Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Service Rules and Procedures to Govern	)	IB Docket No. 05-20
the Use of Aeronautical Mobile Satellite	)	
Earth Stations in Frequency Bands	)	
Allocated to the Fixed Satellite Service	)	

COMMENTS OF
THE DEPARTMENT OF JUSTICE, INCLUDING THE FEDERAL BUREAU OF INVESTIGATION, AND THE DEPARTMENT OF HOMELAND SECURITY

Laura H. Parsky
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Room 2113
Washington, D.C. 20530
(202) 616-3928

Elaine Dezenski
Acting Assistant Secretary for Policy and Planning
Border and Transportation Security Directorate
United States Department of Homeland Security
Nebraska Avenue Complex
Washington, D.C. 20528
(202) 282-8446

Patrick W. Kelley
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.
Room 7427
Washington, D.C. 20535
(202) 324-8067

Tina W. Gabbrielli
Director of Intelligence Coordination and Special Infrastructure Protection Programs
Office of the Assistant Secretary for Infrastructure Protection
United States Department of Homeland Security
Nebraska Avenue Complex
Washington, D.C. 20528
(202) 282-8582

TABLE OF CONTENTS

SUMMARY

The Commission's *Notice* — in which it makes proposals to facilitate the use of two-way satellite-based broadband communications and data capabilities onboard aircraft — raises important public safety and national security issues.

The United States Department of Justice ("DOJ"), including the Federal Bureau of Investigation ("FBI"), and the Department of Homeland Security ("DHS")[1] (collectively, "the Departments") support the Commission's efforts in this and related Commission proceedings to promote the efficient use of spectrum and to enable important new communications services to be provided to passengers, aircraft crew, and law enforcement officers on board aircraft. The Departments take this opportunity, however, to identify for the Commission various public safety and national security-related concerns that stem from the Commission's proposals. In light of the concerns associated with the Commission's proposals, the Departments believe the Commission's inquiry into the appropriate regulatory and licensing framework for the use of two-way satellite-based broadband communications and data capabilities, devices, and services onboard aircraft must consider public safety and national security as well as commercial equities by expressly including an analysis of the potential

[1] The Department of Homeland Security, includes, *inter alia,* the following agencies with equities in this proposed rulemaking: the Bureau of Immigration and Customs Enforcement ("ICE"), including the Federal Air Marshals Service ("FAMS"), the Transportation Security Administration ("TSA"), the Bureau of Customs and Border Protection ("CBP"), the United States Secret Service ("USSS"), and the United States Coast Guard ("USCG").

impact that the Commission's proposal and resulting actions could have on public safety and national security. The Departments believe that the timely roll-out of new commercial airborne communications capabilities can be accomplished in a responsible manner, without unnecessary delay, which both encourages and rewards private sector investment and expedited development while addressing the Departments' public safety and national security concerns. The Departments support such an approach, which will benefit not just the flying public but will lend significant support to the vital mission of law enforcement onboard "at risk" flights and, in that respect, can be viewed as a critical factor in enhancing the safety of those flights.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Service Rules and Procedures to Govern the Use of Aeronautical Mobile Satellite Earth Stations in Frequency Bands Allocated to the Fixed Satellite Service	)	IB Docket No. 05-20

COMMENTS OF
THE DEPARTMENT OF JUSTICE, INCLUDING THE FEDERAL BUREAU OF INVESTIGATION, AND THE DEPARTMENT OF HOMELAND SECURITY

The United States Department of Justice ("DOJ"), including the Federal Bureau of Investigation ("FBI"), and the Department of Homeland Security ("DHS")[2] (collectively, "the Departments") hereby submit their comments on the Commission's Notice of Proposed Rulemaking in the above-captioned docket (hereinafter "*Notice*").[3]

In the *Notice*, the Commission proposes a regulatory framework for the licensing and operation of aeronautical mobile satellite service ("AMSS") systems to communicate with fixed-satellite service networks in the conventional Ku band

---

[2] The Department of Homeland Security, includes, *inter alia,* the following agencies with equities in this proposed rulemaking: the Bureau of Immigration and Customs Enforcement ("ICE"), including the Federal Air Marshals Service ("FAMS"), the Transportation Security Administration ("TSA"), the Bureau of Customs and Border Protection ("CBP"), the United States Secret Service ("USSS"), and the United States Coast Guard ("USCG").

