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

In the Matter of	)	
	)	
Expanding Access to Mobile Wireless Services Onboard Aircraft	)	WT Docket No. 13-301
	)	

Reply Comments of the Safety and Security in the Air Coalition which includes the following organizations:

Association of Flight Attendants-CWA
Federal Law Enforcement Officers Association
Global Business Travel Association
International Association of Machinists and Aerospace Workers
and
Transport Workers Union of America

Christopher J. Witkowski
Association of Flight Attendants-CWA

Jon Adler
Federal Law Enforcement Officers Association

Michael W. McCormick
Global Business Travel Association

Sito Pantoja
International Association of Machinists and Aerospace Workers

Garry Drummond
Transport Workers Union of America

Alan Fishel
Arent Fox LLP
1717 K Street, NW
Washington, DC 20036
Tel: (202) 857-6000 / Fax: (202) 857-6395
E-mail: alan.fishel@arentfox.com
Counsel to Safety and Security in the Air Coalition

Dated: May 16, 2014

Table of Contents

Page

Table of Contents i

Executive Summary ii

Introduction 1

Discussion 2

A. Pre-Operational Surveillance by Terrorists and Crew Recognition of Suspicious Activity 7

B. The Terrorist Attack Phase and Tactical Communications 8

C. Improvised Explosive Devices and Aircraft Sabotage – The Cell Phone Will be the Means to Initiate a Detonation 14

D. Cyberwarfare 16

E. Encouraging More Terrorist Attempts 20

Conclusion 20

Executive Summary

The SSAC respectfully submits these reply comments to the Federal Communications Commission ("Commission") Notice of Proposed Rulemaking on mobile wireless services onboard aircraft. In these comments, the SSAC requests that the Commission terminate this proceeding. The SSAC is greatly concerned that unacceptable risks to U.S. national security will flow from a decision to provide passengers, including terrorists, airborne access to mobile broadband services. These concerns relate to the following five issues involving terrorist and counterterrorist actions enhanced by the ability to use cell phones in flight:

- Pre-operational surveillance by terrorists and crew recognition of these suspicious activities;
- Tactical communications to support terrorist attack planning and implementation;
- Use by terrorists of remotely-initiated explosive devices to commit aircraft sabotage;
- The threat of terrorists adopting cyberwarfare tactics; and
- The encouragement of more terrorist attempts.

Introduction

The following reply comments are submitted in response to the Commission's Notice of Proposed Rulemaking ("NPRM"), *Expanding Access to Mobile Wireless Services Onboard Aircraft*,[1] by the Safety and Security in the Air Coalition ("SSAC"). For the reasons detailed in these comments regarding the grave risks to the safety and security of the U.S. commercial aviation system that will result from allowing the in-flight use of mobile broadband services, the SSAC disagrees with the Commission that, on balance, "it is in the public interest to bring the benefits of mobile communications services on aircraft to domestic consumers,"[2] and therefore strongly recommends that the Commission terminate the subject NPRM and continue to maintain the long-standing U.S. ban on the use of cellular telephones onboard aircraft during flight.

The organizations comprising the SSAC include: the Association of Flight Attendants-CWA ("AFA"), the world's largest flight attendant union representing nearly 60,000 members working for 19 U.S. airlines; the Federal Law Enforcement Officers Association ("FLEOA"), the largest professional association representing federal law enforcement officers, with more than 25,000 members from over 65 different federal agencies; the Global Business Travel Association ("GBTA"), which connects the business travel world and promotes the value of business travel management; the International Association of Machinists and Aerospace Workers ("IAM"), one of the largest industrial trade unions in North America, representing more than 180,000 airline and aircraft manufacturing workers; and the Transport Workers Union of America ("TWU"), which represents 200,000 workers and retirees, primarily in commercial aviation, public transportation and passenger railroads.

---

[1] Expanding Access to Mobile Wireless Services Onboard Aircraft, 79 Fed. Reg. 2615 (Fed. Commc'n Comm'n Jan. 15, 2014).
[2] *Id.* at 2616.

The SSAC members are fully invested in the safety and security of our nation's commercial aviation infrastructure. The traveling public, including the business travelers represented by GBTA, count on the safe, secure travel significantly enhanced by the closely coordinated efforts of the hundreds of thousands of workers represented by AFA, FLEOA, IAM and TWU. All of these workers—flight attendants, pilots, mechanics, customer service agents, baggage handlers, federal law enforcement officers, and many others—have countless critical safety and security responsibilities to perform before, during and after every single flight.

Discussion

The Commission is considering removing the long-standing U.S. ban on the use of cellular telephones onboard aircraft during flight because the Commission apparently believes the reasoning from its initial orders effectively imposing the ban is no longer applicable "on an aircraft equipped with an Airborne Access System." [3] The question the Commission should decide, however, is not whether the specific reasoning in those prior orders is correct today—but whether the final result in those orders is still correct. And the answer to that is unequivocally "yes."

In fact, because of the long-standing U.S. ban put in effect by the Commission's prior orders, there has been no need for other federal agencies to analyze the safety and security risks to the U.S. commercial air transport system that the lifting of the ban would greatly exacerbate. In light of the information set forth herein, it is incumbent upon the Commission, coordinating extremely closely with all other relevant agencies, to forbear from lifting the ban. To even consider removing the ban, it must be clear that such a change in course would not increase safety and security risks. And that is a burden that none of the proponents of this NPRM can even come close to satisfying. For the reasons detailed in these comments regarding the grave

[3] *Id.*

risks to the safety and security of the this nation's commercial aviation system that will result from allowing the in-flight use of mobile broadband services, the Commission should terminate the subject NPRM and continue to maintain the ban on the airborne use of mobile wireless services during commercial flights.

Following the terrorist attacks of September 11, 2001 (9/11), it became obvious that the commercial aviation security industry along with our nation's intelligence and law enforcement communities were not fully prepared to prevent such attacks. The *Congressional National Commission on Terrorist Attacks Upon the United States* stated in its final report, "We believe the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management." [4] As a result, many of us working in these industries collaborated in an unprecedented effort to put into place laws, strategies, policies, tactics, techniques, and procedures to protect against any additional attacks. These efforts led to the creation and development of the Transportation Security Administration ("TSA") and eventually to the Department of Homeland Security ("DHS").

Given all of the hard work that was expended after 9/11 to strengthen our nation's security infrastructure, taking any steps that would undermine current levels of safety and security is more than just ill-advised – given the stakes involved, it is entirely unacceptable. The Commission must not take any action that would enhance the capability of terrorists to once again attack the commercial aviation system and inflict harm on our nation, our citizens, and our economy. And yet that is exactly what the Commission will be doing here if the ban is lifted. In fact, without question, the deadly results that may very well flow from that decision would be

[4] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, at 339 (2004) , *available at* http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf.

completely foreseeable. This is certainly not the time, and the United States is certainly not the place, to make decisions that will make it easier for terrorists to successfully attack our nation's commercial aviation system.

In addition, if such attacks were to occur as a result of a reversal of course by the Commission here, not only would numerous (and potentially at least many thousands of) lives be unnecessarily lost and families destroyed forever, but the economy would also be seriously harmed. Moreover, it would be a gross understatement to state that such a decision by the Commission would not be one that can be rescinded later in a manner that would undo the tremendous adverse consequences. For all of the reasons discussed in these comments, the SSAC believes it is crystal clear that removal of the ban would greatly exacerbate the likelihood of terrorist attacks in the air in the United States. But even if after reviewing this filing the Commission still somehow has any doubts regarding this matter, it should err on the side of caution, not recklessness.

