



AVIATION SECURITY

Keeping GA safe and secure

Amid rising legislative pressures, general aviation continues to refine and enhance security systems.

By Robert Ross
Contributing Writer



Passengers flanked by pilots walk down the ramp at GSO (Intl, Greensboro NC). In today's environment, escorting executives to and

from the corporate jet is a matter of security as much as common courtesy.

Last summer, when an intoxicated young man opened an unlocked hangar at DXR (Danbury CT) in the middle of the night, found the keys dangling from the ignition in a Cessna 172 Skyhawk, and took the plane on an aerial joyride—one that ended 3 hours later at HPN (White Plains NY) just before running out of gas—it sent yet another set of chills through the GA industry.

As if to underscore that wake-up call, a New York State law took effect on Jul 22 that turned the Transportation Security Administration (TSA)'s GA security guidelines into requirements for the state's GA airports.

And, starting this October, small airports in Florida must submit a security plan to that state's Department of Transportation—or lose their license.

It may not be long before other states follow the lead of New York and Florida—and broaden the security plan filing mandate to include airport tenants and users.

I think the subway bombings in London had less of an impact on members of Congress than that turkey in Danbury who flew into New York airspace for several hours, says Robert Olislagers, executive director of the Arapahoe County (CO) Public Airport Authority—the body which oversees APA (Centennial, Denver CO).

In passing laws to tighten security in general aviation, the intent of politicians may be to deprive bombers of an opportunity, but a more immediate benefit could be a stronger bottom line for GA. After all, airports, FBOs and corporate flight operators have always been at greater risk from theft and damage than from terrorism. And, even before plane thefts were in the news, they were looking at ways to upgrade their security.

What they have been doing to address the situation varies along with many factors—including their size, location, level of activity, number of people involved and awareness of potential risk.

Recent conversations with airport managers, FBOs, corporate flight departments and a security system supplier highlight some of the needs, obstacles and benefits involved when it comes to upgrading security.

TSA funds 'labs' at some airports

While some small airports and FBOs may still be complacent because the staff are on a first-name basis with customers, that's no longer the case at W32 (Clinton MD). We're a small place with a smaller space to control than other airports, and we know just about everybody who comes in, says Airport Manager Stan Fetter.

That didn't stop TSA from imposing a special rule that governs his airfield and nearby CGS (College Park MD) and VKX (Friendly MD) because of their proximity to Washington DC. The new security regimen has required Fetter to add staffing, which has raised his costs. The agency paid for him to put up a fence, but he has had to buy electronic cameras at his own expense.



Navigance's Secure Aviation Facilities Environment (SAFE) system lets an airport or FBO operator watch live surveillance video of the facility from anywhere in the world via secure, password-protected Internet connections. At the same time, it archives video to a networked DVR, allowing monitoring of multiple airports, FBOs and airport tenants from a single location.

The biggest changes in security at the 3 Maryland airports, however, have been procedural. Anyone who wants to fly out of here as pilot-in-command or crew has to be fingerprinted and background-checked by FAA and TSA, Fetter says. When a pilot has gotten outside of the established procedures, they're done flying in this

airspace.

At APA—the other end of the GA spectrum—a major grant from TSA has transformed that airport into a working laboratory for testing a variety of security products, systems and procedures.

Rather than installing a single integrated system throughout the airport, says Olislagers, TSA divided APA into simulations of a smaller airport, a flight school operation, a busy gate and a US Customs station. In these smaller settings, it is testing wireless digital cameras, access/entry technologies and alarms in different combinations.

The experiment promises to benefit not only TSA and the airport, but security companies whose products and systems are being tested in the study, such as ADT and Navigance Technologies Group.

Airports on their own

Most GA airports, however, fit somewhere between little W32 and bustling APA and aren't getting money from TSA to enhance their security. They're on their own to weigh security needs, review vendors' proposals and check their bank accounts.

"We have 6 airports and 3 managers, who can't always be present, says Gary Schmidt, director of reliever airports for the Minneapolis–St Paul Metropolitan Airports Commission. It would be great to have an alarm system all hours of the day that lets us check and see if a response is warranted or not.

We need an integrated system that ties all our tenants under one security umbrella, but I don't want to have to go out and put it together myself, Schmidt says.

That's why he's talking to Navigance, a company that creates security packages combining other companies' alarms, cameras, entry/ access technology, fencing, lighting and motion/sound sensors and its own services—monitoring, maintenance, and upgrades. The key benefit of the system Schmidt is considering would be system monitoring and coordinated response.

At PWK (Palwaukee, Chicago IL), Manager Dennis Rouleau has also been considering Navigance. He wants to link his airport's cameras with those of his FBO tenants to create a single online security system that could be monitored from his office or offsite, even by the police. He has decided to employ a combination of magnetic smart cards and coded keypads for entry to restricted areas, but says he may consider switching later to a biometric system that uses thumbprints.

For Bob Brewster, who manages Lynch Corporate Services, an FBO at DAB (Intl, Daytona Beach FL), reliability is a key factor in any new security system he considers. People get tired of false alarms and they turn off their own alarms, he says. It's a common problem. What use is an alarm system when you have to open and close your gates manually? he asks. Here in Florida, the lightning capital of the country, lightning strikes sometimes cause our gates to open.

Brewster says Lynch is looking for a system that isn't so unique it can't be used in different locations should his company open FBOs at other airports. We don't want to have to reinvent the wheel, he says. We want all of our security systems to talk to each other.

John LaFontsee, at Regent Aviation, a Million Air franchise at STP (Downtown, St Paul MN), is planning to install a new motion-sensitive surveillance system to secure 13 hangars on 40 acres.