[3] *In the Matter of Service Rules and Procedures to Govern the Use of Aeronautical Mobile Satellite Earth Stations in Frequency Bands Allocated to the Fixed Satellite Service*, Notice of Proposed Rulemaking, IB Docket No. 05-20, FCC 05-14 (rel. Feb. 9, 2005).

frequencies (11.7 – 12.2 GHz and 14.0 – 14.5 GHz).[4] Aircraft earth stations ("AES") in the AMSS located onboard aircraft would be used to provide broadband communications services (e.g., integrated access to e-mail, voice, high-speed data, video-on-demand, and interactive delivery services) on commercial and other aircraft while in-flight.[5]

The Departments support the Commission's efforts in this and related Commission proceedings to promote the efficient use of spectrum and to enable important new communications services to be provided to passengers, aircraft crew, and law enforcement officers onboard aircraft. However, the Departments believe that the Commission's proposals raise important public safety and national security issues. Thus, the Departments take this opportunity to identify for the Commission their public safety and national security-related concerns.

In the wake of the events of September 11, 2001, both the Nation as a whole and those who are tasked with ensuring its safety have increased their focus on homeland security. The Departments each play a critical part in ensuring the overall security of our Nation and its citizens. The Commission also plays an important part in preserving and promoting homeland security. In fact, homeland security is included

---

4 *Notice* ¶ 1.

5 *Id.* at ¶¶ 1-2.

among the goals listed in the Commission's current five-year strategic plan.[6] Consistent with the Communications Act and the Commission's strategic goal of preserving and promoting homeland security, the Commission's inquiry into the appropriate regulatory and licensing framework for the use of two-way satellite-based broadband communications and data capabilities, devices, and services onboard aircraft must consider public safety/national security as well as commercial equities by expressly including an analysis of the potential adverse impact that the Commission's proposal and resulting actions could have on public safety and national security and consideration of all reasonable remedial measures which may be taken to eliminate or minimize that impact.

The Departments believe that the timely roll-out of new commercial airborne communications capabilities can be accomplished in a responsible manner, without unnecessary delay, which both encourages and rewards private sector investment and

---

[6] *See Federal Communications Commission Strategic Plan FY 2003 – FY 2008* at 5, 7, 18-20, 23 ("FY 2003 – FY 2005 Strategic Plan"). As former Chairman Powell's statement in the FY 2003 – FY 2005 Strategic Plan makes clear, "[w]ith the events of September 11 it has become imperative that the communications community come together to determine [its] role in ensuring homeland security . . . [w]e must be aggressive in ensuring that our policies maximize the many efforts being made to make our Nation safe." *See* FY 2003 – FY 2005 Strategic Plan at Back Cover.

Even if homeland security goals were not expressly stated in the Commission's strategic plan, the Communications Act of 1934, as amended ("Communications Act"), mandates homeland security as a Commission obligation in its statement that the Commission was created for the purpose of ". . . the national defense . . . [and] promoting the safety of life and property . . ." *See* 47 U.S.C. § 151.

expedited development while addressing the Departments' public safety and national security concerns. The Departments support such an approach, which will benefit not just the flying public but will lend significant support to the vital mission of law enforcement onboard "at risk" flights and, in that respect, can be viewed as a critical factor in enhancing the safety of those flights. Indeed, the combined ability of (1) law enforcement and other United States government entities to communicate in an effective manner with the federal law enforcement officers, flight crew, hijackers or terrorists onboard the aircraft and monitor and exercise control over onboard communications, and (2) Federal law enforcement officers to utilize broadband capability in-flight to communicate among themselves onboard the aircraft, with the flight deck and cabin crew, and with law enforcement and military personnel on the ground and in the air in the event of an incident onboard the aircraft, will promote the safety and confidence of the flying public and enhance public safety and national security.

