U.S. looks at which tech proposals will fly Government deluged with ideas for airports, airliners

By Traci Watson
USA TODAY

Remote-controlled flights. Bulletproof cockpit doors. Eye scanners at airport gates.

As federal aviation officials ponder how to make air travel safer after the Sept. 11 attacks, they've been deluged with more than 30,000 ideas such as these for applying technology to airport and airline security.

Ideas for new safety gizmos and smart security systems have rolled in not just from companies with dollar signs in their eyes. Citizens who are trying to be helpful have also offered suggestions since President Bush on Sept. 27 advocated some technological advances in security as a way of restoring public confidence in commercial air travel.

And the government is taking them seriously. The Federal Aviation Administration is wading through the proposals it has received and plans to require the airlines and airports to adopt the best ones. The Transportation Department is doing the same. Bush has set aside $500 million for airlines to spend on security technology, including fortifying jet cockpits.

Among some of the other ideas that are being reviewed:

***** Stun guns. United Airlines has proposed giving all of its pilots stun guns, which can subdue assailants with jolts of electricity. Stun guns are now banned aboard planes.

***** Full-body scans. These modified X-ray machines can look through clothing to see weapons, drugs and other items. The Customs Service uses them to screen some passengers arriving from overseas.

***** Video cameras in the cabin. They'd allow pilots to monitor the rest of the plane without leaving the cockpit. Delta has installed test cameras in one of its planes.

***** Strobe lights and sirens in the jet that could distract hijackers.

Although few dispute that spending more money on people, such as baggage screeners, can make travel safer, aviation experts also say that machines like these can do things people can't.

''Machines don't get distracted,'' says Steve Luckey, head of the security committee for the Airline Pilots Association. ''They don't get tired, they don't need a break, and they don't need to go to the bathroom. Technology's great.''

Although Luckey and other experts share the president's hope that technology can make air travel safer, they also dismiss some suggested fixes, such as Bush's suggestion for remote-control piloting, as naive. Other ideas, such as building tamper-proof transponders or ID cards, have provoked disagreement over their effectiveness and affordability.

Even taking seemingly simple steps as strengthening cockpit doors, which Bush advocated as one of the first steps of applying technology to make flying safer, is not so easy.

For years, the FAA required cockpit doors to be light enough to break through in case pilots had to be rescued. Doors also had to allow air to pass during a sudden decompression, so most were designed to swing open or allow a panel to flip open under pressure. Such doors could be easily battered down.

After the hijackings, the FAA gave airlines 18 months to make it harder to storm cockpits.

It will take clever engineering to design doors that can stop a 250-pound man yet still give way in case of emergency, experts say. But they also say it's possible.

So far, the nation's largest airlines have put new locks and bars on cockpit doors as a stopgap measure. Only Alaska Airlines, which flies on the West Coast, and JetBlue Airways, which flies mostly out of New York's Kennedy International Airport, have started installing doors lined with material used in bulletproof vests on all their craft. It's not clear yet whether the doors will meet FAA standards.

Less feasible, experts say, is Bush's suggestion that technology be developed to allow controllers on the ground to land jets if trouble, such as a hijacking, broke out.

''I don't know anybody who's thought about it hard who thinks it's a good idea,'' says John Hansman, a professor of aeronautics and astronautics at the Massachusetts Institute of Technology.

Hansman and others say that such a ground-control system would be just as vulnerable to terrorists as airplanes are -- and to computer hackers as well. Security experts also fear that the takeover of an aircraft's flight controls could prompt desperate hijackers to start killing passengers on the plane to get what they want.

In addition, less than half of the nation's commercial fleet is equipped for this technique. Bringing the fleet up to snuff would cost billions of dollars, experts say. And controllers would need extensive training to handle the task.

''That's one for the reject bin,'' says Robert Poole, director of transportation studies at the Reason Public Policy Institute, a free-market think tank.

Discarding obviously unworkable ideas is easy. Much harder is deciding what to do about technology that has generated both criticism and enthusiasm. For example, Bush has said that the government would fund research on transponders that cannot be switched off in the cockpit.

Transponders, which are normally kept on during flights, identify jets to radar. The Sept. 11 hijackers turned them off so that ground controllers couldn't see the jets' altitude or identification codes.

The recommendation sounds simple enough. But such a step should be approached cautiously, says Charles Higgins, head of a newly created division of Boeing that works on security technology.

For example, what would happen if a redesigned transponder shorted out and began sparking? In modern jets, pilots can shut off power to devices to prevent fires. Should the transponder be given different safety standards than the rest of the electronics?

And what about the hazards of rewiring the cockpit? Wiring is one of aviation's top safety concerns, and work on jet wiring has led to numerous safety incidents. Safety officials say the idea is feasible, but they warn that a rushed effort to redo the wiring of thousands of jets could cause trouble.

Critics also have strong grievances about a technology that has won widespread favor from airlines and some security experts: voluntary identification cards.

Passengers would get one by undergoing a strict background check. Card holders could then breeze through the airport without being subjected to rigorous searches. Automated airport scanners would verify cardholders' identity by checking their palms or the irises of their eyes. Both body parts are as unique as fingerprints.

Similar systems already are in place for passengers entering the Amsterdam airport from abroad. London's Heathrow Airport will soon start a trial of iris-linked ID cards for Americans and Canadians who travel to Britain frequently.

At a congressional hearing last month, FAA Administrator Jane Garvey called this body-based technology, known as biometrics, ''one I'd like to see all of us embrace and advance in an even more aggressive fashion.''

The Air Transport Association, the trade group for airlines, goes a step further. It says such ID cards could be linked to databases held by the FBI, the Immigration and Naturalization Service and other security agencies. That way anyone who's had any trouble with the law would be stopped before getting on a plane.

''If you don't subscribe to the voluntary approach, you're going to go through a very rigid, invasive'' search, says Michael Wascom, the association's vice president of communications.

That's precisely the problem, according to opponents.

''People will effectively be coerced into getting these cards to avoid intrusive, sometimes demeaning searches,'' says Barry Steinhardt, associate director of the American Civil Liberties Union.

Besides, say Steinhardt and others, the purpose of the cards could easily be undermined. It's so easy to concoct a new identity that criminals could get a biometric ID card under a fake name and legal history, Steinhardt says. Others point out that such a system probably wouldn't have prevented the Sept. 11 attacks.

''Seventeen of the nineteen Sept. 11 terrorists were ordinary, law-abiding citizens until after they were on the planes,'' says James Wayman, director of the National Biometrics Test Center at San Jose State University. ''They had Social Security cards and frequent-flier numbers. How could any biometric device have stopped them?'' Even the loudest critics don't doubt that some technologies can improve safety. The ACLU, for example, doesn't oppose the use of biometric ID cards to bar access to

areas off-limit to the public. Such cards are in use at O'Hare International Airport in Chicago.