IATA POLICY POSITION [1] ON AVIATION CYBERSECURITY

REQUEST FOR ACTION FROM CIVIL AVIATION STAKEHOLDERS, REGULATORS AND AUTHORITIES

BACKGROUND

A major shift in the digital transformation of the civil aviation ecosystem is currently taking place. Dependency on Information Technology as well as the interest to augment connectivity is ever increasing. These new capacities could expend vulnerabilities and risks if not adequately managed and controlled, especially when it could affect or have an impact on safety, security, operations, and airworthiness. Therefore, to ensure safety of flight and airworthiness, the civil aviation industry needs to be working collaboratively, be more transparent and exchange information on risks that this industry shares.

IATA's members agree that cybersecurity matters for all aviation stakeholders, including their respective supply chains. Each stakeholder has a fundamental role to play in safeguarding the information, systems, and assets of the aviation ecosystem, where collaboration and information sharing among all are essential.

Moreover, at the same time of this massive digital transformation, Operators are facing extensive cybersecurity regulation proliferation. The lack of harmonization and duplication of efforts are challenging all aspects of the Operator's cybersecurity operations, in support of compliance, in due time.

Whether an Operator is bound by regulations within its own region or while operating in multiple others, it is crucial that reporting and compliance be harmonized to ensure an efficient way for Operators to demonstrate the same compliance evidence to each regulator, therefore one to many approaches is essential.

IATA'S Role

In this context of cybersecurity regulations being articulated worldwide, IATA and its governance groups are committed to continue working on standards and guidance material aiming to strengthen civil aviation resilience.

IATA is currently developing its IOSA Cybersecurity for Safety, Security and Airworthiness Standards and Recommended Practices ISARPs, to support harmonization of Operators' compliance with as many regulations as possible. It is important that Regulators weigh in on the mapping and equivalence of the proposed set of ISARPs being developed. IATA encourages all regulators to support the development of those SARPs so that Operators lighten their compliance efforts/burden and focus on the development of cybersecurity posture.

[1] **Endorsed by the IATA Cybersecurity Management Working Group CMWG**

POSITION

REGULATORS AND AUTHORITIES:

1. Regulators to establish a mutual understanding and harmonization of their approach to cybersecurity requirements, including reporting of cybersecurity events and incidents.
2. Regulators to support IATA Operational Safety Audit Cybersecurity for Safety, Safety and Airworthiness Standards and Recommended Practices CSSA ISARPs development and recognize the work as permissible Means of Compliance.
3. Regulators to recognize the potential impact on safety and airworthiness of new and existing interconnected technologies and their associated supply chain who have minimal existing requirements in civil aviation regulation.
4. Regulators to recognize that some supply chain partners not bound by Civil Aviation or other critical infrastructure regulations may pose systemic risks to the aviation sector, for example technology Managed Service Providers. Recommend that Criteria be established to identify which should have cyber security regulatory oversight and how this may be achieved.

INDUSTRY:

5. Industry to implement efficient cyber security controls based on periodic risk assessments, as more equipment and new technologies are connected to the internet, to reduce the risks and increase resilience.
6. Industry to increase the level of transparency over responsible information sharing and exchange, including cybersecurity events and vulnerabilities, as well as assessing the shared risks and dependencies between aviation stakeholders and supply chain partners for the benefit and resilience of the industry.
7. Industry to encourage collaboration between aviation Original Equipment Manufacturers OEMs/Suppliers and Operators to increase the availability of security log information and alert profiles for Operators, and increase the context OEMs receive, with alert notifications from operators to facilitate earlier detection of potential cyber events.