In fact, a recent precedent exists for taking just such a prudent approach. In early 2011, the Federal Aviation Administration ("FAA") decided to disable all chemical oxygen generators in the lavatories of U.S. commercial aircraft. At the time, perhaps out of an abundance of caution, the FAA justified the action as "prompted by reports that the current design of chemical oxygen generators in the lavatories presents a hazard that could jeopardize flight safety."[5] By February 2012, the FAA was publicly characterizing this "flight safety" concern as a security issue: "The FAA chartered an Aviation Rulemaking Committee … to recommend regulatory

[5] Airworthiness Directives; Various Transport Category Airplanes Equipped With Chemical Oxygen Generators Installed in a Lavatory, 76 Fed. Reg. 12556 (Fed. Aviation Admin. Mar. 8, 2011).

changes and guidance that could be used to restore oxygen in affected lavatories while addressing the security vulnerability."[6]

Without wading into a sensitive discussion of exactly what this "security vulnerability" is, it is important to acknowledge the precedent: the FAA recognized the vulnerability and took significant and immediate steps to remove it. We mention this precedent because it further counters one possible argument for moving forward with airborne mobile broadband services, which may be expressed as follows: "Given that some international airlines have been allowing cell phone services for several years, why should we be concerned in the United States if we remove the ban?" We, like the FAA with the lavatory chemical oxygen generator issue, are concerned about the potential for terrorists to exploit a vulnerability to attack the citizens, infrastructure, and economy of the United States. Like it or not, the United States is the highest priority target for international terrorist organizations (not to mention some nation states that support terrorist organizations as proxies.)

In fact, according to a March 2011 *Wall Street Journal* report,[7] the European Aviation Safety Agency ("EASA") cited a lack of authority in not agreeing to follow the FAA's lead and require the removal of chemical oxygen generators from the lavatories of commercial airplanes. This claim was subtly questioned in the *Journal* article, which stated that "EASA didn't elaborate on what authority it lacks."

It may be that EASA does not perceive the terrorist threat to their commercial aviation system is significant enough to justify the cost and effort. Similarly, the apparent absence of terrorist acts on international airlines that recently began to allow passenger use of airborne

---

[6] Security Considerations for Lavatory Oxygen Systems, 77 Fed. Reg. 11385, 11386 (Fed. Aviation Admin. Feb. 27, 2012).

[7] Andy Pasztor, *Europe Airline Regulators Don't Adopt U.S. Antiterrorist Rules on Oxygen Equipment*, WALL STREET JOURNAL, Mar.16, 2011.

mobile broadband services is not indicative of the potential threat posed to the United States. In fact, it may very well be that the terrorists are waiting for the United States to build such infrastructure to the point that it is mature and ubiquitous, and thus easily leveraged to enhance the probability of successful attacks, including multiple aircraft attacks. Clearly, given the years that separated the World Trade Center bombing in 1993[8] and the 9/11 attacks, terrorists are content to plan slowly, carefully, and methodically. From another perspective, a small-scale, successful attack now, while devastating in terms of lives lost, may be seen as counterproductive to the terrorist mastermind, as it could effectively terminate work on implementing this infrastructure, possibly for as long as decades.

In the following sections, we describe many of the unacceptable risks to U.S. national security that will flow from a decision to permit passengers access to airborne mobile broadband services on commercial transport airplanes. These sections include the following: a discussion of several of the specific security threats that will be greatly exacerbated, with information provided regarding pre-operational surveillance by terrorists and crew recognition of these suspicious activities; the critical importance of tactical communications to support terrorist attack planning and implementation; use by terrorists of explosive devices to commit aircraft sabotage through use of the cell phone to initiate the detonation; and the serious threat posed by terrorists adopting cyberwarfare tactics.

---

[8] *1993 World Trade Center bombing*, WIKIPEDIA, http://en.wikipedia.org/wiki/1993_World_Trade_Center_bombing (last visited May 16, 2014).

A. Pre-Operational Surveillance by Terrorists and Crew Recognition of Suspicious Activity

In November 2001, Congress passed the Aviation and Transportation Security Act[9] that required, among other things, that all aviation crewmembers be able to "recognize suspicious behavior" and respond according to a specific set of mandated guidelines. Several of the SSAC members helped craft these guidelines. Lifting the ban on cell phone usage on airplanes will make it impossible for crewmembers to effectively implement these mandated guidelines, which are considered sensitive security information.

Without exposing any of this sensitive information, it is important to understand some of the behaviors displayed by terrorists. It is known by intelligence, law enforcement, and counterterrorism experts that terrorist groups typically follow a process commonly known as the "Terrorist Attack Cycle" before, during and after an actual attack. It is no different for those terrorists that desire to either hijack or sabotage a commercial aircraft for purposes such as mass murder. Much of this suspicious behavior includes tactics used by terrorists conducting pre-operational surveillance during so-called "Targeting and Deployment Phases." Specifically, terrorists are attempting to gather information regarding the aircraft and its operations so as to expose vulnerabilities for their planned attack. Cell phones, along with their common ability to take photos and gather video intelligence, allow this to become a fairly simple task. Fortunately, the United States law that prevents onboard cell phone use during flight has not only made this more difficult for terrorists, it also creates an environment where this behavior is more easily seen, recognized and acted upon by flight attendants, the Federal Air Marshal Service ("FAMS") other law enforcement personnel, and even alert and aware passengers. Creating an environment

[9] Aviation and Transportation Security Act, Pub. L. No. 107-71 (codified as scattered sections of 49 U.S.C.).

where everybody and anybody can use their cell phones throughout a flight will allow this important and illicit terrorist behavior to increase in relative anonymity.

For clarity's sake, the SSAC understands that some carriers allow the use of cell phones and other portable electronic devices during flight as long as they are in "airplane mode." Therefore, passengers are allowed to have their cell phones out to access data already stored on their phones. This is current normal behavior. However, should individuals use their cell phones for voice communications or picture or video capture while in flight, this behavior would be considered suspicious today and is likely to be noticed by flight attendants. As trained, flight attendants would use their authority to address this issue and if necessary report it to the captain of the aircraft and the appropriate law enforcement authorities. This is an important security measure that allows for the recognition and disruption of a variety of criminal and terrorist behaviors. If the Commission enables the open use of cell phones during flight for voice and/or data transmissions, current behavioral norms will change, severely weakening and possibly even eliminating this important security tool.

B. The Terrorist Attack Phase and Tactical Communications

For numerous reasons, allowing terrorists to use cell phones for voice and data communications on flights would greatly exacerbate the likelihood of successful attacks on our airlines. Enabling the in-flight use of cell phones will give terrorists reliable command, control and communications capabilities that do not exist today. These capabilities will factor into terrorist attack planning and preparations and real-time tactical communications because they will:

1. Provide Terrorists Access to Reliable Communications with Expert Accomplices at the Moment the Terrorist Act Is Intended to Occur

At the moment a terrorist on an airplane is seeking to initiate an act of terrorism, if anything is not going according to plan, the terrorist would greatly benefit by being able to communicate with expert accomplices not onboard the airplane that can provide him or her with the exact advice or information needed to ensure the attack is successful. This communication can make the difference between success for the terrorist (and doom for the passengers and potentially others on the ground) and a failed attempt. Removing the ban on airborne mobile wireless services would ensure that terrorists can have such reliable communications with their expert accomplices at the most critical moments for them.

2. Provide Terrorists Access to Reliable Communications with Expert Accomplices While In Flight Prior to the Attack to Obtain Needed Information from Such Accomplices

Once the airplane is in flight, the terrorist may learn information that may make it more difficult for him or her to accomplish the terrorist act. This information could involve air marshals, flight attendants, other passengers, or virtually anything else. At that point in time, prior to the initiation of the attack but after the plane is in flight, it would be extremely helpful to the terrorist if he or she could communicate with expert accomplices on the ground to best determine how to overcome such potential obstacles. Removing the ban would ensure that terrorists can have such reliable communications with their expert accomplices at such times and overcome the hurdles presented by those seeking to protect themselves and the public.