I. CALEA IN AN AIR-TO-GROUND COMMUNICATIONS CONTEXT

Lawfully-authorized electronic surveillance is an invaluable and necessary tool for federal, state, and local law enforcement in their fight against terrorists and other

criminals.[7] In 1994, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA").[8] CALEA's purpose is to maintain law enforcement's ability to conduct court-ordered electronic surveillance despite changing telecommunications technologies by (1) further defining the telecommunications industry's obligation to provision electronic surveillance capabilities when served with a court order or other legal process, and (2) requiring industry to develop and deploy CALEA intercept solutions in their networks. CALEA is a technology-neutral statute[9] that applies to all "telecommunications carriers" — including those using platforms such as wireline, wireless, cable, satellite, and electric or other utility.[10]

In the *Notice*, the Commission proposes a regulatory and licensing framework for the use of two-way satellite-based broadband communications and data capabilities, devices, and services onboard aircraft. The Commission is currently examining in a separate, CALEA-specific proceeding the applicability of CALEA to broadband internet

---

[7] "Electronic surveillance" as used herein refers to the interception of call content and/or call-identifying information pursuant to lawful process, such as wiretap, pen register, and trap and trace orders.

[8] Pub. L. No. 103-414, 108 Stat. 4279 (1994); 47 U.S.C. § 1001 *et seq*.

[9] "CALEA, like the Communications Act, is technology neutral. Thus, a carrier's choice of technology when offering common carrier services does not change its obligations under CALEA." *In The Matter of Communications Assistance for Law Enforcement Act*, Second Report and Order, 15 FCC Rcd 7105, 7120 n. 69 (1999) ("*CALEA Second Report and Order*").

[10] *See* CALEA Legislative History, H.R. Rep. No. 103-827(I), reprinted in 1994 U.S.C.C.A.N. 3489, 3500 ("CALEA Legislative History").

access services, including those delivered by satellite systems.[11] The Commission tentatively concluded in the *CALEA NPRM* that providers of facilities-based broadband internet access services and managed voice-over-Internet protocol ("VoIP") services are subject to CALEA.[12] As the Commission has acknowledged in the *Notice*, AMSS operators will likely be subject to any rules the Commission adopts in that proceeding regarding CALEA obligations of satellite-based providers of broadband internet access.[13] To the extent the Commission ultimately concludes in its separate CALEA rulemaking proceeding that providers of satellite-based broadband internet access service are subject to CALEA, the Departments urge the Commission to confirm in any statement or decision issued in this proceeding that the satellite-based service providers/carriers are subject to CALEA with respect to broadband air-to-ground communications carried on their networks.[14]

---

[11] *See Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling, 19 FCC Rcd 15676 (2004) ("*CALEA NPRM*").

[12] *See CALEA NPRM* at 15676 ¶ 2, 15693-4 ¶ 37. The Commission noted in its tentative conclusion that broadband internet access providers include, but are not limited to, wireline, cable modem, satellite, wireless, and broadband access via powerline companies. *Id.* at 15694 ¶ 37.

[13] *See Notice* n. 7.

[14] The Departments note the Commission's acknowledgement in the *CALEA NPRM* that if the Commission ultimately decides that broadband internet access providers are subject to CALEA, entities that had previously not been subject to CALEA will have to comply with its requirements and will need a reasonable amount of time within which to do so. *See CALEA NPRM* at 15742-3 ¶¶ 140-141, 143. The Departments would

Beyond the issue of applicability, because of the unique context of communications capability onboard aircraft, the issue of how CALEA should function in the context of air-to-ground communications must be carefully examined by the Commission.

