UNITED STATES COPYRIGHT OFFICE

Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201

[ ] Check here if multimedia evidence is being provided in connection with this comment

ITEM A. COMMENTER INFORMATION

As a consumer advocacy organization, we have limited our comments to copyright and policy questions raised by the proposal, rather than a technical analysis of relevant TPMs, methods of circumvention, and market players.

These comments are submitted by Air Informatics LLC. Air Informatics is a for-profit company addressing the business challenges of the new generation of digital aircraft, providing information, communication, analytics, informatics and cyber security services to the e-Enabled Aviation community.

Interested parties can contact Bruce Jackson, bruce.jackson@airinformatics.com as the representative in this request. Air Informatics can be contacted at:

Air Informatics, LLC
800 Fifth Avenue, Suite 4100
Seattle, WA 98133
206 801-1893

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 11: Computer Programs—Avionics

ITEM C. OVERVIEW

The development of aircraft has evolved to incorporate information technology in the design, function and maintenance of aircraft of all types. The aircraft recently develop and entering into fleet operations are digital, software and data intensive, and connected. Core to these aircraft is an

integrated centralized computerized flight systems interconnecting the control and information avionics subsystems of the aircraft. Older aircraft are being updated with information and communications system to more effectively fly and maintain the aircraft. Satellite communication systems have been installed for passenger entertainment and connectivity, as well as aircraft data and flight crew communications.

FAA document FAR 8900-1, Volume 3, Chapter 61, Paragraph 2-4892 "Aircraft Network Security Program," states "New aircraft designs use advanced technology for the main aircraft backbone connecting flight critical avionics as well as passenger information and entertainment systems in a manner that makes the aircraft an airborne interconnected network."

These aircraft are typically considered to be "e-Enabled." Examples of these aircraft are not restricted to type or size. These digital aircraft are manufactured by all the aircraft companies and incorporating software embedded avionics components made by a variety of avionics manufacturers. The Airbus A350, Boeing 787, Gulfstream G650 and others typify these aircraft.

It is widely recognized that the collection and analysis of sensor and component information and data has been responsible for dramatic increase in the safety and business effectiveness of past generations of aircraft. It is anticipated this new generation of aircraft will further increase the safety and business efficiency.

These aircraft create and hold large volumes of data that, when analyzed, address and improve flight safety, quality assurance, flight operations and security. The types of data include flight operations, fuel economy, digital flight data recorder, maintenance, fault and information security. The data is collected during ground and flight operations of the aircraft and is considered to be the property of the aircraft owner.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

The information, data, files and security logs are transfers in a protected format either encrypted or using a PKI process. The process includes the collection of the log, information or data in a folder that is then compressed. The individual digital information elements can be encrypted. The data folder, known as a "crate", is transferred from the aircraft to the aircraft owner, maintainer or operator using a PKI process. The transfer is completed by an 802.11 secure connection, typically using WPA 2 security protocol. The wired means is typically through a maintenance laptop with secure cryptographic digital certificate protocols in place.

Circumventing the Technical Protection Mechanisms is difficult and a function of the current state of art security practices. It is common that the aircraft and avionics manufacturers do not use the most current and best available security practices. The adopting of best practices

as defined by NIST and others is most frequently delayed to the end of the recommended adoption period. While difficult, the circumvention means maybe known. This slow adoption the most advanced means of protection further the need for the review of the security logs to detect any malicious third party actions.

The request for the exemption does not alter the ownership of the data, nor does it allow the unauthorized collection or use of the data. The data is only available to a third part by the specific authorization by the aircraft owner or operator. The avionics component manufacturers have included digital encryption, public key and other forms of technical protection means to restrict access to the data.

This exemption request does not include the removal of protections to prevent the unauthorized interception of information. The exemption is to allow the circumvention of the technical protection mechanisms when authorized by the owner or operator of the aircraft. The use of this information is to review and analyze the data that is necessary to improve flight safety, operations, efficiency and security.

The circumvention, review and analysis of the sensor, security, quality and flight information is conducted in a controlled setting such as in an office or data management environment. The data would not be exposed in any real time flight operations setting.

The requested exemption does not provide any risk to aircraft or flight safety. The exemption is to allow in the analysis and review of data to enhance the safety and security of aircraft. The FAA has mandated the review of the data, information, logs and other information as a means to ensure safety, security and regulatory compliance. This exemption allows highly skilled and knowledgeable individuals to support the airlines in their efforts to comply with federal regulations, improve operations, provide quality assurance, reduce unsafe operations and pilot errors.

The availability of the data allows researchers the opportunity to increase flight safety, quality assurance, maintenance and security. This circumvention also allows educational institutions the opportunity to work with samples of actually information, data and log in an education and training setting. There is a growing lack of skilled staff trained in the digital management, maintenance and security of e-Enabled aircraft.

