Aviation Security
Fact Sheet

Overview
UN Security Council Resolution 2309 makes it clear that governments have the primary responsibility for aviation security. The industry is fully committed to a partnership relationship with governments that keeps passengers, crew and cargo secure. The promotion of aviation security is a central priority for IATA, with its activities delivered through advocacy, standards-setting and adoption as well as services and products.

Guiding Principles
The IATA Aviation Security work plan is focused on delivering outcomes based on the following principles endorsed by the membership (IATA Security Advisory Council):

• Drive improvement in aviation system security performance and response
• Drive government trust and confidence in airline management system principles
• Collaborating on evolving threats and improving crisis management
• Improve security efficiency through risk-based policies

IATA is calling for an increase in coordination and collaboration between airlines, airports, regulators, law enforcement agencies and intelligence communities to effectively address the threat trajectory and quality of aviation security measures. States are responsible for the collection of protective security intelligence. They must share this information with operators to effectively support the precision of their risk management systems.

IATA’s work plan aims to take a proactive strategic approach based on risk management and security situational awareness. Adopting a risk-based policy to the implementation of shared security measures ensures efficient, cost-managed and accurate controls are in place. With such an approach security could play a role of enabler in the industry restart.

IATA strongly encourages the regulators to ensure:

- Effective Implementation of baseline security measures imposed via the core ICAO Annex 17 Standards
- More transparency with respect to the outcome of audits and inspections (for example for subcontractors)
- Timely sharing of all relevant risk information with industry
- Appropriate and timely consultation with stakeholders, in particular when imposing additional measures
- Rigorous cost-benefit analysis is conducted
- A holistic risk-based approach is taken to identified problems
- New regulations are consistent, harmonized and coherent
- Proportionate enforcing measures and adequate implementation

Collectively, States and the industry need to develop smarter and faster next-generation aviation security solutions for airline passengers and cargo customers. Again, security in the current times, should be seen not only as a set of safeguards but also as a confidence reassuring enabler in the entire aviation restart process.
Governments and industry partners must improve their agility and readiness to manage emerging threats and while the passenger traffic rebounds gradually and cargo transport increases and gets more attention (e.g. in the global distribution of vaccines). Regulators need to identify opportunities for recognition and reassurance of respective aviation security systems or their components.

**Objectives**

1. Be the first and reliable point of contact for association members and appropriate authorities in terms of industry outreach on aviation security

2. Facilitate effective allocation of airline security costs and improve understanding of performance measurements in security (e.g. IATA 100% Hold Baggage Screening One-Stop-Security initiative)

3. Be the lead association in promoting and supporting innovation as well as developing a forward-thinking culture in aviation security (e.g. Security Risk Intelligence Portal) [www.iata.org/security](http://www.iata.org/security)

4. Lead, support, promote, consult, and advise on international, regional and industry standards, regulations, recommended practices, guidance, and best practices

5. Develop an industry-led cyber/digital security strategy with the core focus on preventing and defending against intentional acts of electronic interference and/or acts of unlawful interference [www.iata.org/cyber-security](http://www.iata.org/cyber-security)