In a similar vein, a terrorist may have forgotten an important step in the plan, or how to perform a certain aspect of an important step in the plan, once the flight has taken

off, and would need to gain information from expert accomplices on the ground to ensure that he or she can take all necessary steps to complete the terrorist act. Once again, removing the long-standing ban will guarantee that such communications can be reliably effectuated.

3. Provide a Terrorist Access to Reliable Communications with Expert Accomplices While In Flight to Provide Any Necessary Reassurance to the Terrorist

The terrorists can be planning the attack for months, but when the day finally arrives and the flight is in the air, it is entirely possible for the terrorist to get nervous and consider backing out. However, if the terrorist can access reliable communications with the masterminds on the ground who can assure the terrorist he or she should move forward with the attack, that can be the difference between the attack moving forward successfully or not.

4. Allow Terrorists to Plan an Attack Secure in the Knowledge that They Will Have Access to Reliable Communications with Co-conspirators up to and Including the Point of Attack

The availability of a known, reliable communications infrastructure to support attack coordination will obviously factor into terrorists' decisions to select targets, and will inform their planning and preparation activities. In fact, many terrorists will undoubtedly be very excited about the potential to combine their existing operational tactics with a robust wireless cell phone conduit onboard commercial aircraft.

5. Allow Terrorists to Coordinate Operations Between Multiple Attackers on Different Airplanes and Coordinators on the Ground

Even though the attacks of 9/11 involved multiple aircraft, these operations were not coordinated while in flight. Access to mobile broadband communications will make it easier for

operatives on multiple flights to communicate not only with each other, but with the masterminds behind the plot to ensure the maximum chaos.

As the above illustrates, as important as pre-operational surveillance is for those choosing a target and planning the attack (which is discussed in Section A), tactical communications discussed immediately above are even more important for operational success. Allowing the use of cell phones for voice and data transmissions during flight will dramatically increase terrorists' capability for tactical communications during their attack phase.

Since the successful attacks of 9/11, there have been other attempted attacks on commercial aircraft. Fortunately, most of these attacks have been unsuccessful, and thus it may appear that we have established a security system that is difficult to penetrate. While improvements have been made, it must be noted that none of these attacks took on a level of sophistication needed for multiple attackers onboard numerous aircraft to attack multiple targets both in the air and on the ground. This is not without good reason. The hard work of the professionals across the intelligence, law enforcement and aviation security industries are to be commended. Nevertheless, there have been several near misses along with a few successful attacks on aircraft and other targets that must be understood in order to correctly understand this ever evolving threat.

On December 22, 2001 Richard Reid, the infamous Shoe Bomber, boarded American Airlines Flight 63 from Paris, France to Miami, Florida and unsuccessfully attempted to detonate explosives packed into the shoes he was wearing. Reid had not acted alone but had received

training and support from an Al-Qaeda terrorist camp in Afghanistan and an Islamic school in Pakistan.[10]

A similar case occurred on Christmas Day in 2009, when Umar Farouk Abdulmutallab, also known as the "Underwear Bomber", boarded Northwest Airlines Flight 253 en route from Amsterdam to Detroit, Michigan.[11] He had plastic explosives hidden in his underwear and, like Richard Reid, he unsuccessfully attempted to detonate them while the plane was in flight. Also, like Reid, Abdulmutallab did not work alone but was rather trained and supported by a Yemen-based terrorist organization known as Al-Qaeda in the Arabian Peninsula ("AQAP"). This organization is currently considered by the U.S. government to be the most dangerous of all Al-Qaeda affiliates.

Neither of these men were the master planners behind these attacks nor the designers of the bombs meant to carry out their suicide missions. Ground support enabled by reliable cellular voice or data communications could have provided both Reid and Abdulmutallab sufficient real-time encouragement and information. In fact, either or both of these terrorist actions could have worked, resulting in scores of people killed and immense damage to the commercial aviation system and our economy. Had either of these men had the opportunity to tactically communicate directly with bomb experts on the ground, would they have overcome their procedural mistakes in detonating their improvised explosive devices? Would the planning and operational approaches have changed had they and their handlers known ahead of time that they could have direct voice or data communications once they were on the plane and in the air? We will probably never know the answers to these questions in these two particular cases, but it takes

---

[10] Nick Paton Walsh, Kamal Ahmed & Paul Harris, *MI5 blunders over bomber*, THE OBSERVER (Dec. 29, 2001, 09:21 PM EST), http://www.theguardian.com/world/2001/dec/30/terrorism.september11.

[11] *'Underwear bomber' Abdulmutallab pleads guilty*; BBC NEWS (Oct.12, 2011), http://www.bbc.co.uk/news/mobile/world-us-canada-15278483.

little knowledge of counterterrorism measures to recognize a scenario where the answer is unequivocally "yes." The introduction of picocells as a relay through satellites or cell towers will change the equation by giving terrorists a clear and trusted line for tactical communications. Commercial aviation, already prized by terrorists for its overwhelming significance to the infrastructure and economy of the developed world, and its symbolic and psychological media value when attacked, would become an even more attractive and vulnerable target.

The Reid and Abdulmutallab attacks are examples of individual terrorists attempting to bring down single airplanes. Neither of these attacks took on the level of sophistication that would be needed to coordinate multiple attackers onboard numerous aircraft, attacking multiple targets both in the air and on the ground. For the commercial aviation industry, this is the ultimate nightmare scenario foreshadowed by a different recent attack, one not directly related to commercial aircraft but nevertheless critical in understanding the tactics that terrorists choose to employ.

On November 26-29, 2008, ten young but well-trained and heavily armed terrorists traveled from Pakistan and conducted a well-planned and orchestrated attack against numerous targets in the city of Mumbai, India.[12] Along with firearms, ammunition, hand grenades, and improvised explosive devices complete with timers, they each carried a Nokia cell phone with a headset, a GPS device for each group and a satellite phone to coordinate with handlers in Pakistan. With 164 killed and 308 wounded,[13] this attack is seen as one of the most successful

---

[12] Vappala Balachandran, *Dealing with Aftermath of Attacks: Lessons from Mumbai and elsewhere on what to do and what not to do*, Pluscarden Programme Conference on The Future of International Cooperation in Countering Violent Extremism at St Antony's College, Oxford University (Oct. 8-9, 2010), *available at* http://www.sant.ox.ac.uk/centres/Balachandranpaper.pdf.

[13] Press Release, Press Information Bureau, Ministry of Home Affairs, Government of India, HM Announces Measures to Enhance Security (Dec. 11, 2008), *available at* http://pib.nic.in/newsite/erelease.aspx?relid=45446.

and impactful terrorist attacks ever. Right up to the time that the last terrorist died he was on the phone, receiving orders and advice from the experienced and hardened handlers in Pakistan on how to prolong the event and cause as many casualties as possible, as well as direction on how to evade and counter the law enforcement and military personnel responsible for bringing this horrific attack to a close.[14]

There are many lessons to be learned from this attack. One of the most chilling is that like our own military and law enforcement agencies, the leaders of terrorist groups choose to exercise command and control when conducting operations. To do this, they realize that it is critical to have direct communications with their operatives during the attack phase and they plan their operations with this in mind.

C. Improvised Explosive Devices and Aircraft Sabotage – The Cell Phone Will be the Means to Initiate a Detonation

In addition to the grave concerns raised above relating to attacks on commercial airlines made far more probable by terrorists use of cell phones as communications tools while in flight, we are also well aware of terrorists' affinity toward acts of sabotage designed to destroy one or more aircraft while in flight through use of a cell phone that can remotely initiate a detonation. In those instances, the cell phone would act as a switch to set off an Improvised Explosive Device ("IED") secreted onto an airplane. Two of the more disturbing trends designed to overcome current security measures are the practice of secreting explosives inside live human body cavities and the use of cell phones as detonators.

