Electronic Consignment Security Declaration (e-CSD)

1. The Consignment Security Declaration (CSD) is a printed form in a standard format which provides security information relating to consignments of air cargo and mail as they move along the supply chain. This enables entities handling cargo and mail to ensure that the proper level of security is maintained or applied and provides an auditable trail for regulators.

2. In 2010, IATA, working closely with other stakeholders, developed an electronic version of the CSD, the e-CSD, similarly intended to provide a common international standard for cargo and mail shipments. This was adopted by IATA Resolution 651 in March 2015.

3. The layout for the electronic template was based on that of the paper CSD and requires the following data to be entered:
   
   • the entity responsible for securing the cargo and maintaining its integrity until loading onto the aircraft (e.g. unique identification of a regulated agent);
   
   • the content of the consignment such as the unique consignment identification, the cargo description and security status. e.g. secured for all aircraft (SPX) or secured to high risk standards (SHR);
   
   • the reason why the security status was issued (e.g. known cargo coming from a known consignor);
   
   • details of any screening applied (e.g. x-ray equipment);
   
   • the name of the person who issued the security status, or an equivalent individual identification;
   
   • the date and time when the security status was issued; and
   
   • any country specific requirements with which secure operators have to comply.

4. Like the CSD, the e-CSD can be used in conjunction with a house or master air waybill for direct and indirect (consolidation) shipments by all regulated agents and airlines. It can be used in all States which have a recognized cargo security program in place and/or accept the use of an e-CSD as a means of complying with the provisions of ICAO’s Annex 17.
E-CSD example

CSD example
1. The Known Consignor (KC) applies security measures to the consignment before it is tendered to the Freight Forwarder/Regulated Agent (RA).

2. The Freight Forwarder/RA receives the secured and protected cargo, assigns the appropriate security status and transmits the e-CSD to the Aircraft Operator (AO) or Ground Handling Agent (GHA) RA acting on behalf of the AO.

3. GHA RA or AO will acknowledge receipt of the security status, accepting it from the previous party and transmitting the e-CSD to the transfer or destination airport.

4. For the audit trail, any RA or AO should demonstrate that the security of the cargo has been maintained and the secure supply chain has not been broken.

5. The e-CSD requires that security information be transmitted electronically, consistent with the industry's e-AWB/ e-cargo proposition. In the event that a regulator demands a paper security declaration, operators can produce it from the electronic records.

**E-CSD benefits**

1. *Avoids unnecessary duplication of screening*: this is possible only if the consignment is protected against unauthorized access along the supply chain and the e-CSD is transmitted along the line to prove that the chain of custody has not been broken.

2. *Facilitates prompt and standardized responses for regulatory bodies*: the e-CSD provides a means of meeting legal requirements and a mechanism for tracing targeted cargo very rapidly (a couple of minutes or less).

3. *Increases productivity*: shipments can be processed faster ensuring loading is as scheduled and further avoiding unnecessary screening at transfer points.

NB The integration of a full data content of a RA and KC database into the IT infrastructure of the RA/AO will allow an automated mapping of valid RA and KC accreditations against the incoming e-CSD messages, significantly reducing processing times.
E-CSD challenges

**IT systems**

1. Lack of compatibility between IT systems can result in the information not being transmitted correctly on entirely. (This most commonly occurs when data is being transferred from Cargo-IMP systems to XML.)

2. Lack of connectivity, meaning that data cannot be transmitted/received because the sending or receiving network is not live.

**Data Quality**

3. Inaccurate or incomplete data: the e-CSD allow shipment to be submitted faster, but depends on good quality data being entered with no missing elements.

**Regulations**

4. Lack of harmonization in the regulations and delays in implementation may impede the e-CSD process.

**International implementation tools:**

- ICAO Doc 8973 (Restricted) - Chapter 13 – Appendix 33 Security Declaration and completion instructions.

- IATA e-CSD Functional Specifications which define the e-CSD business process and provide guidance to secure operators to comply with the e-CSD standards.

- IATA e-CSD operational procedures together with the most common “10 e-CSD scenarios” provide guidance as to how to move cargo with its associated information through the secure supply chain – from one Regulated Agent to the next. These procedures complete the Functional Specifications mentioned in previous bullet point. They also provide a detailed guideline on the steps that stakeholders should follow to secure cargo, issue the security status declaration, and pass this security declaration to the next stakeholder while preserving cargo integrity; and

- IATA’s Other Customs, Security and Regulatory Control Information (OCI) Composition Rule Table is a technical tool to guide business experts and message providers in the development of the Customs and security solutions.