AIRBUS
GROUP

11 January 2016

The Honorable Edward J. Markey
United State Senate
255 Dirksen Senate Office Building
Washington, DC 20510-2107

Dear Senator Markey,

Thank you for your letter dated December 2, 2015. Allan McArtor, Chairman and CEO of Airbus Group, Inc., has asked that we respond to your inquiry regarding our company's efforts and activities in the area of cyber-security.

The civil aviation sector is experiencing a very rapid integration of new technologies, including the extensive use of communications and connectivity technologies that are essential in meeting the growing demands of our industry. Without proper precautions the use of these critical technologies could result in an increased exposure to cyber-security threats.

Airbus recognizes that potential threat, and along with other members of the civil aviation community, has placed the highest priority on identifying and addressing threats to aircraft security, including cyber-security and other external safety risks. From the very beginning of our company, and in close collaboration with government oversight authorities and our customers, Airbus implemented a robust effort to manage security in the design, production and operation of all our aircraft.

This effort is led by a senior Airbus executive who directs a dedicated organization focused on identifying potential cyber-security threats and developing protective measures. Airbus has continued to strengthen its cyber-security focus and capabilities through the expansion of this internal security organization, the creation of an Aircraft Security Users Panel and ongoing participation with government and industry oversight organizations tasked with setting and overseeing safety of flight protocols.

Given that certain facets of our industry could be impacted by cyber-security threats, Airbus has from the very beginning advocated a collaborative approach to the development and promulgation of cyber-security protective measures and technologies. We actively participate in this holistic and systemic approach to addressing cyber-security threats and interact with international, federal, local and industry in developing initiatives and efforts aimed at thwarting cyber-security threats.

The aviation cyber-security environment continues to evolve. As such, the Airbus cyber-security organization is constantly anticipating, identifying and evaluating potential security threats and implementing effective countermeasures.

Cyber-security systems, protections and protocols are very sensitive and highly proprietary to Airbus. Thus, you can appreciate that we cannot disclose in writing all the specifics of our security principles. However, we are able to provide the following points that reflect the questions raised in your letter.

Airbus places the highest priority on creating a safe and secure flight experience for our customers. Every step of the aircraft design, manufacturing, test and delivery process is hyper-focused on flight safety—including protection from both current and emerging cyber-security threats. The following principles guide our cyber-security approach:

- Execution of a formal aircraft security management system:

  Information/ Cyber Security is fully embedded in all aircraft development phases, including concept, specification, implementation, validation, verification, and industrial activities. Airbus has developed and implemented a robust Information/Cyber Security Management system (Aircraft Security Management System) built upon recognized NIST or ISO security standards. This security management system is operated by highly experienced security and aircraft specialists who are supported by independent third-party security professionals. All of the Airbus aircraft, whether in the "e-enabled" configuration or not, benefit from these activities.

- Employing a layered defense-in-depth strategy:

  Cyber-security defense strategies built upon a foundation of layered defense and defense in-depth protocols are implemented to manage cyber security risks linked to remote, close-in, and direct unauthorized access to airborne systems in their overall life-cycle. These defense strategies contemplate all currently known and foreseen security threat sources (purposeful attacks either from the outside/inside of the aircraft or casual or accidental viral infections during operation and planned maintenance of aircraft systems.)

- Pursuing a continuous improvement process

  The aircraft security activities and defense strategies are regularly reviewed and assessed through procedural and technical (i.e., penetration testing) evaluations, constantly updated and reflecting security environment evolutions or a detected security event.

As reflected above, Airbus takes a broad, systemic approach to ensuring cyber-security, including aircraft flight control systems, aircraft-to-ground data and communication links. In this way, Airbus is continually engaging with the entire civil aviation industry to raise awareness of emerging threats and to develop effective partnerships with all contributing stakeholders to aviation security.

This "community" approach to aviation security has been at the heart of our cyber-security strategy since the very beginning. In the end, the aircraft is the "last line of defense" against cyber-security intrusions. Hence the need for a coordinated industry and government approach.

Broad aviation stakeholder coordination and collaboration will promote:

- Designing and implementing streamlined, gap-free, and affordable security strategies that mitigate cyber-security risks to a minimum,
- Quickly adjusting the strategy according to identified security environment evolutions (vulnerabilities, threats, incidents) through rapid information sharing,
- Identifying and correctly assigning the responsibilities of each member of the security community, as Original Equipment Manufacturers (OEMs) cannot address threat issues or be responsible for modifications made under STC (Supplemental Type Certificate) after aircraft delivery, or for the Buyer Furnished Equipment (BFE) which are out of the Type certification process of the OEM (for example the In-Flight Entertainment system (IFE) or the engines).

U.S. government agencies, including the Department of Transportation, Department of Homeland Security, Transportation Safety Administration, Federal Bureau of Investigation and the Federal Aviation Administration, as well as many international organizations and trade associations, play a critically important role in thwarting cyber-security threats.

Airbus maintains an ongoing accountability to and collaboration with relevant government agencies, international organizations and trade associations responsible for identifying and addressing safety and security issues. We actively contribute to the creation of standards and protocols that support safety of flight in all areas and are actively engaged developing and establishing cyber-security "best practices" in our industry, including:

- Airbus is actively engaged with governments and airworthiness rulemaking bodies to integrate cyber-security in regulations applicable to the civil aviation sector (including ICAO, EASA, FAA, and CEAC)
- Airbus is actively participating in many local, regional and international think tank and working group initiatives launched by the industry (including ASD, and Industry High Level Group) aimed at understanding and anticipating security threats, and at developing risk response plans.
- Airbus also participates, and chairs, industry standards initiatives jointly coordinated by European (EUROCAE) and U.S. (RTCA) industry standards bodies.

- Airbus collaborates with many governmental entities and agencies tasked with civil aviation transport and law enforcement. We seek their inputs and correspondingly provide them our experience and potential mitigations to cyber-security threats.

In conclusion, an important element in addressing evolving cyber-security threats in the aviation area is the fact that there is healthy collaboration between manufacturers in the area of security and flight safety. We all take this responsibility seriously—and collectively.

Thank you for the opportunity to respond to your letter. I would be pleased to follow-up with you or your staff.

Sincerely,

Guy M. Hicks
Senior Vice President
Government Relations
Airbus Group, Inc.

Dr. Pascal ANDREI
Vice President
Chief Product Security Officer & Executive
Expert Head of Aircraft Security
Airbus