From the October 10, 1933 mid-air bombing of an United Airlines Boeing 247 over Chesterton, Indiana, to Pan Am Flight 103 over Lockerbie, Scotland on December 21, 1988, to the October 29, 2010 cargo bombing attempts against both UPS and FedEx, there have been in

[14] TERROR IN MUMBAI (HBO Documentaries 2009), *available at* http://www.hbo.com/documentaries/terror-in-mumbai#/.

excess of 88 cases of commercial airline bombings, with at least 56 having led to an accumulation of thousands of deaths.[15] On August 24, 2004, two Chechen women with the help of conspirators purchased tickets at the last minute and boarded two separate flights leaving Moscow's Domodedova Airport.[16] Volga-AviaExpress Flight 1303 and Siberia Airlines Flight 1047 suffered near simultaneous onboard explosions and crashed leaving no survivors among the crew and passengers. According to sensitive sources, the subsequent investigation revealed that both women had entered the lavatories on each aircraft where their IEDs were detonated. It is speculated by many security experts that they may have smuggled explosives through security at the most modern airport in Russia by hiding the explosives in body cavities, possibly their vaginal and/or rectal orifices.

On August 27, 2009, AQAP conducted a suicide bomber attack on the Assistant Interior Minister of Saudi Arabia, Prince Muhammad bin Nayef, using a Body Cavity Bomb type IED that was secreted into the attacker's rectum.[17] Although the Prince survived the attack, it should be noted that the bomber possibly used a cell phone to remotely detonate the device once he was in position next to the target.[18] Body cavity devices similar to the 2009 AQAP bomb can be used to evade most common airport explosive sensor strategies; certainly, AQAP will continue to work on ways to sabotage commercial aircraft through the use of explosives and suicide bombers. If the long-standing ban discussed in this filing is removed, AQAP will be able to confidently utilize cell phones to detonate their well hidden body cavity bombs remotely,

---

[15] *Commercial Airline Bombing History*, AEROSPACEWEB.ORG, http://www.aerospaceweb.org/question/planes/q0283.shtml (lasted visited May 16, 2014).
[16] C. J. Chivers, *Russians Cite Porous Security in Terror Bombings of 2 Planes*, N. Y. TIMES (Sept.16, 2004), http://www.nytimes.com/2004/09/16/international/europe/16moscow.html.
[17] Matthew Harwood, *Saudi Suicide Bomber Hid IED in His Anal Cavity*, SECURITY MANAGEMENT (Sept. 9, 2009), http://www.securitymanagement.com/news/saudi-suicide-bomber-hid-ied-his-anal-cavity-006178.
[18] Frank Gardner; *Why al-Qaeda in Yemen scares the West*, BBC NEWS (Aug. 6, 2013), http://www.bbc.com/news/world-middle-east-23593126.

including even if their trained suicide bombers get cold feet and change their minds at the last minute. These are near-perfect guided missiles that can be used to attack the cockpit and other vulnerable targets on the aircraft. And if this happens, they may very well be capable of once again taking control of the aircraft and using it as a weapon of mass destruction against targets on the ground.

D. Cyberwarfare

The SSAC has grave concerns that the fast changing and improving dynamic of cell phone and wireless technologies will hand terrorists the capability to attack commercial aircraft using cyberwarfare, or "politically motivated hacking to conduct sabotage and espionage … a form of information warfare sometimes seen as analogous to conventional warfare."[19] This is a significant, emerging threat, and is one more reason why the Commission must have a complete and detailed understanding of security operational plans, training, and counter-terrorism exercises, as well as the concerns that we and other aviation security stakeholders share regarding the proposal to allow onboard cell phone usage.

A recent commentary, *Cyberwarfare Goes Wireless*,[20] prepared by Isaac R. Porche III, a senior researcher at the nonprofit, nonpartisan Rand Corporation, discusses these concerns. Mr. Porche notes that this past March, a U.S. surveillance drone was intercepted above the Ukrainian region of Crimea. The drone was reportedly flying at above 12,000 feet and was virtually invisible from the ground. Apparently, a Russian state-owned arms and technology group said

---

[19] *Cyberwarfare*, WIKIPEDIA, http://en.wikipedia.org/wiki/Cyberwarfare (last visited May 16, 2014).

[20] Isaac R. Porche III, *Cyberwarfare Goes Wireless*, RAND CORPORATION, http://www.rand.org/blog/2014/04/cyberwarfare-goes-wireless.html (last visited May 16, 2014).

that they used complex radio-electronic technology to separate the drone from its operators and that the drone fell "almost intact into the hands of self-defense forces." [21]

For purposes of these comments, we have extracted a few very pertinent points from Mr. Porche's analysis of this incident:

1. Among the most significant challenges now facing the U.S. military is the increasingly blurred boundary between wired and wireless technologies.
2. In the military and commercial worlds, "cyberoperations" long referred to attacking and defending networks and connected devices. Nefarious hacking is typically thought of as an intrusion into remote computers through wired channels. But cyberoperators have gone "wireless." Radio and other frequencies that span the electromagnetic spectrum are the new contested domain. Sometimes this contest involves keeping these wireless channels up and running. At other times, it involves seeking to shut them down through jamming.
3. The past decade has seen a proliferation of wireless technologies, such as those used to fly U.S. drones and those allegedly used to intercept one of them over Crimea. Stories of insurgents using smartphones to detonate improvised explosive devices have gone from the Hollywood script to the newspaper.

Although the reports out of Russia may be suspect, it is clear, based on the opinions of Mr. Porche and many cyberwarfare experts, that this is a very serious threat that cannot be ignored by the Commission when considering changing the current rules and regulations to allow the open use of cell phone and wireless technology while in flight.

Over the past several years, with growing concern, security experts have followed incidents around the world regarding the threat of cyberwarfare. One such significant attack is known as Stuxnet. In 2009, the Stuxnet computer virus was used to target and physically damage

[21] *Russia Says It Intercepted A US Drone Over Crimea*, AGENCE FRANCE PRESSE (Mar. 14, 2014), http://www.businessinsider.com/russia-intercepted-us-drone-over-crimea-2014-3.

984 centrifuges in the Iranian uranium enrichment facility in Natanz.[22] Without speculating on the source of this incredibly destructive cyberweapon, suffice it to say that it was most likely the design of a nation state or several nations working together to slow the nuclear ambitions of Iran.

Since the Iranian Stuxnet attack, many nation states around the world have stepped up their efforts at both designing cyber weapons and protecting their infrastructure from these types of attacks. For example, it is widely known that China possesses a very sophisticated cyberwarfare capability that has a very strong focus on U.S. critical infrastructure components. A February 18, 2013 New York Times article, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*,[23] is an informative open source article that provides a good degree of insight into the magnitude of this ever growing Cyberwarfare threat.

It is quite conceivable that terrorist groups could obtain and use digital weapons to attack commercial aircraft. This would not be the first time a nation state worked together with a terrorist group to bring down a civilian airliner. The sabotage of Pan Am Flight 103 over Lockerbie, Scotland was a terrorist attack initiated by the nation state of Libya.[24]

Clearly, cyberwarfare is an ever-growing and evolving security threat that must be evaluated thoroughly before a decision can be made about the true vulnerability of commercial aircraft. While it is possible that a commercial aircraft's operational systems can be physically separated from the new proposed cell phone systems, some cyberwarfare experts appear to

---

[22] William J. Broad, John Markoff & David E. Sanger; *Stuxnet Worm Used Against Iran Was Tested in Israel*, N. Y. TIMES (Jan.15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[23] David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N. Y. TIMES, (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

[24] *Pan Am Flight 103: Qaddafi ordered it bombed, says Libyan minister*, CHRISTIAN SCIENCE MONITOR (Feb. 23, 2011), http://www.csmonitor.com/World/Latest-News-Wires/2011/0223/Pan-Am-Flight-103-Qaddafi-ordered-it-bombed-says-Libyan-minister.

believe otherwise. These concerns are well-documented in a recently published Christian Science Monitor article: [25]

> [S]ecuring new aircraft against cyberattack is a question the ... [FAA] and airplane manufacturers are wrestling with in the newest fly-by-wire aircraft ... [C]ybersecurity researchers, in the academic rather than hacker community, also warn of key aircraft communications systems that are potentially vulnerable to hacking either through insertion of malware into flight data uploaded to the flight management system or manipulation through wireless connections ... "Credible examples of potential misuse by such an adversary in future aircraft include: malware to infect an aircraft system, exploit of onboard wireless for unauthorized access to aircraft system interfaces," a team of Boeing and University of Washington researchers found in a 2011 study.