CALEA requires that a telecommunications carrier ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept all wire and electronic communication (i.e., call/communication content), and to access call-identifying/communication-identifying information that is reasonably available to the carrier.[15] CALEA itself does not prescribe a timeframe within which an intercept order must be provisioned; however, the Commission has previously stated that carriers should promptly provision such orders and comply with any other relevant

---

assume that any CALEA compliance transition period adopted by the Commission for broadband internet access providers would apply in both a terrestrial and air-to-ground context.

[15] *See* 47 U.S.C. §§ 1002(a)(1), 1002(a)(2). It should be noted that national security operations in an air-to-ground communications context will require that the unobtrusive interception of the target's (e.g., terrorist's or hijacker's) communications begin immediately upon provisioning (e.g. surveillance activation) and that collection of content not be delayed until the next target communication setup. This will require interception to be activated "mid communication," without having initial communication set-up information.

statutes related to carriers' duty to assist law enforcement in performing interceptions.[16] The absence of a specific timing requirement and a lack of clear guidance as to what constitutes "promptly" provisioning an intercept order has led to debate and some degree of uncertainty in traditional terrestrial interception circumstances. There is no room for such uncertainty in the air-to-ground context where delays of minutes and seconds could make the difference between life and death for passengers and crew aloft and those on the ground below. Given the nature of both air travel and air-to-ground communications, any historical, terrestrially-based interpretation of the term "promptly" is, in the Departments' view, not adequate in this context. There is a short window of opportunity in which action can be taken to thwart a suicidal terrorist hijacking or remedy other crisis situations onboard an aircraft, and law enforcement needs to maximize its ability to respond to these potentially lethal situations.[17] Thus, defining or interpreting "promptly" in a way that is meaningful relative to this unique

---

[16] *See In the Matter of Communications Assistance for Law Enforcement Act*, Report and Order, 14 FCC Rcd 4151, 4163 ¶ 26 (1999).

[17] Indeed, with respect to three of the flights that were hijacked by terrorists on September 11, 2001, the amount of time that elapsed between the determination that each aircraft had been hijacked and when each plane crashed ranged from 12 to 27 minutes. *See The 9/11 Commission Report* (released July 22, 2004) at 5-10 (the FAA's Boston Air Traffic Control Center learned of the hijacking of American Airlines Flight 11 just before 8:25 a.m. and the flight crashed into the North Tower of the World Trade Center at 8:46 a.m. (21 minutes); awareness that United Flight 175 had been hijacked occurred at approximately 8:51 a.m. and the flight crashed into the South Tower of the World Trade Center at 9:03 a.m. (12 minutes); suspicion that American Airline Flight 77 had been hijacked occurred at 9:00 a.m., the hijacking of Flight 77 was definitely known just before 9:10 a.m., and the flight crashed into the Pentagon at 9:37 a.m. (27 minutes)).

context is critical. Accordingly, the Departments request that the Commission specify that, in the context of an air-to-ground intercept, the CALEA term "promptly" be defined as "forthwith, but in no circumstance more than 10 minutes" from the moment of notification to the telecommunications carrier of lawful authority to intercept or otherwise conduct lawful electronic surveillance to the moment of real-time transmission to law enforcement or other authorized government agents.[18]

The Departments also request that the Commission require, by a date certain, that any satellite-based communications capability to or from an aircraft operating in United States airspace or international airspace contiguous or attendant to the United States exclusively utilize ground stations located within the United States' borders only and not ground stations located along the border in neighboring countries.[19]

---

[18] Having the ability to immediately provision an intercept is most critical in the air-to-ground context, where every moment matters. As history has shown, crisis situations typically strike without advance warning and there is often little or no lead or "ramp up" time. For this reason, a carrier's system must be in "pre-ready" condition so that carriers are in a position to react in an immediate and effective manner in such situations.

