



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.