Widespread installation in commercial aircraft of picocell systems to facilitate mobile broadband access would present a huge opportunity to hackers and terrorists, as it provides a multitude of vulnerable entry points into the complex electronics systems of the U.S. commercial aviation fleet. We recommend highly the entire article's contents for the Commission's consideration, as it provides a wealth of useful, publicly available information regarding cyber threats to the commercial aviation system.

While the SSAC members lack the comprehensive knowledge and understanding of what is and isn't capable now or in the future relative to cyberwarfare, we are confident that no other aviation regulators and industry stakeholders, including the Commission, FAA, DHS, TSA, and the airplane manufacturers and airline operators, possess the totality of knowledge and capabilities necessary to assure the public and the rest of the aviation community that such threats are not viable.

---

[25] Mark Clayton, *Malaysia Airlines Flight MH370: Are planes vulnerable to cyber-attack?*, CHRISTIAN SCIENCE MONITOR (March 24, 2014), http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0324/Malaysia-Airlines-Flight-MH370-Are-planes-vulnerable-to-cyber-attack-video.

E. Encouraging More Terrorist Attempts

As discussed above, removal of the long-standing ban will greatly exacerbate the likelihood that acts of terrorism relating to our commercial aviation system will be successful. But to make matters even worse, lifting the ban would encourage more terrorist attempts, because it would provide terrorists with additional tools to use in connection with their plots. It would, in effect, open up a variety of new opportunities for them. Accordingly, given the safety and security issues relating to this proceeding, removing the ban represents a lose-lose scenario (more attempts, and likely more successful attempts). Ironically, if any terrorist groups took the unprecedented step of submitting comments in this proceeding, they undoubtedly would support removal of the ban. It would, after all, make their job a whole lot easier – at the expense of everyone else.

Conclusion

The organizational members of the SSAC work together with the full range of aviation industry stakeholders to protect the safety and security of our nation's commercial aviation infrastructure. The SSAC organizations are united in recognizing that providing passengers the ability to use cell phones during commercial flights will introduce unacceptable risks to aviation security. For this reason alone, the Commission must keep in place its existing ban on in-flight use of mobile broadband technology.

Respectfully submitted,

Christopher J. Witkowski
Director, Air Safety, Health and Security
Association of Flight Attendants-CWA

Sito Pantoja
General Vice President
International Association of Machinists and
Aerospace Workers

Jon Adler

Jon Adler
National President
Federal Law Enforcement Officers Association

Garry Drummond
Director Air Transport Division
Transport Workers Union of America

Michael W. McCormick
Executive Director and Chief Operating Officer
Global Business Travel Association

Alan G. Fishel
Counsel, Safety and Security in the Air
Coalition
Arent Fox LLP

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

In the Matter of	)	
	)	
Amendment of the Commission's Rules to	)	WT Docket No. 04-435
Facilitate the Use of Cellular Telephones	)	
and Other Wireless Devices Aboard	)	
Aircraft	)	

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 ii

I. CALEA IN AN AIR-TO-GROUND CONTEXT 4

II. NON-CALEA OPERATIONAL CAPABILITIES 8

III. POSSIBLE INCREASED RISK OF THE USE OF RADIO-CONTROLLED IMPROVISED EXPLOSIVE DEVICES AS A RESULT OF CONNECTIVITY TO AND FROM AIRCRAFT 13

IV. INTERFERENCE ISSUES 15

V. WIRELESS IN-FLIGHT SERVICE AND ITS POTENTIAL IMPACT ON PASSENGER CONDUCT 15

CONCLUSION 18

SUMMARY

The Commission's proposal to modify and relax its current ban on the airborne use of personal/passenger-owned wireless telephones and other devices — including those used for broadband applications — represents a significant change in the Commission's approach to the use of such devices aboard aircraft. The proposal raises not only regulatory and technical/operational issues, but also important public safety and national security issues.

Although 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 to make additional communications options available to Americans, and to protect and promote public safety and homeland security by increasing airborne communications options available for public safety and homeland security personnel, the Departments take this opportunity to identify for the Commission various public safety and national security-related concerns that stem from the Commission's proposal. In light of the concerns associated with the Commission's proposal, the Departments believe the Commission's inquiry into the appropriateness of lifting its current ban on in-flight personal wireless

---

[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").

telephone use must consider public safety and national security as well as commercial equities by expressly including an analysis of the potential impact that the Commission's proposal and resulting actions could have on public safety and national security.

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

In the Matter of	)	
	)	
Amendment of the Commission's Rules to	)	WT Docket No. 04-435
Facilitate the Use of Cellular Telephones and	)	
Other Wireless Devices Aboard Aircraft	)	

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]

The Commission's rules currently prohibit the airborne use of personal/passenger-owned wireless telephones onboard aircraft.[4] In the *Notice*, the

---

[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 Amendment of the Commission's Rules to Facilitate the Use of Cellular Telephones and Other Wireless Devices Aboard Aircraft*, Notice of Proposed Rulemaking, WT Docket No. 04-435, FCC 04-288 (rel. Feb. 15, 2005).

[4] *See* 47 C.F.R. § 22.925 (prohibiting the airborne use of personal 800 MHz cellular telephones on commercial and private aircraft); 47 C.F.R. § 90.423 (restricting the use of Specialized Mobile Radio (SMR) handsets while airborne in certain circumstances).

Commission proposes to modify and relax this ban in order to facilitate the use of personal/passenger-owned wireless telephones and other devices — including those used for broadband applications — on aircraft in appropriate circumstances.

The Departments support the Commission's efforts to (1) make additional communications options available to Americans and (2) protect and promote public safety and homeland security by increasing airborne communications options available for public safety and homeland security personnel, including a greater ability to engage in direct air-to-ground communications in an emergency. However, the Commission's proposal represents a significant change in the Commission's approach to the use of personal wireless telephones aboard aircraft and — in addition to numerous regulatory and technical/operational issues — raises important public safety and national security issues relating to such use. Thus, the Departments take this opportunity to identify for the Commission various national security-related concerns that stem from this proposal.

Although the Commission's rules technically cover only "cellular" or SMR-based wireless telephones, the Commission's ban effectively prohibits the in-flight use of wireless phones operating in the Personal Communications Service ("PCS") and Wireless Communications Service ("WCS") because of the separate Federal Aviation Administration's ban on the use of wireless telephones and other portable electronic devices on aircraft. *See* 14 C.F.R. § 91.21; "Use of Portable Electronic Devices Aboard Aircraft," Advisory Circular, AC No. 91.21-1A at ¶ 1 (Oct. 2, 2000).

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 among the goals listed in the Commission's current five-year strategic plan.[5] Consistent with the Communications Act and the Commission's strategic goal of preserving and promoting homeland security, the Commission's inquiry into the appropriateness of lifting its current ban on in-flight personal wireless telephone use 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.

---

[5] *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.

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.[6] In 1994, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA").[7] 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[8] that applies to all "telecommunications carriers" — including those using platforms such as wireline, wireless, cable, satellite, and electric or other utility.[9]

---

6 "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.

