POSITION PAPER

26POS05
24 February 2026

Cyber Threats

NOTE

This paper supersedes 16POS08, of the same name.

INTRODUCTION

IFALPA and IFATCA continue to monitor the threat of cyberattacks against aircraft, ground facilities, and other critical infrastructures which pose a significant threat that may cause disruption, unsafe situations, or ultimately loss of life. The purpose of this paper is to articulate this threat, draw attention to ways in which it is being addressed and propose a way forward.

BACKGROUND

Today's commercial flights, whether passenger or cargo, generate and require a large amount of data and interfaces that are critical to the safe operation of the aircraft. Much of the technology currently in use was developed at a time when aircraft were relatively unconnected to the external environment, and therefore most of the systems were not originally designed with cybersecurity principles in mind. Furthermore, communications between such systems cannot be checked for integrity and are unencrypted.

Cyberattacks can be carried out from virtually anywhere, by anyone with sufficient knowledge, using low-budget methodologies. These attacks can have several objectives, such as obtaining confidential, critical or sensitive information, manipulating or erasing information and/or controlling or destroying systems or services. In many cases, the compromised system may not even have been targeted but is taken down as a result of an attack elsewhere (collateral damage).

Cybersecurity should therefore be considered throughout all aviation communications pathways and applications. This cannot be done in silos, i.e., by single entities for their own systems only. Due to the many interdependencies in civil aviation, cybersecurity should be a shared responsibility of National Authorities, aircraft manufacturers, airlines, airports, and Air Navigation Service Providers (ANSPs), together with their respective supply chains. Since public safety is at stake, States and oversight entities should have the authority to ensure all parties act in accordance with current standards.

REGULATIONS

IFALPA and IFATCA welcome actions taken by States to establish regulations and procedures that set the minimum requirements that the aviation industry must meet. Many Authorities have either created or are in the process of drafting their own regulations concerning information security. Recognizing that it will take time for these regulations to come into full force and be audited, IFALPA and IFATCA encourage affected entities to comply at the earliest opportunity. States lacking cybersecurity regulations should develop and implement them without delay. IFALPA and IFATCA also welcome ICAO's Cybersecurity Action Plan (CyAP), which provides the foundation for States, industry stakeholders, and ICAO to work together to develop the ability to identify, prevent, detect, respond to, and recover from cyberattacks on civil aviation.

State regulations should mandate proper training of all relevant personnel so that they can detect and report actual cyberattacks and vulnerabilities in a timely manner, and act accordingly. Compliance should be audited by the relevant authorities.

INFORMATION SHARING

In other industries, information sharing has proven to be essential in the protection of critical infrastructure. In many countries, structures have already been set up for civil aviation. It is essential that all stakeholders share information on security breaches, detected attacks, and best practices to enhance the overall security of the system. This requires a great degree of trust and confidentiality, and the assurance that the information on the methodology behind any security breach will not be made public until appropriate countermeasures have been implemented. State regulations should mandate the timely reporting of relevant cyber events (including attempted attacks).

POSITION

The cyber threat landscape is of significant concern to the safety and security of civil aviation. This threat should continue to be addressed in a coordinated manner, both by industry and regulators.

BRIEFING LEAFLET ON CYBER THREATS

The dedicated IFALPA Briefing Leaflet, 17SECBL01 provides guidelines to help establish an environment in which cyber threats are fully understood and managed, reducing risk to an acceptable level.