturer.

Our members are aware of the need to maintain the integrity of their aircraft navigation and communications systems during the transition to NextGen, just as with any transition to a new system. We also recognize, as does the FAA, that the FAA has a central role in assuring that integrity. We have and will continue to collaborate with airframe, equipment and systems manufacturers, the FAA and other federal agencies about this matter.

Our members work with a variety of federal agencies to maintain the integrity of data that they transmit to these agencies and in combatting cyber threats associated with them. For example, airlines transmit throughout the day pre-departure passenger information to both the Transportation Security Administration and Customs and Border Protection. An important element of the interface between airlines and those agencies is maintaining and improving data-security protocols.

Of particular interest to us is the role of federal agencies in tackling cyber threats. We believe that the federal government has a central role in fostering effective cooperation and information sharing, especially when federal intelligence or security agencies know of potential threats to airline systems. We hope that the recently enacted Cybersecurity Information Sharing Act of 2015 will be such a facilitator. We also hope that the Office of Foreign Asset Control's publication on December 31 of regulations implementing Executive Order 13694 ("Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities") will deter malicious cyber actors.

An additional area in which the U.S. Government can be an especially useful facilitator is in helping resolve conflicts between foreign governments' sometimes contradictory policies about handling passenger information. Such contradictory policies can create conflicts of law and unnecessary challenges for U.S. airlines with international operations.

Airline passenger reservations contain personally identifiable information about customers. Airlines that operate international flights transfer that information, typically in the form of passenger name records. For example, a reservation may be made in a foreign country on a U.S. airline and then sent to the airline's reservation system in the United States. Airlines maintain tight safeguards over this necessary collection and commercial flow of information.

A problem can arise for us when countries demand passenger information for aviation security and border-control purposes. One foreign government's requirement that airlines supply passenger information to it for such purposes can conflict with the restrictions that the country in which the information was collected imposes on the transborder transmission and use of the information. This has

occurred most notably for passenger information collected in the European Union. The insoluble issue in these situations is that the airline can be confronted with contradictory instructions from the two governments which it has no authority to resolve. As more countries enact data-privacy legislation, this is likely to become increasingly burdensome for U.S. airlines with international operations. In light of that, we believe that the U.S. Government should adopt a policy of assisting in mediating these foreign intergovernmental conflicts, to the extent that they affect U.S. airlines.

Airlines also work closely with federal agencies that have responsibility for responding to and mitigating cybersecurity threats, including the FBI, with which we have a close and ongoing relationship. Federal agencies are quite valuable because they can have access to information and analyses that we in the private sector do not. This reality underscores the importance of a vigorous collaborative approach between government and the private sector.

Your interest in these issues is timely and appreciated. We would be happy to meet with you or your staff to expand upon our responses in this letter. Given the sensitivities of the matters to be discussed in such a meeting, it would be preferable that such a meeting be closed.

Sincerely,

A handwritten signature in black ink, appearing to read "D. A. Berg", with a long, sweeping horizontal stroke extending to the right.

David A. Berg