ALLIED PILOTS ASSOCIATION

The Threat of GPS Jamming and Spoofing

Global Positioning System (GPS) jamming and spoofing has become a major threat to the safety of commercial aviation worldwide. Previously observed mainly in conflict zones such as Ukraine and the Middle East, GPS jamming and spoofing systems have rapidly proliferated in the last year, with incidents increasing from a few dozen each day in late 2023, to hundreds a day in the early months of 2024, to over a thousand a day as of October 2024.

Spoofing—where a threat system will "hijack" a GPS signal to an aircraft, sending the aircraft erroneous time and position signals—is particularly insidious due to its wide-ranging effects on not only navigation, but also secondary critical systems such as Enhanced Ground Proximity Warning Systems (EGPWS), Automatic Dependent Surveillance Broadcast (ADS-B), and Controller-Pilot Datalink Communications (CPDLC). Loss of navigational performance has been severe enough to force aircraft off the North Atlantic Organized Track System (NAT-tracks) ocean-crossing jet routes. Erroneous EGPWS alerts have triggered, prompting crew responses in congested airspace. ***An aircrew fighting widespread systems degradation due to GPS spoofing presents significant safety-of-flight concerns.*** Couple that systems degradation with potential in-flight emergencies, poor weather, and/or low visibility, and the consequences could be disastrous.

This issue is geopolitically complex, as U.S. allies and partners use this technology for their own defense. It is not diplomatically realistic to simply ask a nation to "turn it off." Thus, addressing the threat of GPS spoofing will require multiple lines of effort spanning technology, procedures, training, and regulation.

Measures needed to mitigate the risk from GPS spoofing include:

- **Technical**: adaptation of existing equipment to better integrate ground-based position references from existing navigational aids; installation of alerting system to warn aircrew of possible spoofing/jamming; installation of GPS "on/off"-style switch to stop erroneous GPS signals from reaching subsystems
- **Procedural**: incorporation of aircrew procedures directing response to indications of GPS spoofing and jamming by reverting to inertial-only navigation, or using secondary systems such as ground-based navigational aids (NAVAIDS) and Distance Measuring Equipment (DME)
- **Training**: development of simulator-based training scenarios to instruct aircrew on indications of GPS spoofing and proper response and Air Traffic Controller training on proper handling of affected aircraft
- **Regulatory**: revision of policy to create a more resilient system of position, navigation, and time reference, incorporating proven systems such as ground-based NAVAIDS and DME alongside GPS and Global Navigation Satellite Systems (GNSS); and revision of Federal Aviation Regulations publications to permit needed technical fixes to equipment

While all these lines of effort will be critical to addressing the threat of GPS jamming and spoofing, it is essential to understand that there also needs to be a change in mindset. For decades, aircraft and systems have been designed with the assumption that satellite navigation would always be accurate and available. That assumption is no longer valid. ***Commercial carriers and aircraft manufacturers must design systems which do not require GPS to maintain full functionality, and policymakers must ensure that a strong network of ground-based aids to navigation remains funded and maintained into the future.***

For questions or additional information please email GAC-Chairman@alliedpilots.org

Current as of December 1, 2024