[19] The Departments believe that the requirement that satellite-based broadband service providers and carriers (who do not themselves offer air-to-ground VoIP services) exclusively use, by a date certain, ground stations located in the United States for the transmission of the subject communications should not serve as a basis for delay in the timely roll-out of satellite-based, airborne broadband service so long as there is provisioned in the interim a lawful, reliable means of intercepting and accessing such broadband communications at a location within the United States.

II. NON-CALEA OPERATIONAL CAPABILITIES

As noted above, the uniqueness of service to and from an aircraft in flight presents the possibility that terrorists and other criminals could use air-to-ground communications systems to coordinate an attack (e.g., a hijacking). For example, the use of satellite-based communications and data services onboard aircraft could potentially facilitate a coordinated attack between (1) a person on the aircraft and a person on the ground, (2) persons traveling on different aircraft, and/or (3) persons traveling on the same aircraft located in different sections of the cabin, who could communicate with one another using these services.[20] In the event that such a coordinated attack is carried out, the inability of law enforcement or United States government entities to communicate with the aircraft (whether it be federal law enforcement officers who may be on the flight, the crew, or a hijacker or terrorist) in any

[20] As documented in the 9/11 Commission Report, the hijackers/terrorists involved in the September 11, 2001 attacks utilized existing telecommunications options from within the terminals at Boston's Logan Airport to communicate and coordinate the planned attacks. *See The 9/11 Commission Report* at 1, 451 n. 3 (noting that while checking in for American Airlines Flight 11, hijacker Mohammed Atta reportedly received a call on his cell phone from fellow hijacker Marwan al Shehhi, which was placed by Shehhi from a payphone located in Terminal C of Logan Airport between the screening checkpoint and the boarding gate for United Airlines Flight 175). Although the communications were effectuated on the ground using existing communications facilities, it is not difficult to conclude what additional/further coordination could have occurred if other options – such as in-flight broadband communications and data capabilities – had been available.

effective manner,[21] means that capabilities in addition to those required by CALEA will be necessary.[22]

For example, once a determination has been made that an airborne aircraft represents a threat to public safety and/or national security, the identification of both the destination of all communications originated from broadband-enabled communications devices on such an aircraft and the origin of communications directed or terminated to broadband-enabled communications devices located on that aircraft becomes critically important for law enforcement and can influence time-sensitive decisions about how to respond to the threat. Accordingly, this truly unique operational situation compels the Departments to request that the Commission require that all satellite-based service providers and carriers (1) create and maintain the capability to record (and do record) at some central, land-based storage facility located within the United States, at a minimum, non-content communication records relating to all communications processed to and from broadband-enabled communications devices onboard aircraft operating within United States air space, international air space contiguous or attendant to United States air space, and international air space used

---

[21] Unlike traditional terrestrial interception scenarios in which time may similarly be of the essence, in the air-to-ground context, law enforcement cannot typically avail itself of the operational option of physically surrounding and penetrating an aircraft while in flight.

[22] The Departments emphasize that they consider these additional capabilities to be separate and distinct from, and not required by, CALEA.

enroute to or from United States air space or destinations, and (2) provide law enforcement with immediate access to such records upon lawful request.[23]

Other operational capabilities that the Departments request include that the satellite-based service provider or carrier be able, by a date certain, to:

(1) Expeditiously identify the verified location/seat number (if available) or relative location (i.e. forward or aft) of the user of a given broadband-enabled communications device on a given aircraft which has a communication in progress;[24]

(2) Expeditiously identify all broadband-enabled communications device users on a given aircraft who have communications in progress to or with a

---

[23] Upon acquisition of any necessary lawful process (e.g. court order, search warrant, etc.) records of air-to-ground communications subject to the requirement of immediate law enforcement access should include, at a minimum, all communications processed during each domestic U.S. flight and each U.S. inbound and outbound international flight. These records of the air-to-ground satellite-based service provider or carrier need only be maintained for a 24-hour period following the termination of the flight in order to afford law enforcement a reasonable opportunity to secure lawful process to compel disclosure of the records before their destruction by the provider or carrier. The Departments note that satellite-based service providers and carriers that operate on a common carrier basis are already required to maintain toll records for a period of at least 18 months under the Commission's existing rules, *see* 47 C.F.R. § 42.6, but the additional requirement sought for these providers and carriers would include non-toll communication records as well.

