International Civil Aviation Organization

WORKING PAPER

A36-WP/180
EX/65
12/09/07
English only

ASSEMBLY — 36TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 15: Aviation Security Programme

DISCREET, SECURE, HANDS-FREE, WIRELESS COMMUNICATIONS FOR CIVIL AVIATION CABIN CREW MEMBERS

(Presented by the International Transport Workers' Federation)

EXECUTIVE SUMMARY

The International Transport Workers' Federation ("ITF") recommends that airline operators equip cabin crew members with discreet, secure, hands-free, wireless communications devices. Such devices would enhance communications between cabin and flight crew members, available law enforcement personnel, and ground-based support staff, and thereby minimize the potential for a successful re-enactment of the terrorist attacks of 11 September 2001. To support the rapid and widespread adoption of this important terrorism prevention tool, the ITF invites the Assembly to work with union, industry, and government security representatives to develop technical implementation plans, and encourage Contracting States to adopt these plans.

Action: The Assembly is invited to:
a) note this working paper;
b) study the effectiveness of discreet, secure, hands-free, wireless communications methods for enhancing coordination during security incidents among cabin crew members, between the cabin and the flight compartment, and with ground support personnel, and report these findings as recommendations to Contracting States for rapid and widespread adoption; and
c) Express a commitment to dialogue and ITF participation in any security initiatives involving crew members arising from this 36th Session.

Strategic Objectives:	This working paper will further Strategic Objective B by enhancing global aviation security through improvements to crew communications, which will help to counter terrorist acts perpetrated on board civil aviation transport aircraft.
Financial implications:	Not Applicable.
Reference:	*Manual on the Implementation of the Security Provisions of Annex 6* (Doc 9811, AN/766, First Edition – 2002)

1. INTRODUCTION

1.1 Following the terrorist attacks of 11 September 2001 (9/11), the United States 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 18 January 2002, a Detailed Guidance document, commonly known as Common Strategy #2, was issued to airline operators by the United States Federal Aviation Administration (FAA). Shortly thereafter, on 15 March 2002, ICAO adopted requirements for a flight crew compartment (also known as the "flight deck") door, as well as discreet notification for cabin security breaches, in Chapter 13 of Annex 6, with implementation required by 1 November 2003.

1.2 The aforementioned documents describe strategies that represent a dramatic improvement over those that were so ineffective on 9/11. However, with the flight deck door now locked, and the flight crew no longer readily accessible to the cabin crew, methods are needed to provide for immediate notification to the pilot during a suspected threat in the cabin. The Common Strategy #2 document 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 International Transport Workers' Federation (ITF) supports the development of discreet, secure, hands-free, wireless communications systems as one means to prevent a potentially catastrophic security breach by terrorists.

2. DISCUSSION

2.1 Crew communications and coordination are considered 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 the ITF that communication is the primary point of failure during live situational scenarios. A device that is discreet, meaning 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, which will help 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 would of necessity have to be wireless. Additionally, these devices could allow all communications generated under emergency conditions to be:

- Recorded onto the flight recorder for future investigations (while recognizing that such communications, like cockpit voice recordings, should be protected from disclosure);
- Monitored by onboard law enforcement officers (if available); and
- Monitored by authorized outside responders for real-time transmission to
  - The relevant Security Operations Center;
  - National Hostage Rescue Team and local crisis response teams;
  - Local Airport Emergency Responders; and
  - Military responders.