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

8 "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*").

9 *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").

In the *Notice,* the Commission proposes to allow passengers to use their own wireless telephones aboard aircraft while in-flight. Under this scenario, a call from the passenger's personal wireless telephone would connect to an onboard phone system (such as a "pico" cell) that would then relay the call to the ground and connect it to the passenger's terrestrial wireless carrier (or a different terrestrial wireless carrier pursuant to a roaming arrangement). As both the statutory text of CALEA and the Commission's own pronouncements make clear, wireless carriers are "telecommunications carriers" for purposes of CALEA.[10] Thus, the wireless carriers implicated by this proceeding are "telecommunications carriers" that must comply with the requirements of CALEA.[11] Accordingly, such wireless carriers clearly would be required to comply with CALEA

---

[10] *See* 47 U.S.C. § 1001(8)(B)(i) ("[t]he term 'telecommunications carrier' . . . includes . . . a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))"); CALEA Legislative History at 3500 (the definition of telecommunications carrier in CALEA includes cellular carriers, providers of personal communications services (PCS), and any other common carrier that offers wireless services for hire to the public); *CALEA Second Report and Order* at 7114 -7117.

[11] The Commission recently reiterated that Commercial Mobile Radio Service (CMRS) providers are subject to a variety of obligations under the Communications Act and the Commission's rules, including CALEA. *See In the Matter of Wireless Operations in the 3650-3700 MHz Band; Rules for Wireless Broadband Services in the 3650-3700 MHz Band; Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band; Amendment of the Commission's Rules With Regard to the 3650-3700 MHz Government Transfer Band,* Report and Order and Memorandum Opinion and Order, ET Docket Nos. 04-151, 02-380, and 98-237 and WT Docket No. 05-96; FCC 05-56; 2005 FCC LEXIS 1655 ¶ 37 (2005) (". . . if a wireless licensee provides Commercial Mobile Radio Services (CMRS), which makes the licensee a common carrier, other obligations attach as a result of [the licensee's] decision [to provide CMRS] under Title II of the Communications Act or the Commission's rules (*e.g.,* universal service, CALEA)").

with respect to both terrestrial and air-to-ground communications carried on their networks, and the Departments urge the Commission to affirm this obligation in any statement or decision issued in this proceeding.

Although CALEA applies to wireless carriers in the context of air-to-ground communications, the issue of how CALEA should function in this context 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 content), and to access call-identifying information that is reasonably available to the carrier.[12] 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 statutes related to carriers' duty to assist law

---

[12] *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 call," without having initial call set-up information.

enforcement in performing interceptions.[13] 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.[14] Thus, defining or interpreting "promptly" in a way that is meaningful relative to this unique context is

---

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

[14] 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)).

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.[15]

The Departments also request that the Commission require that any wireless telecommunications capability to or from an aircraft operating in United States airspace utilize mobile switching centers ("MSCs") located within the United States' borders only and not MSCs located along the border in neighboring countries.[16]

II. NON-CALEA OPERATIONAL CAPABILITIES

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

---

[15] 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.

[16] Likewise, to the extent that any telecommunications capability to or from an aircraft relies upon a satellite-based delivery method (e.g. satellite band downlink), the Commission should require that the telecommunications capability utilize ground stations located within the United States' borders only and not those located along the border in neighboring countries.

coordinate an attack (e.g., a hijacking).[17] For example, the use of personal wireless telephones 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 their personal wireless telephones.[18] 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 on the flight, the crew, or a hijacker or

---

[17] Flight attendants and other members of the flying public have also expressed concern that cell phone use could enable terrorists to coordinate a plan of attack more effectively. *See e.g.,* Comments of American Airline Flight Attendant Joyce Berngard; Comments of Flight Attendant Mary Frances Knod; Comments of John D. Bush at ¶¶ 4-5; Comments of Mark Wehrwein; Comments of Nancy Eskau; Comments of Joan MacVicar; Comments of Karen O'Donnell; Comments of Connie Moreno; Comments of Marilyn Begor; Comments of David Gregoli.

[18] 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 cell phone use – had been available.

terrorist) in any effective manner,[19] means that capabilities in addition to those required by CALEA will be necessary.[20]

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 wireless telephones on such an aircraft and the origin of communications directed or terminated to a wireless telephone 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 wireless/air-to-ground carriers/pico cell providers (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 call records relating to all calls processed to and from wireless telephones onboard aircraft operating within United States air space, international air space contiguous or attendant to United States air space, and international air space used enroute to or from United

---

[19] 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.

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

States air space or destinations, and (2) provide law enforcement with immediate access to such records upon lawful request.[21]

Other operational capabilities that the Departments request include that the carrier/pico cell provider be able 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 personal wireless telephone on a given aircraft which has a communication in progress;[22]

(2) Expeditiously identify all personal wireless telephone users on a given aircraft who have communications in progress to or with a personal wireless

---

[21] Upon acquisition of any necessary lawful process (e.g. court order, search warrant, etc.) records of air-to-ground calls subject to the requirement of immediate law enforcement access should include, at a minimum, all calls processed during each domestic U.S. flight and each U.S. inbound and outbound international flight. These records of the air-to-ground carrier/pico cell provider 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 carrier/pico cell provider. The Departments note that, as common carriers, air-to-ground service providers 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 air-to-ground providers would include non-toll call records as well.

[22] 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.

telephone 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 personal wireless telephone 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 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 personally-owned wireless telephones and similar communications devices in-flight.[23] The ability to turn on a wireless telephone or device located onboard an aircraft and have that telephone gain access (i.e. connect) to wireless 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 wireless telephone or device in-flight and use that device as an RCIED.

---

[23] 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 both their provider's network and the pico cell provider and register their location on the aircraft before being able to use their personal wireless telephone in flight;[24]

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

(3) carriers and service providers (including pico cell providers) 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.[25]

---

[24] 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 pico cell provider and the airline to determine the passengers on the airline's manifest that are authorized to use personal cell phones in-flight and their seat locations.

[25] 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 wireless telephone transmissions may cause interference with aircraft navigation and communications equipment that could affect air safety and security.[26] 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 wireless telephones 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. WIRELESS IN-FLIGHT SERVICE AND ITS POTENTIAL IMPACT ON PASSENGER CONDUCT

The Departments note that a significant portion of the public comments filed in this proceeding to date have expressed concern about the effect that passengers' ability to use personal wireless phones in-flight will have on the overall atmosphere of flights and the conduct of passengers. In particular, the Departments note other commenters' concerns that the unrestricted use of personal wireless telephones by multiple

---

[26] In addition to any radio frequency interference that might result from in-flight wireless telephone 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.

passengers on flights could result in an increase in "air rage" incidents among passengers.[27] The Departments believe that the conduct of passengers making use of in-flight personal wireless phones could have serious implications for Federal law enforcement onboard aircraft whose status is unknown to fellow passengers. The first and overriding priority of Federal law enforcement onboard aircraft is to ensure the safety of the aircraft and the flight. 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 in-flight cell phone

---

[27] According to a recent poll sponsored by the National Consumers League and the Communications Workers of America, three out of four travelers said that the use of cell phones on planes would increase the likelihood of air rage. *See In Flight Calls Could Cause Turbulence, Opponents Say,* Washington Post, Page E-1 (Apr. 8, 2005). The comments filed in this proceeding tend to confirm that view, and flight attendants and other members of the flying public have expressed similar concerns about these issues. *See e.g.,* Comments of the Professional Flight Attendants Association at 1; Comments of the Association of Flight Attendants – CWA, AFL-CIO at 2 (expressing concern that even the possibility of regulatory acceptance of in-flight cell phone use will lead to unacceptable levels of unauthorized use, resulting in compromises to operational safety and security via an increase in passenger/crew distractions, misunderstandings, and conflicts); Comments of American Airline Flight Attendant Joyce Berngard ("[t]he introduction of [personal] cell phone use in the cabin will not only increase tension among passengers, it will compromise flight attendants' ability to maintain order in an emergency"); Comments of Flight Attendant Mary Frances Knod; Comments of Flight Attendant A. Aiwohi (flying on a full plane with passengers talking on personal cell phones would create chaos, irate passengers, and an unsafe environment); Comments of Flight Attendant Georgia Leonard (in-flight use of cell phones would incite more incidents of air rage); Comments of Susan Campau at ¶ 3; Comments of John D. Bush at ¶ 3 (conflicts resulting from rude cell phone users are certain to occur, and if these conflicts disrupt or distract a flight it becomes a safety and security issue); Comments of Ruth Kinkead (permitting personal cell phones to be used in-flight is asking for trouble and air rage).

use. Accordingly, the Departments suggest that the Commission, in consultation with the airlines, should establish rules and/or policies concerning in-flight personal wireless phone use and related conduct to minimize any potential for the increase in air rage incidents which could result from unrestricted use of personal wireless telephones on flights.

