

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

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

**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. Comm'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 1993⁸ 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 Act⁹ 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>.

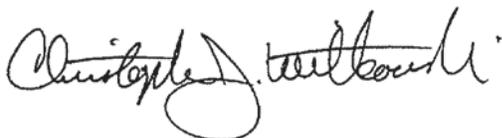
E. Encouraging More Terrorist Attempts

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.

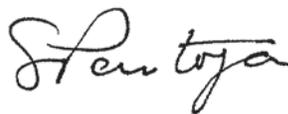
Conclusion

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



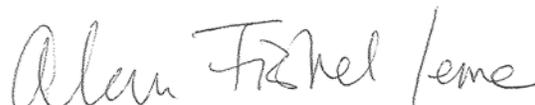
Jon Adler
National President
Federal Law Enforcement Officers Association



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