[24] Location information is invaluable to quickly establishing the identity of terrorists/hijackers aboard an aircraft. As confirmed in *The 9/11 Commission Report*, the information relayed by the flight attendants on American Airlines Flight 11 to authorities on the ground about the hijackers (including their seat assignments) and the events taking place onboard the aircraft was critical to enabling authorities to establish the hijackers' identities. *See The 9/11 Commission Report* at 5.

broadband-enabled communications device user onboard another aircraft that are serviced by the same or an associated provider;

(3) Expeditiously interrupt a communication in progress on a given aircraft;

(4) Expeditiously conference law enforcement with or to a communication in progress on a given aircraft;

(5) Expeditiously redirect all communications destined to or originating from a given aircraft;

(6) Expeditiously terminate the ability of all broadband-enabled communications device users on a given aircraft to send or receive communications without impairing the ability of authorized personnel to communicate;

(7) Provide the ability to transmit emergency law enforcement/public safety information to airborne and terrestrial resources, as appropriate; and

(8) Provide a dedicated service or reserve bandwidth (which can be accomplished through preemption protocols) to support the transmission and reception of emergency communications information to and from aircraft security elements, independent of passenger use;

(9) Assure the technology used is compatible with Wireless Priority Service to enable National Security/Emergency Preparedness (NS/EP) users connectivity in emergency situations.

III. POSSIBLE INCREASED RISK OF THE USE OF RADIO-CONTROLLED IMPROVISED EXPLOSIVE DEVICES AS A RESULT OF CONNECTIVITY TO AND FROM AIRCRAFT

The Commission's proposal would allow for connectivity from aircraft to the ground and vice versa. Although the potential for terrorists and other criminals to use communications devices as remote-controlled improvised explosive devices ("RCIEDs") already exists, the risk of RCIED use may, at least in theory, be increased as a result of the ability of aircraft passengers to now effectively use broadband-enabled and similar communications devices in-flight.[25] The ability to turn on a broadband-enabled communications device located onboard an aircraft and have that device gain access (i.e. connect) to broadband service or reach a communications carrier's network — which was not previously possible in a reliable way — presents the possibility that either a passenger or someone on the ground could *reliably* remotely activate a broadband-enabled communications device in-flight and use that device as an RCIED.

[25] The Departments acknowledge that the risk to aircraft posed by RCIEDs exists separate and apart from the existence of communications connectivity to aircraft. Mitigation of the RCIED threat occurs substantially, in the first instance, through advanced screening techniques that would prevent the device from coming onboard an aircraft. While it is acknowledged that, historically, far simpler RCIEDs (i.e., those not requiring remote connectivity) have been used to successfully attack aircraft, the Departments believe that the new possibilities generated by airborne passenger connectivity must be recognized. It is imperative that the Commission examine the full range of new possibilities and take affirmative steps to try to mitigate these possibilities.

The Commission should adopt mechanisms designed to mitigate this potential increased risk. The Departments, therefore, request that the Commission, at a minimum, require that:

(1) users be authenticated to the onboard network and register their location on the aircraft before being able to use their broadband-enabled communications device in-flight;[26]

(2) there be strong network security controls required of communications equipment onboard aircraft; and

(3) satellite-based service providers and carriers design onboard communications systems in such a way that they will deny network access and connectivity to any device that is stored in the cargo hull.[27]

---

[26] As discussed in note 19, *supra*, location information is invaluable to quickly establishing the identity of terrorists or hijackers onboard an aircraft. Although the Departments acknowledge the expertise of providers to best engineer these solutions, some providers have suggested that authentication security capabilities could be accomplished, for example, through positive response systems, such as a user login requirement, or via an interface between the satellite-based service provider or carrier and the airline to determine the passengers on the airline's manifest that are authorized to use broadband-enabled communications devices in-flight and their seat locations.