CONCLUSION

For the reasons set forth above, the Commission should carefully examine public safety and national security-related concerns before modifying, relaxing, or lifting its current ban on the airborne use of personal/passenger-owned wireless telephones 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: May 26, 2005

A bold voice for transportation workers

May 16, 2014

Ms. Amanda Huetinck
Mobility Division,
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th ST SW
Washington, DC 20554

RE: Expanding Access to Mobile Wireless Services Onboard Aircraft
WT Docket No. 13-301; FCC 13-157
Notice of Proposed Rulemaking
Federal Communications Commission

Dear Ms. Huetinck:

On behalf of the Transportation Trades Department, AFL-CIO (TTD), I write in opposition to the Notice of Proposed Rulemaking (NPRM) issued by the Federal Communications Commission (FCC) that would change its longstanding rules that currently ban passengers from using mobile communication services while in-flight. By way of background, TTD consists of 32 affiliated unions that represent workers in all modes of transportation, including those who work in the aviation sector who would be directly impacted by this rulemaking. Several of these affiliates have also submitted comments into the docket, specifically, the Air Line Pilots Association (ALPA); the Association of Flight Attendants-CWA (AFA-CWA); the International Association of Machinists and Aerospace Workers (IAM); and the Transport Workers Union of America (TWU).

TTD opposes the FCC NPRM which seeks to issue new rules to provide airlines subject to applicable Federal Aviation Administration (FAA) and Department of Transportation (DOT) rules, the choice of whether to enable mobile communications services using an Airborne Access System, and if so, which specific services to enable. As TTD stated in the comments we filed to the DOT's ANPRM addressing the potential implications of this FCC rulemaking, we believe allowing passengers access to mobile communication services while in-flight would create

Transportation Trades Department, AFL-CIO
815 16th Street NW / 4th Floor / Washington DC 20006
Tel:202.628.9262 / Fax:202.628.0391 / www.ttd.org
Edward Wytkind, President / Larry I. Willis, Secretary-Treasurer

needless safety issues and security risks.[1] Overturning the two-decades-old ban would allow passengers to talk on their phones, increasing cabin noise levels and making it difficult for flight attendants and pilots to communicate routine and emergency safety announcements to passengers. It could also provide terrorists with new opportunities to inflict harm on our aviation system by making it easier to launch a coordinated attack by communicating in real time with other terrorists aboard the same or multiple aircrafts. We believe that this rulemaking, if implemented, would be detrimental to the safety of our aviation system, and we urge the FCC to withdraw the NPRM.

TTD agrees with the significant security concerns raised by AFA-CWA, IAM, TWU and others in their joint filing. Their comments highlight several new capabilities created by this rulemaking that terrorists could exploit to improve their chances of successfully carrying out attacks using our aviation system. As the commenters note, our nation's aviation system remains a target for terrorists, and we must do what we can to continue ensuring the safety and security of the system while rejecting policies that would move in the opposite direction.

Additionally, we agree with the concerns raised by ALPA, who also requests the FCC to withdraw the NPRM. As ALPA notes, allowing passengers to talk on their phones while in-flight could create adversarial interactions between passengers and crewmembers and possibly endanger the safety of others in the aircraft cabin. We also agree with their concern for the potential of passengers to use cell phones for nefarious use that would jeopardize the security of a flight.

For the reasons noted above and the safety and security concerns articulated by our affiliates, we urge the FCC to reconsider the implications of its rulemaking and withdraw its proposal.

Sincerely,

Edward Wytkind
President

[1] DOT ANPRM on the Use of Mobile Wireless Devices for Voice Calls on Aircraft, Docket No. DOT-OST-2014-0002, comments filed on March 26, 2014.

AIR LINE PILOTS ASSOCIATION INTERNATIONAL

THE WORLD'S LARGEST PILOTS UNION • WWW.ALPA.ORG

535 Herndon Parkway • PO Box 1169 • Herndon, VA 20172-1169 • 703-689-2270 • 888-FLY-ALPA

May 15, 2014

Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Comments Submitted Electronically

Subject: WT Docket No., 13-301, Expanding Access to Mobile Wireless Services Onboard Aircraft

Dear Sir/Madam:

The Air Line Pilots Association, International (ALPA), representing more than 51,000 airline pilots flying for 32 airlines in the United States and Canada, appreciates the opportunity to comment on the Federal Communications Commission's (FCC's) Notice of Proposed Rulemaking (NPRM) to adopt new rules governing mobile communications services aboard airborne aircraft. These rule changes would give airlines, subject to applicable Federal Aviation Administration (FAA) and Department of Transportation (DOT) rules, the choice of whether to enable mobile communications services using an Airborne Access System and, if so, which specific services to enable.

In comments to a separate but related rulemaking, on May 23, 2005 we opposed a similar FCC proposed rulemaking [1] concerning the use of cell phones aboard aircraft. While technology now exists that, if installed, may help to ensure that cellular technology will not adversely affect the navigation and communication avionic components on the aircraft, safety and security concerns for allowing the use of this technology to transmit on or from the aircraft while in flight remain unchanged.

ALPA agrees with the comments submitted by the Association of Flight Attendants-CWA, AFL-CIO (AFA) during the initial comment period,[2] and provides the following supporting remarks concerning inflight safety and security:

- The overall safety of an entire flight, both on the ground and in flight, is primary. The use of cell phones by passengers may have a negative operational safety impact on the ability of flight attendants to perform their required duties. Passenger use of cell phones for

[1] ALPA comments to WT Docket Number: 04-435, FCC 04-288; Amendment of the Commission's Rules to Facilitate the Use of Cellular Telephones and other Wireless Devices Aboard Airborne Aircraft, dated May 23, 2005.
[2] C. Witkowski, Comments of the Association of Flight Attendants-CWA, AFL-CIO, February 14, 2014. http://apps.fcc.gov/ecfs/document/view?id=7521073351

conversations during flight could result in flight attendants being required to have adversarial interactions with passengers to resolve avoidable arguments and/or disputes. The overall cabin atmosphere may more frequently deteriorate to unacceptable levels, perhaps even to the point of adversely affecting and even jeopardizing the safety of all occupants. The flight crew's involvement may also be required if a diversion is necessitated due to unruly passenger behavior.

Security of flight is also essential and ALPA is involved with various efforts to maintain and enhance aviation security. Inflight use of mobile broadband technology could be exploited by terrorists to harm aviation security, negating any of the technology's benefits to law enforcement. We do not believe this public docket is the proper forum to discuss specifics of our concerns, but we would be pleased to discuss them privately.

During review of the FCC website, we noted that three of the agency's five commissioners—Pai, Rosenworcel, and O'Rielly— provided dissenting opinions with this rulemaking that are consistent with our own concerns

In conclusion, ALPA opposes the proposed rulemaking and urges the FCC to withdraw it. Doing so will maintain the current ban on the use of cellular technology while inflight and help protect safety and security.

