International Civil Aviation Organization

WORKING PAPER

A42-WP/667
EX/292
12/9/25
(Information Paper)
English only

ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security — Policy

INDUSTRY INITIATIVE TO ADOPT CYBERSECURITY RECOGNITION ARRANGEMENTS

(Presented by the International Air Transport Association (IATA))

EXECUTIVE SUMMARY

The international cybersecurity regulatory landscape is becoming unnecessarily complex. States are enacting unique cybersecurity regulations that are not conducive to harmonization or coordination between other Member States. This causes global airline operators to navigate through an increasingly complex and often conflicting landscape of cybersecurity requirements. While this situation is acknowledged, and the subject of harmonization often discussed, a more practical approach is required.

Strategic Goals:	This working paper relates to Strategic Goals: *Every Flight is Safe and Secure* and *The Economic Development of Air Transport Assures the Delivery of Economic Prosperity and Societal Well-Being for All.*
Financial implications:	Not applicable.
References:	Annex 17 — *Aviation Security* ICAO *Aviation Cybersecurity Strategy* ICAO *Cybersecurity Action Plan* A41-19 Addressing Cybersecurity in Civil Aviation

1. COMPLEXITY OF EXISTING CYBERSECURITY REGULATORY ENVIRONMENT

1.1 ICAO demonstrated strong leadership by recognizing the need to address cybersecurity when it included SARPs on measures relating to cyber threats in Annex 17 Chapter 4 – *Preventive Security Measures*.

1.2 While Annex 17 establishes a baseline cybersecurity SARP for States, there are other factors which contribute to regulatory complexity and support the need for a recognition framework.

1.2.1 Most States have enacted additional National cybersecurity requirements that include incident reporting, implementation of extra controls and measures, and extensive compliance obligations. Although some States use standards or similar approaches to cybersecurity regulations, they often differ in implementation, scope, definitions, thresholds, data protections, and inspection/auditing requirements.

1.2.2 In some cases, information developed for compliance with States' cybersecurity regulations is sensitive information, making it difficult for air carriers to share directly with foreign States.

1.2.3 States may also allow covered operators to retain sensitive information at operators' headquarters which require regulators to travel to an operator's location to conduct audits and inspections.

1.2.4 Operators make cybersecurity decisions at their headquarters, which is not always within States in which they operate.

1.2.5 The competent authorities for civil aviation are not always responsible for all their State's cybersecurity requirements that apply to air carriers. Operators must consider numerous State regulator requirements to ensure compliance with a myriad of State cybersecurity regulations.[1] [2]

1.2.6 While operators' critical systems are global, they are managed within the operator's national State which makes adhering to auditing or inspection requirements by other States impractical.

2. NEED FOR SIMPLIFICATION

2.1 Existing cybersecurity requirements have created an overly complex, duplicative, and increasingly disparate environment. In some cases, National carriers face numerous State cybersecurity requirements that apply extraterritorially, while others are only obligated to follow their own State's requirements.

2.2 States' incident reporting requirements are often informed by national security priorities and concerns. Some States restrict cybersecurity incident reporting, which creates disharmonized and conflicting requirements between States. Operators must choose between conflicting requirements which may limit reporting due to legal concerns or to protect proprietary information.

2.2.1 To address this and facilitate information sharing, some States have created information sharing agreements that allow cybersecurity incidents to be shared among signatory parties. These arrangements often enable better information sharing to include lessons learned and best practices, which can inform implementing stronger mitigation measures.

---

[1] In the U.S., air operators are subject to cybersecurity requirements from numerous departments and agencies including Federal Aviation Administration, Transportation Security Administration, Department of Defense, Customs and Border Protection, Security and Exchange Commission, General Services Administration, and Cybersecurity and Infrastructure Security Agency.

[2] In the European Union, air operators are subject to cybersecurity requirements from EASA (Part IS), Member State (Aviation Security) and EU (NIS2).

2.3 Simplifying cybersecurity requirements across States will allow operators to better use their cybersecurity resources for prevention, detection, mitigation, and recovery.

3. OTHER APPROACHES TO SIMPLIFY CYBERSECURITY REQUIREMENTS

3.1 Harmonization of cybersecurity requirements within and among States is an admirable long-term goal, but this requires adoption of similar definitions, standards, and processes. Additionally, harmonization of requirements does not resolve the issue of multiple and often disparate compliance and incident reporting obligations.

3.2 Reciprocity is another approach to simplify cybersecurity requirements. It requires States to develop frameworks to accept each other's requirements or certifications which is generally codified in an agreement. The aviation sector has a history of adopting and using reciprocity agreements to simplify air travel and improve security and safety. However, cybersecurity reciprocity arrangements can be difficult to achieve due to national security considerations.

3.3 Exemptions are another option for States to consider. When an operator is following its own National cybersecurity requirements, exemptions from another State's cybersecurity requirements is a feasible alternative. Exemptions can be explicit (specific State regulations detail an exemption) or implied (State regulations limit scope to National carriers).

4. RECOGNITION ARRANGEMENTS

4.1 Recognition arrangements are frequently leveraged in the aviation and cargo security domains and allow States to recognize and accept another's National Civil Aviation Security Programme requirements. This concept has not migrated into the cybersecurity domain, which leaves operators and entities with a patchwork of disparate regulations and requirements they must now comply with.

4.2 A recognition arrangement may consist of:

4.2.1 States conducting a validation of equivalency between State cybersecurity requirements and oversight. In many cases, States are already issuing substantially similar cybersecurity requirements that are based on accepted standards which simplifies validation. [3]

4.2.2 State recognizes that another State's cybersecurity requirements and oversight are sufficient based on the validation.

4.2.3 If necessary, States codify recognition of equivalency using an appropriate agreement framework.

4.3 Recognizing another State's cybersecurity requirements are equivalent with their own State's requirements which reduces the need for industry to duplicate efforts. It would also enable industry to maximize cybersecurity resources and provide confidence between States that air operators are abiding by ICAO and equivalent national level requirements and oversight. A recognition arrangement can be codified within an agreement, but simply requires States to validate, recognize, and accept another State's cybersecurity requirements and oversight. Recognition can serve as a bridge until a more extensive harmonization effort and/or reciprocity bilateral agreement is established. This approach can ensure sufficiency and help simplify and address an increasingly complex regulatory landscape for cybersecurity.

— END —

[3] Examples include National Institute of Science and Technology (NIST) 800-171 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27001, and ICAO's Annex 17