2.2 In many ICAO Contracting States, development of wireless and wired network systems for use by passengers on airplanes in flight is being pursued by some air carriers. For purely economic reasons, a wireless communications system for use by airline crew members might utilize these proposed passenger-based systems. However, given the potential for security compromises inherent in shared communications hardware, the ITF recommends that wireless systems for crew members be dedicated and separate from any passenger-accessible systems. Furthermore, the ITF recommends that before moving to deploy any proposed communications systems for passenger-owned devices, rigorous evaluations be conducted to eliminate, to the greatest extent possible, potential adverse impacts to safety and security of the aviation system. Of particular concern are systems that are intended to provide wireless or wired access to passenger-owned devices for Internet and cellular telephone network access 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 and one that has been discussed by the United States Departments of Justice and Homeland Security and the Federal Bureau of Investigation in comments to the Federal Communications Commission related to the issue of in-flight use of cellular telephones.[1] Equally disturbing are potential threats to airplane software and hardware systems; for example, laptop computers could be used to plant viruses through the wireless network, or music/video players plugged into hard-wired ports could be used to send electrical pulses into airplane electronic systems, with the potential to disrupt operations.

2.3 Besides hands-free wireless communications systems, other notification methods have been suggested or are presently in use. For example, crew members could perform visual confirmation through the use of a viewing device, such as a peephole, installed in the flight deck door, with audio confirmation from a cabin side crew member. The ITF does not agree that this solution meets either the intent of the ICAO standard or the requirements of Common Strategy #2, as these types of viewing devices are easily defeated with rudimentary tactics such as covering with chewing gum or painting with liquid correction fluid. Furthermore, experts in aviation security with experience in breaching contend that once this is accomplished, the hardened cockpit doors now in use could be removed in a matter of seconds. In addition, hijackers can easily compromise (or forcibly remove from the wall) the existing interphone system, a weakness of the system clearly demonstrated by the events of 11 September 2001 and Operation Atlas, a multi-jurisdictional simulated hijacking exercise conducted in the United States on 4 June 2005.

2.4 Neither does the ITF support a procedure that uses the evacuation alarm to substitute for a discreet, secure, hands-free, wireless device. First, it is possible during a multi-terrorist coordinated team hijack attempt that none of the cabin crew members will be able to reach the location of the evacuation alarm. Second, under the stress of an emergency situation, crew members will instinctively revert to their trained responses: This procedure is counter-intuitive to the safety and evacuation training of crew members. The use of the evacuation alarm as a security notification device will add to confusion and most likely trigger reactions inappropriate during a security threat. During Operation Atlas it was discussed as an option but under the stress of the exercise nobody thought to use the evacuation alarms for security purposes.

2.5 It is the experience in the United States that even with hardened cockpit doors, the Federal Flight Deck Officers program and the Federal Air Marshal Service, all crew members must be prepared to immediately respond during a crisis. In these situations a lag in response time due to poor communications and coordination can prove fatal. As was observed on 9/11, despite the heroic efforts of

[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. Available at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6517617789

all those involved with United Airlines Flight 93, communications lag time led to the tragic deaths of every person on board the aircraft. Finally, the first edition of ICAO's *Manual on the Implementation of the Security Provisions of Annex 6* released in 2002, stated in Chapter 5 *Crew Communication, Coordination and Response,* section 5.1.3:

> There is a strong, natural tendency of the cabin crew to feel isolated, unimportant, and forgotten in back, to feel as dispensable victims of the terrorists. Understandably, those feelings can have a most detrimental effect on crew coordination and on-board communication. This has to be taken into account both during training and during the pre-flight briefing.

2.6 In the future, the Civil Aviation sector must not be lulled into complacency by a perceived lack of threat or relatively limited number of actual terrorist events. In the United States, despite the lack of a serious terrorist attack since 9/11, the Department of Homeland Security admits that aviation remains a target, and that terrorists may seek to involve an increased number of operatives to overcome increased flight security or the resistance of passengers or crew members. Additionally, the 9/11 Commission Staff Monograph on the Four Flights and Civil Aviation Security states on page 54:

> The absence of attacks [prior to 9/11] instilled a confidence that U.S. counterterrorism, at least domestically, was working, allowing the FAA to focus on other serious policy challenges facing civil aviation, including capacity problems, the industry's economic woes, the demand for better customer service, and the ever present issue of safety. To the extent there was a threat, numerous FAA and air carrier officials told us the threat was predominantly overseas.

We cannot allow ourselves to fall back into this dangerous line of thinking.

— END —