Please do not hesitate to contact me at sean.cassidy@alpa.org or ALPA Senior Staff Engineer Rick Kessel (703/689-4202, rick.kessel@alpa.org), if there are any questions or comments about our position on this matter.

Thank you for providing ALPA the opportunity to comment on this important NPRM.

Sincerely,

Sean P. Cassidy

Captain Sean Cassidy
First Vice President and
National Safety Coordinator

cc: Veda Shook, AFA-CWA

SC:rk

ASSOCIATION OF FLIGHT ATTENDANTS – CWA, AFL-CIO
501 Third Street, NW, Washington, DC 20001-2797
PHONE 202•434•1300 FAX 202•434•1319

RESTRICTIONS ON USE OF COMMUNICATIONS SYSTEMS BY COMMERCIAL AIRPLANE PASSENGERS

The use of communications technologies by passengers (excepting designated law enforcement officers) on commercial airplanes raises a serious security risk: the potential to facilitate terrorist activities. Of particular concern are systems that provide wireless or wired access to passenger-owned devices for access to the Internet, cellular telephone networks, or onboard in-flight entertainment systems. The potential for terrorists to use such systems to communicate and coordinate tactics, both within the airplane and to team members on the ground and even on other airplanes, is a grave concern to aviation security experts, and one that has been discussed relative to the in-flight use of cellular telephones by the U.S. Departments of Justice and Homeland Security and the Federal Bureau of Investigation in comments to the Federal Communications Commission.[1] Footnote 18 of the DOJ/FBI document states:

> 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 cell phone use – had been available.

Passenger electronic devices pose additional potential threats to airplane software and hardware systems. These threats include, for example, laptop computers that could be used to plant viruses through the wireless network, or music/video players plugged into hard-wired ports that could be used to send electrical pulses into airplane electronic systems, with the potential to disrupt operations.

To minimize the risks to aviation safety and security from the use of onboard communications systems by passengers, the Association of Flight Attendants-CWA, AFL-CIO (AFA) recommends that the appropriate government security agencies, in consultation with the communications industry, immediately conduct rigorous threat evaluations and develop appropriate performance standards for hardware, software and operations. As a further measure to ensure national security, AFA recommends that all wireless communications systems for use by commercial airplane passengers be kept off during periods of high or severe risk for terrorist attacks (as defined by the Department of Homeland Security).

---

[1] *Comments of the Department of Justice, Including the Federal Bureau of Investigation, and the Department of Homeland Security*, In the Matter of Amendment of the Commission's Rules to Facilitate the Use of Cellular Telephones and Other Wireless Devices Aboard Aircraft, FCC WT Docket No. 04-435, Dated May 26, 2005.

ASSOCIATION OF FLIGHT ATTENDANTS – CWA, AFL-CIO
501 Third Street, NW, Washington, DC 20001-2797
PHONE 202•434•1300 FAX 202•434•1319

DISCREET, SECURE, HANDS-FREE, WIRELESS COMMUNICATIONS FOR FLIGHT ATTENDANTS

Following the 9/11 terrorist attacks, the U.S. Congress and various local, state and Federal agencies and experts from the aviation security industry collaborated in unprecedented efforts to prevent the occurrence of similar incidents. On January 18, 2002, a Detailed Guidance document (aka Common Strategy #2) was issued to airline operators by the Federal Aviation Administration (FAA). This document describes strategies that represent a dramatic improvement over those that were so ineffective on 9/11. However, now that locking of the cockpit door is required, restricting access to the flight crew by the cabin crew, and a simulated hijacking exercise has shown the potential for disabling of standard cabin interphone systems by terrorists, it is critical that new technologies and procedures be developed to allow immediate notification to the pilot during a suspected threat in the cabin. Common Strategy #2 stressed the importance of each additional minute of early communication during a security threat, both from the cabin to the flight deck and from the flight deck to the ground, in improving the effectiveness and response by persons on the ground. To best address this need, the Association of Flight Attendants-CWA, AFL-CIO (AFA) supports the development of discreet, secure, hands-free, wireless communications systems as one means to prevent a potentially catastrophic security breach by terrorists.

Crew communications and coordination are absolutely critical as they relate to the survival of all crew members and passengers and the overall control of the aircraft. Tactical communications experts from the military and law enforcement have advised AFA that communication is the primary point of failure during live situational scenarios. A device that is discreet, or as small and innocuous as possible, will allow all crew members to carry on their person the ability to communicate from anywhere in the aircraft at any time under any circumstance. Each personal device must have capability for encrypted, bidirectional communications to allow plain language communications during crisis situations; this will ensure security and reduce confusion. Security of the system is further ensured through use of dedicated hardware components that are accessible only to authorized personnel such as crew members and, potentially, any active law enforcement officers who may have presented credentials to the crew prior to the flight. The hands-free concept will allow crew members under both general emergency (e.g., medical crises, emergency evacuations) and security threat conditions to use their hands to protect themselves, the cockpit, other crew members, passengers, and the aircraft while continuing to coordinate and communicate with the cockpit, the ground, and the rest of the crew. Obviously, a device possessing such characteristics must be wireless.

Additionally, these devices will allow all emergency communications to be:

- Recorded onto the flight recorder for future investigations (while ensuring that such communications, like cockpit voice recordings, are protected from disclosure);
- Monitored by onboard law enforcement officers (if available); and
- Monitored by authorized outside responders for real-time information to
    - Transportation Security Operations Center;
    - FBI Hostage Rescue Team and local SWAT Teams;
    - Local Airport Emergency Responders; and
    - NORAD.

Development and implementation of wireless and wired network systems for use by passengers on airplanes in flight is being pursued by many U.S commercial airplane operators. If cost were the sole constraint, a wireless communications system for use by airline crew members might utilize such passenger-based systems. However, given the potential for security compromises inherent in shared communications hardware, AFA recommends that wireless systems for crew members be completely separate from passenger-accessible systems. Furthermore, to ensure system-wide conformity and harmonization, AFA recommends that development, procurement and installation of hardware and software elements of these systems be maintained within the government. Finally, AFA recommends that the government take responsibility for development of model operational procedures and training curricula for these systems.

Qantas security chief warns of threat to aviation

http://www.heraldsun.com.au/news/qantas-security-chief-warns-of-threat-to-aviation/story-fni0fiyv-1226943398990

- *Alex White*
- *Herald Sun*
- June 04, 2014 8:00PM

AN air security chief has warned that terrorists and foreign spies are the top threats to Australia's aviation industry.

Qantas head of security Steve Jackson, addressing security experts in Melbourne, said he could not rule out a catastrophic attack on an Australian airline.

While declining to discuss any recent threats he confirmed Qantas had worked closely with the Australian Federal Police and ASIO to identify risks.

"I will not dismiss out of hand any potential for a catastrophic cyber attack,'' he said.

"I can't. No one can.

"But I can say to the public: have confidence in your companies and have confidence in your airlines, that we will never compromise your safety or security."

Potential risks included terrorist groups using technology to take over planes in the air, he said.

But Mr Jackson said the most common problem involved hackers trying to disrupt passenger services to damage airlines' reputations.

Countries such as China, which has reportedly used its intelligence services against foreign companies, also posed a threat.

The security chief said foreign spy agencies posed a major threat to the privacy of the 40 million passengers flying Qantas each year.

Mr Jackson used his speech to the Security Exhibition and Conference to encourage businesses to be transparent about security and engage closely with government agencies.

He said white collar crime by "trusted insiders" was also a problem.

He confirmed Qantas worked closely with the AFP last year to catch one of its financial services officers involved in a large-scale fraud.

Mr Jackson, who was a 21-year veteran of the AFP, was on the task force that investigated the Bali bombings.