Let FAA failure be a wake-up call

System shutdown highlights importance of infrastructure investment

By SHELDON H. JACOBSON

On Jan. 11, the Federal Aviation Administration Notice to Air Missions system failed. This resulted in a nationwide ground stop, impacting thousands of flights and thousands of passengers.

Could this failure have been avoided?

The National Airspace System is the highway for air travel, with the FAA serving as the de facto "traffic cops." One of their objectives is to ensure the safe and efficient flow of air travel, from the moment airplanes leave their departure gate, on their trek to the runway, between takeoff and landing, and their path back to a deplaning gate. With around 25,000 flights every day, air traffic controllers are the unsung heroes of air travel in the United States.

Yet their job is only as effective as the computer systems available to monitor flights and possible hazards that can compromise air travel safety.

The Notice to Air Missions system is designed to provide short-term information for pilots prior to their departure. These may include emerging bird hazards at airports, runway closures or low-altitude construction obstacles that may be temporary or transient, all of which provide information that supports pilots and safe air travel.

The failure of the Notice to Air Missions system may have been due to either software or computer hardware. A corrupt database file appears at the root of the issue. No matter what the cause, any system that provides useful information to pilots and enhances flight safety is critical. Given that the FAA was communicating such information overnight via telephone hotlines, this suggests that the information was available, but the computer systems used to relay it had broken down.

Will such a failure occur again?

Every computer system in use by air traffic controllers is vulnerable. Whether it be due to cyberattacks, software glitches or hardware breakdowns, any computer system can fail. That is why any software involved should have multiple backups or redundancy to ensure that if a hardware failure (or even a ransomware attack) occurs, mechanisms are in place to restore the system as quickly as possible.

This incident highlights how vulnerable our nation's critical infrastructures are to disruption. The ripple effect of a national air system ground stop for a few hours percolated into thousands of flights delayed or canceled, with many not even scheduled during the initial ground stop. This may seem odd to most travelers, who wonder why their 1 p.m. flight was delayed or canceled given that the ground stop ended at around 9 a.m.

The lessons learned from the FAA ground stop is that safety must always come before efficiency and service. Air travel is a national treasure, with the ease at which people and goods can safely move across the nation.

Computer systems can fail based on the age of the hardware, or glitches in the software. Maintenance and updates can avert many such failures, but not all. Given that system failures like the one just experienced are relatively rare, this suggests that air traffic controllers are doing a good job in spite of system limitations.

Can they do better? Of course. But at what price? Like any maintenance schedule, the cost of maintenance must be balanced against the cost of failure.

As the FAA was critical of Southwest Airlines for its failed computer system a few weeks ago, an FAA computer system failure shut down the air system, costing airlines millions of dollars. Lessons learned from both computer system failures are noteworthy for all stakeholders to heed.

In a few days, the memory of the Notice to Air Missions system failure will be forgotten. The important lesson learned is how vulnerable our critical infrastructures are to any type of failure, and why investments in critical infrastructures are important for everyone.

Sheldon H. Jacobson is a professor of computer science at the University of Illinois at Urbana-Champaign. He has also studied aviation and aviation security for over 25 years, providing the technical foundations for risk-based security and TSA PreCheck. He wrote this column for The Dallas Morning News.