[27] Some providers have suggested to the Departments that this capability may be simply accomplished, for example, by the installation of a separate antenna array in the cargo hull. The Departments would look to the expertise of the Commission and the providers to devise these solutions.

IV. INTERFERENCE ISSUES

In-flight broadband-enabled communications device transmissions may cause interference with aircraft navigation and communications equipment that could affect air safety and security.[28] The Departments recognize that the Federal Aviation Administration ("FAA") prohibits the use of personal electronic devices on airplanes unless the operator of the aircraft has determined that the device will not cause interference with the navigation or communication system of the aircraft. The Departments support the Commission's assessment that the use of broadband-enabled communications devices will remain subject to the rules and policies of the FAA and aircraft operators and that any change in the Commission's rules will not affect the applicability of the FAA's rules.

V. POTENTIAL IMPACT OF IN-FLIGHT USE OF BROADBAND-ENABLED COMMUNICATIONS DEVICES ON PASSENGER CONDUCT

The Departments note that in recent months, there has been significant media attention given to both the Commission's pending proposals to allow passengers to use personal wireless phones and broadband-enabled communications devices in-flight and

---

[28] In addition to any radio frequency interference that might result from in-flight broadband-enabled communications device transmissions, passenger use of power supplies or circuitry onboard aircraft which are used to simultaneously transmit data or intelligence related to aircraft operations or communications may also represent an interference risk.

the concerns expressed by flight attendants and other members of the flying public about the effect that such use will have on the overall atmosphere of flights and the conduct of passengers. In particular, the Departments note the flying public's concerns that the unrestricted use of such devices by multiple passengers on flights could result in an increase in "air rage" incidents among passengers. The Departments believe that the conduct of passengers making use of broadband-enabled and other communications devices in-flight could have serious implications for Federal law enforcement onboard aircraft whose status is unknown to fellow passengers. Affirmative measures should be adopted to diminish the probability that law enforcement's on-board mission will either be complicated or compromised unnecessarily by disputes concerning the use of broadband-enabled and other communications devices in-flight. Accordingly, the Departments suggest that the Commission, in consultation with the airlines, should establish rules and/or policies concerning in-flight use of these devices and related conduct to minimize any increase in air rage incidents which could potentially result from the unrestricted use of such devices on flights.

CONCLUSION

For the reasons set forth above, the Commission should carefully examine public safety and national security-related concerns in considering the appropriate regulatory and licensing framework for the use of two-way satellite-based broadband communications and data capabilities, devices, and services onboard aircraft.

Respectfully submitted,

THE UNITED STATES DEPARTMENT OF JUSTICE

/s/ Laura H. Parsky

Laura H. Parsky
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Room 2113
Washington, D.C. 20530
(202) 616-3928

THE DEPARTMENT OF HOMELAND SECURITY

/s/ Elaine Dezenski

Elaine Dezenski
Acting Assistant Secretary for Policy and Planning
Border and Transportation Security Directorate
United States Department of Homeland Security
Nebraska Avenue Complex
Washington, D.C. 20528
(202) 282-8446

THE FEDERAL BUREAU OF INVESTIGATION

/s/ Patrick W. Kelley

Patrick W. Kelley
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.
Room 7427
Washington, D.C. 20535
(202) 324-8067

THE DEPARTMENT OF HOMELAND SECURITY

/s/ Tina Gabbrielli

Tina W. Gabbrielli
Director of Intelligence Coordination and Special Infrastructure Protection Programs
Office of the Assistant Secretary for Infrastructure Protection
United States Department of Homeland Security
Nebraska Avenue Complex
Washington, D.C. 20528
(202) 282-8582

Dated: July 5, 2005