The new cameras' clarity and ability to zoom in are amazing, he says. You can say, 'Show me all the movement in just this one area during the past 24 hours.' He's intrigued by biometric systems that use thumbprints for identity, but wants to wait until they're perfected.

Human line of defense

Even the newest technology is nothing without people, LaFontsee says. Our industry has to train our employees and even the FBO population to keep an eye out and look for suspicious activity. He makes security a regular part of his employee briefings and monthly tests for line techs.

It's tougher with customers, says LaFontsee. We ask for their help, but it's a delicate balance between the aircraft's convenience and locking it down. After Sep 11, half of our customers said, 'Make security tougher,' but the other half said, 'Don't take my freedom away.'

Jennifer Weishaupt, manager of security for Shell Aviation, advises 305 FBOs around the US on security practices. She and her staff look for lights that work, a secure fence line, and a gate that is controlled from the FBO office or with a swipe card. At the larger locations, I recommend changing the access code once a week, or at least once a month, she says.

Weishaupt tells FBO owners they have to hold their employees responsible for reporting anything that seems out of place, including packages and people.

There has to be the expectation that each person is the last line of defense. Better that 2 people report it than no one, she says.

Flight departments check ahead

We rely on FBOs and their personnel for security wherever we travel, says Ron Houle, chief pilot of Churchill Industries' Gulfstream G200, which flies regularly to GON (Groton CT), APF (Naples FL) and STP, its home base. Our policy is, if you can't see the plane it has to be locked. He says he expects FBOs to have fencing, lights, an alarm system and cameras to monitor their employees.

Al Rudd, owner of Minnesota Jet, which operates 6 aircraft, looks for FBOs that have security procedures in place, not just technology. All the airports we go to have raised the bar much higher, he says. Of course, the issues are different at Havre MT than at Minneapolis.

Foreign destinations, however—particularly Mexico and the Caribbean—are another matter for Rudd. In remote areas, you start to be concerned about theft or that someone could kidnap your executives, he says, adding that he sometimes puts a 24-hour watch on a plane when it's abroad.

Pentastar, based at PTK (Pontiac MI), operates jets for Detroit area auto companies, whose engineers and executives fly frequently to plants in Brazil, Europe, Mexico and elsewhere. If we schedule a flight into an airport that's new for us, we call ahead to verify the security situation and details about the airport, says Kellie Rittenhouse, director of Pentastar's managed aircraft services. We work with local handlers and do a risk analysis based on their security recommendations.

Thinking beyond security

We're not only dealing with security to block terrorists, but also vandalism or acts of revenge against an owner, says DAB-based Lynch Corporate Services' Brewster. People want to know their property is safe when they're not there.

A good security system is a form of protection against fraudulent claims, Houle adds. Several years ago, after a plane was damaged in a hangar here, the line guys denied moving it. But they pulled the videotape and saw them moving the plane.

We're more likely to be affected by a disgruntled employee or someone in a messy divorce whose spouse makes trouble, says Rouleau at PWK, or someone who doesn't pay his bill or a contractor who tries to visit a construction site off hours. With the smart card system, you can block them out.



[http://www.propilotmag.com/September/images for Sept/NaviganPatt_big.jpg](http://www.propilotmag.com/September/images%20for%20Sept/NaviganPatt_big.jpg) Navigance system uses an array of security tools, including (clockwise from lower R) laptop computers, which can be used for worldwide monitoring of GA airports and FBOs, perimeter fencing products, fingerprint device and card readers, which can be used as access controls to doors or gates, and DVR-supported pan/tilt/zoom cameras, which permit easily retrievable 24-hour surveillance.

As Rouleau learns more about wireless digital technology, he imagines new uses that are unrelated to its primary security function. He says, A lot of my time is wasted waiting for FAA to show up and issue a release to move a single-engine plane with collapsed gear from the runway. I'll have 6 or 7 planes orbiting overhead. With a Web-based digital video system, I could have FAA go online, see the image of the plane, and release it without having to come out.

Another novel use for the system, as Rouleau envisions it, would be to let airborne pilots look up runway conditions from their cockpit before landing at PWK during the winter.

Not surprisingly, Bob Jandebour, president and CEO of Navigance, encourages this kind of possibility thinking about the security systems he markets, and offers a few ideas of his own. Jandebour even promotes the use of his motion and sound-sensitive security cameras as tools for evaluating and training new employees and improving operations.

Paying for it all

After all the security holes have been addressed, there is that hole in the bank account to consider. Jandebour says his company can put a security system together for as little as \$100,000 at a small airport and from \$200,000–300,000 for a larger airport.

Regent Aviation's LaFontsee calls the security system he hopes to buy very pricey, knowing full well the market will probably bring the cost down. You never thought you could buy a Dell computer for \$700, he says wistfully, but we can't wait for the price to go down.

With state legislatures beginning to force general aviation to develop security plans, waiting may not be an option.

A certain percentage of FBOs believe they don't need anything, Brewster says. They think, 'Who would want to break into our hangars' But, as security evolves, the level of sophistication even at smaller airports will have to come up. It's not cheap, but like radios and avionics, the technology will be adopted when people see that it's better.

To make its systems more palatable to the low-bid tastes of airport boards, Navigance has developed monthly payment plans. That could work for Schmidt at MSP, who allows that if everything falls into place, the security package he's weighing will cost about \$2000 a month. That's if we assess fees from our tenants, he adds.

Rouleau says charging an extra cent in users' fuel flowage fees to pay for improved security at PWK is an option, but one he'd rather avoid. We're looking at other ways to make it happen, he says, including trying to interest TSA or FAA in funding a security laboratory at his airport because of its proximity to Chicago.

Yet, even with the most sophisticated technology in place, you still have to lock the gate at night.

Robert Ross is a Florida-based freelance writer specializing in aviation-related topics.