The bulk data, in the form of files and logs, requested does not include software embedded in the avionics components. Modification of any embedded software is under the strict control and certification by the FAA and not allowed. The operator installation and use of any software (typically known as a Loadable Software Aircraft Part) is restricted only that which is FAA certified and approved for use. The operator is maintenance activities are subject to review, inspection and enforcement. Un authorized modification is strictly prohibited. The format of the data is defined and is publically available through the various aviation standard bodies.

The tremendous increase in the complexity of the aircraft, on-board computers, sensors, digital systems, data volume and wireless connections pose new challenges. The Federal Aviation Administration has recognized this challenge. In addition to the regulations the FAA has put forward to certify components and software regulations exist to allow only FAA certified components and software (LSAP) the maintenance by airlines and strict oversight of operations.

The level of the FAA efforts to ensure the safety and security of the aircraft data is evident in the recent effort regarding information security for e-Enabled aircraft. New policies have been put in place to address the information security challenges. Over two-dozen aircraft have been identified as needing special conditions for the certification of the aircraft and the continued operation of the digital, data and software intensive connected aircraft now operated by the airline and business jet owner and operators.

The FAA has published a National Policy N8900.358, "Aircraft with Electronic System Security Special Conditions." This document identifies 'aircraft needing special operational and maintenance procedures regarding electronic security." The FAA has released Advisory Circular, AC No: 119-1, "Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP)" The purpose of which is to describe "acceptable means, but not the only means, of obtaining operational authorization for an aircraft certified with a special condition (SC) related to security of the onboard computer network." In that document it states, "current designs have adopted several technological advances such as Internet Protocol (IP) connectivity to capitalize on speed and weight savings. This advanced technology can be found not only in new aircraft designs but also in post-delivery modifications."

As a means to ensure the security and safety of the aircraft, the avionics components and sensors produce and deliver data that represent the status or proper function of the individual component or aircraft operation. Each of the major components delivery this information to common collection point. The aircraft also poles avionics components and system to determine function, status and security. The aggregate of this date is collected in a bulk data format as files and logs. This forms a collection of bulk information for delivery off the aircraft. Log and data file are collected into a digital folder, compressed, encrypted or incorporate other form of technical protection mechanisms. This bulk data is then available for delivery to the operator or owner for review, safety and security analysis. The data can be delivered by secure wireless and wired means.

The FAA, OEMs and industry have determined that to maintain the security and safety of the aircraft the security logs must be downloaded, reviewed and analyzed on an ongoing basis. This is called out in the manufacturers manuals such as the Boeing Document, "Airplane Network Security Operators Guidance (ANSOG). The necessity to collect the data is also defined by FAA regulations, industry standards and guidelines.

The download and review of these logs are based on the industry standard, RTCA DO-

355, "Information Security Guidance for Continued Airworthiness" and FAA Regulations. The purpose of the analysis is to detect a security incident or event. The action of downloading and review of the security logs are completed as a routine and on going task. The aviation standard groups have addressed the data collection, format and use. The development of this guidance is considered a collaborative effort and the format are considered non-proprietary, including security log content and formats.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

The circumvention of the copyright will not impact the existing market of copyrighted work, the embedded software of the aircraft avionics components. The need for copyright avionics software will not be impacted. The increasing complexity of aircraft ensures the continued and increasing need for aircraft software and software embedded avionics. The need for security aware software and avionics components will increase. The aviation and avionics industry is increasing and has a greater need for security. The research and education value of the exemption will increase the knowledge and the availability to skilled staff.

The ban of circumvention has several direct and immediate impacts. It limits the development of the avionics and data analytics market to those who write the software and develop the components. The ban will severely limit the growth of the third part analytics market and discourage new entrance companies. Innovation will be hampered and stifled. The growth of the e-Enabled aircraft development and sale will continue and increase.

Individual operator data is required to be stored and maintained by the operator or owner. The use of the information and data described has an airline community value. The collection, aggregation and analysis of de-identified information serve the aviation community for the purpose of research and on-going operational analysis. De-identified data can be used to identify trends, past and emergent, and predictive analytics. This is similar to the aggregation of de-identified disease and health data to determine public health of a community and the active on-going process for the detection of emerging infectious disease and syndromic surveillance.

The airlines currently do not have experienced and knowledgeable staff. The ban on circumvention will hamper educational and limit the training and availability of knowledgeable aviation staff. Research initiatives will be limited and the development of advanced methods to address cyber security threats will be reduced.

Only with the further review and subsequent understanding of the operational, safety, maintenance and security data will the risks to the industry, operators and aircraft be addressed. If the security, maintenance, quality assurance challenges of these data intensive are not addressed the e-enabled aircraft growth will be hampered.

Air Informatics LLC addresses the digital airplane and the operators need for understand

5

the large data that these aircraft generate. Without circumvention of the technical means to control the data the analysis and analytics will not be possible and operation of the aircraft and the operator will suffer.