

**57<sup>TH</sup> CONFERENCE OF  
DIRECTORS GENERAL OF CIVIL AVIATION  
ASIA AND PACIFIC REGIONS**

*Incheon, Republic of Korea,  
4 – 8 July 2022*

**AGENDA ITEM 5: AVIATION SECURITY AND FACILITATION**

**CARGO SECURITY: SECURITY STATUS DIGITALIZATION**

Presented by the International Air Transport Association (IATA)

**SUMMARY**

IATA's vision is to achieve a fully digitally connected and integrated air cargo supply chain. This encompasses the digitalization of all freight, trade and security related paper documents that accompany the consignment. This paper provides the current standing of security status digitalization implementation globally through the survey of electronic Consignment Security Declaration (e-CSD) and invites Forum members to work in partnership with IATA to accelerate security status digitalization.

## **CARGO SECURITY: SECURITY STATUS DIGITALIZATION**

### **1. INTRODUCTION**

1.1 IATA's vision is to achieve a fully digitally connected and integrated air cargo supply chain. This encompasses the digitalization of all freight, trade and security related paper documents that accompany the consignment.

1.2 This paper provides the current standing of security status digitalization implementation globally through the survey of electronic Consignment Security Declaration (e-CSD) and invites Forum members to work in partnership with IATA to accelerate security status digitalization.

1.3 There are various possible methods to submit security status electronically with the existing technology today:

- e-CSD
- Security declaration through pdf format via email
- Mobile application
- API connectivity between regulated agents, airlines and state security system
- IATA ONE Record

### **2. CONSIGNMENT SECURITY DECLARATION (CSD) AND “e-CSD”**

2.1 The Consignment Security Declaration (CSD) and Electronic Consignment Security Declaration (e-CSD) provide regulators with an audit trail of how, when and by whom cargo has been secured along the supply chain. In both cases, the objective is to meet ICAO requirements (Annex 17 Standards 4.6.5 and 4.6.8), ensuring that each consignment received by an aircraft operator has been confirmed or accounted for by a regulated agent, a known consignor or an entity that is approved by an appropriate authority and that a security status has been issued, either in an electronic format or in writing. Each consignment comes with different types and formats of documentation, either on the e-Air Waybill or on a separate declaration, and to avoid a plethora of different security declarations, IATA developed a standard CSD in cooperation with the industry and regulators and ICAO security working groups.

2.2 In November 2015, the IATA e-CSD/CSD Resolution 651 entered into force. It offers industry stakeholders and IATA carriers a universal standard, that provides consignment information in accordance with the requirements of ICAO Security Manual Doc. 8973 and the Commission Implementing Regulation (EU) 1998/20. Following the phasing out of the Account Consignor status by ICAO in June 2021, a revised version of the IATA Resolution 651 has been approved with an applicability date of July 2022 and IATA is working with the relevant ICAO Working Groups for updating the Security Manual accordingly.

2.3 The Consignment Security Declaration (CSD) or its electronic format (e-CSD) contain information according to the requirements of the appropriate regulation is shown in Attachment A.

2.4 Electronic Consignment Security Declaration (e-CSD) can be provided by means of IATA Cargo-IMP messages, IATA Cargo-XML and IATA ONE Record messages. e-CSD eliminates the use of the paper security status declaration by employing existing technology and infrastructure and only requires security information to be inserted into FWB OCI column.

### 3. **ELECTRONIC SECURITY STATUS DECLARATION BENEFITS**

3.1 The industry will benefit greatly through the digitalization of all form of security status. Key benefits of electronic security status include:

- Perform advance and remote safety and security risk assessments on each consignment before its physical arrival at departing, transfer and arrival facilities
- Enable use of new technology to share security declaration data elements among key stakeholders to ensure timely and accurate security declaration submission throughout the secure supply chain
- Support total digitalization of cargo supply chain, allowing industry to bring in more innovations to improve cargo operation efficiency.
- Respond faster to regulatory bodies when regulator requests confirmation that the cargo has been secured
- Promote environment sustainability through elimination of paper usage

### 4. **STATUS OF SECURITY STATUS DIGITALIZATION**

4.1 IATA conducted a survey<sup>1</sup> in April 2022 to identify the acceptance of e-CSD globally. The survey provides an analogous standing of security status digitalization globally. Out of 197 States approached, 150 (76%) states replied that they implement or accept CSD which is an encouraging result. Out of the 150 replies, 58 (39%) accept electronic version and 92 (61%) continue to mandate the use of paper security status declaration according to our understanding of the answers.

4.2 These results (at least 76% compliance with the issuance of security status) are notably higher than the ones shared by the ICAO Universal Security Audit Programme – Continuous Monitoring Approach (USAP-CMA) in its last Analysis of Audit Results (10<sup>th</sup> Edition -2020). In the USAP-CMA table 3.4 titled “Indicative compliance with Annex 17 Standards”, the indicative implementation of Standard 4.6.8 (issuance of a security status) was at 45% globally (40% in the Asia Pacific region).

4.3 These results raise questions about the apparent reluctance or inability of some appropriate authorities to accept the electronic format of the security status as all security declarations are created electronically (software, web platforms), even if their printouts are used for administrative compliance. It would be useful to gather and analyze the operational reasons that create such situations and develop solutions for improving processes for all stakeholders and regulators.

### 5. **ACTION BY THE CONFERENCE**

5.1 The Forum is invited to:

- a) Explore ways Forum members can accelerate the acceptance of electronic security status declaration such as e-CSD
- b) Explore the possibility of integrating other formats and solutions for the transmission of digital security declaration status.
- c) Work with IATA on the above with a report of the results during the next session.

-----

---

#### Notes

1. IATA e-CSD Survey –

<https://www.iata.org/contentassets/538b4a1ea4e74990842cf2a752e1d2aa/iata-e-csd-acceptance-may-2022.pdf>

**APPENDIX A**

The Consignment Security Declaration in paper (CSD) or electronic format (e-CSD) may contain part or all the following information according to the requirements of the appropriate regulation:

- unique identification number of the Regulated Agent (RA)/ Known Consignors (KC) or other Authorized Entities (AE) issuing the Security Status
- unique means of reference, such as the air waybill number or house waybill number
- content of the consignment and/or indication of consolidation, if applicable
- origin of the consignment
- destination of the consignment
- transfer or Transit point of the consignment (if known)
- the Security Status of the consignment, stating whether it is secure for:
  - passenger, all-Cargo and all-Mail aircraft (SPX) or
  - passenger, all-Cargo and all-Mail aircraft, in accordance with High-Risk requirements (SHR)
- the reason the Security Status was issued, indicating whether the consignment is:
  - received from an approved RA/KC/AE
  - screened using appropriate Screening methods (methods as defined by ICAO) or
  - exempted from Screening (grounds for exemption as defined by ICAO)
- the unique identification number of any RA/KC/AE accepting the Security status and stating that the consignment has been kept secure and not tampered with while in custody.
- the name or unique identification number of a RA/KC/AE staff member with the proper training and authority to issue the declaration.
- the date and time when the security declaration was issued, if requested by regulation.
- any additional Security information or emergency amendment that may be required by the appropriate authority.

— END —