

Strange Occurrences Highlight Insider Threat to Aviation Security

August 14, 2018 (IN10954)

Related Author

- [Bart Elias](#)

Bart Elias, Specialist in Aviation Policy (belias@crs.loc.gov, 7-7771)

On the evening of August 10, 2018, an airline ramp worker [stole a 76-seat turboprop](#) from Seattle-Tacoma International Airport, crashing it on a remote wooded island in an apparent suicide. Days later, on August 13, 2018, a corporate pilot released on bail following a domestic violence arrest hours earlier stole a business jet and [crashed it into his Utah home](#). In [another incident in Utah in July 2012](#), a SkyWest Airlines pilot sought by authorities regarding the stabbing death of his girlfriend stole a regional jet from the St. George Municipal Airport and crashed it through an airport fence before fatally shooting himself inside the cockpit.

While the only fatalities in these three incidents were to the individuals who commandeered the aircraft, the events raise concerns about mitigating the risk of aircraft thefts carried out with the intent of causing harm on the ground. This occurred on January 5, 2002, when a 15-year-old student pilot, apparently inspired by the terrorist attacks of September 11, 2001, stole a single-engine Cessna and deliberately [crashed it into a skyscraper in downtown Tampa, FL](#). A common factor in all of these incidents was that the perpetrators exploited their knowledge of the aviation system and their access to aircraft to steal and crash them, highlighting long-standing concerns about what has been commonly referred to as the "[insider threat](#)."

Background Checks and Threat Assessments

Historically, the insider threat has been dealt with at airports through background checks, credentialing, and access control measures. The Transportation Security Administration (TSA) requires that all airport and airline workers undergo [criminal history records checks](#) and [security threat assessments](#) before being issued credentials granting them unescorted access to secured areas of commercial airports and airline aircraft. The criminal background check requirements were put in to place after a disgruntled former airline employee boarded a [regional jet in California on December 7, 1987](#), with a loaded handgun that he used to shoot his former boss and the two pilots before crashing the airplane, killing all 43 on board. Additional checks against terrorist watchlists were instituted following the 9/11 attacks. A recent enhancement to the vetting process incorporates regular checks against the Federal Bureau of Investigation's [RapBack](#) service to provide notification of criminal and terrorist activity involving individuals in positions of trust including credentialed airport and airline workers. Additionally, for pilots and mechanics, a Federal Aviation Administration (FAA) database is continuously compared against the Terrorist Screening Database to determine if any

[FAA certificate holders](#) might have ties to terrorist organizations. Student pilots must demonstrate proof of citizenship, and [non-U.S. citizens](#) must undergo TSA background clearances before starting their flight training.

Security Awareness Training and Resources

TSA requires flight instructors and certain other flight school employees to complete initial and annual refresher training on [security awareness](#). These online and computer-based courses include information on detecting and reporting suspicious behaviors. Similarly, commercial airport workers with access credentials must undergo [security training](#), including training to prevent unauthorized access to secured areas and detecting and reporting suspicious activities. At general aviation airports, [Airport Watch](#), an initiative modeled after neighborhood watch programs, provides educational materials to pilots and airport workers and a hotline to report suspicious activities.

Access Controls and Surveillance Technology

Commercial airports are required to implement [access control and credentialing systems](#) to control entry to secured areas. While access control measures vary from airport to airport, most large airports implement a layered system in which workers have limited access to only those areas relevant to their job functions. [Analysis of video](#) and access logs may be used to detect and highlight certain activities and events, such as accessing areas not authorized by an individual's clearance level, accessing areas not related to the individual's job functions, or accessing areas during nonwork hours. Monitoring and analysis of surveillance and access system data may help detect potential threats in some cases. Detecting security incidents as they unfold nonetheless may be difficult, particularly in a busy airport environment, because threat actions may be quite subtle and may not stand out from routine airport activities. At small general aviation airports, on the other hand, suspicious activities may go undetected because few individuals may be present, particularly at odd hours, and access control measures and surveillance resources and capabilities are often more limited.

Mental Health Concerns

Detecting possible changes in the mental health of airport and airline workers, particularly changes that may lead someone to engage in violence at the workplace or use their access to aircraft to commit suicide or carry out a targeted attack, poses unique challenges. Mental health monitoring and reporting in the aviation industry was addressed in policy discussions after it was revealed that the copilot responsible for [the suicidal crash of a Germanwings airliner on March 24, 2015](#), was being treated for depression and a possible psychosis. In response, French authorities urged changes in international laws to require that mental health providers report pilots whose psychological condition may pose a threat. Others have pushed for routine [mental health screening for pilots](#). However, mental health screening may have limited effectiveness because screenings may not be performed frequently enough to detect changes in an individual's mental health status, and workers may be motivated to mask possible mental health conditions for fear that they could lose security credentials and aviation certifications required for their job. Requiring mental health checks of aviation workers, particularly those who have no specific certification requirements, may prove challenging both legally and practically. However, efforts to raise mental health awareness and encourage employees to self-report issues with impunity or express concerns about coworkers, perhaps under existing [safety reporting protocols](#), could potentially help identify individuals who may pose a safety risk to aviation.