



## ADVANCE CARGO DATA AND RISK MANAGEMENT

### An information paper by the Global Express Association<sup>1</sup>

This paper addresses the different types of cargo information transmitted to border authorities during the importation process. It aims to dispel any misconceptions about the timing and purpose of such transmissions. If properly designed, these transmissions - and the targeting tools that analyse the data - **facilitate the flow of legitimate trade** while helping to enhance security and to detect and stop fraud and illicit trade. Yet, border authorities regularly ask for additional data without first establishing whether it is available or fit for purpose. This can lead to disruptions in legitimate trade flows without necessarily improving the authorities' revenue collection and detection capabilities – especially where security risks are involved.

\* \* \*

The three members of the Global Express Associations (DHL Express, FedEx Express and UPS) provide sophisticated logistics services to carry goods and documents across the globe. They operate in 220 countries and territories. Typical delivery times range from overnight (in some cities, same day) to up to 72 hours after pick up, depending on the type of service contracted and the distance. They serve a range of industries that depend on time-sensitive deliveries for their value chains. They also convey an ever-increasing volume of e-commerce shipments and meet this dynamic sector's ever changing demands and needs.

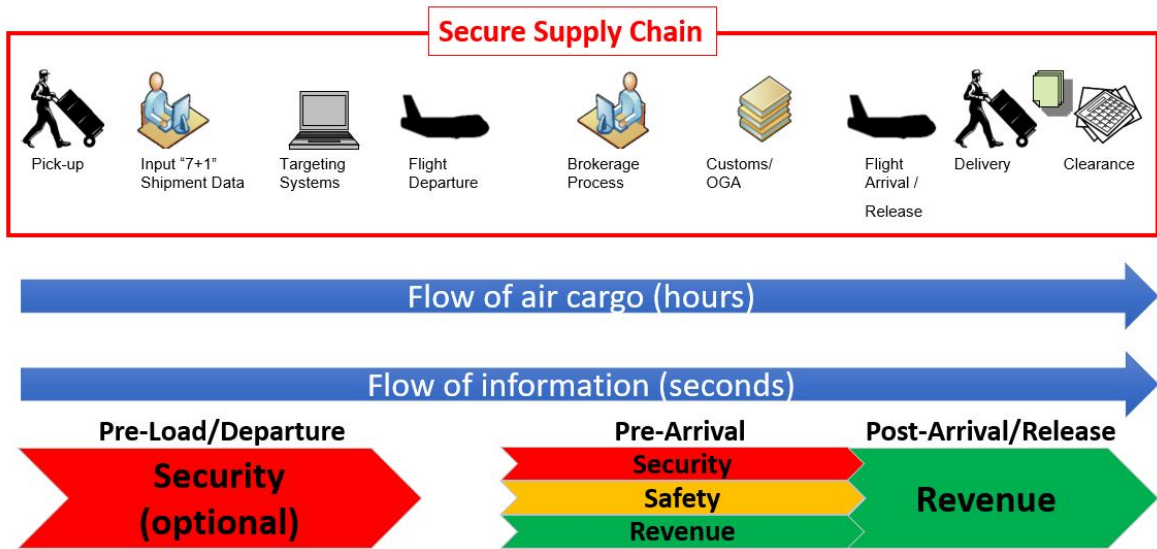
In order to make this possible, GEA members rely on their compliance commitments, their secure supply chains and their ability to convey advance electronic information on every shipment to border authorities so they can assess the risk associated with each of them. This facilitates the movement of shipments throughout the entire supply chain, including the importation process.

Express delivery carriers convey advance electronic information to border authorities at different stages during the shipment's transit through their supply chain and **for three clearly mandated, defined and different risk assessment purposes, namely security, safety and revenue**, which we explain in this paper. In turn, different government authorities receive and process it, also at various stages in the process.

---

<sup>1</sup> The Global Express Association represents the three leading express delivery carriers DHL Express, FedEx Express and UPS. More information is available at [www.global-express.org](http://www.global-express.org)

## Risk Management – different times for different purposes



For *air cargo security* purposes, some data is provided as early as the information is available to the express operator. At the latest, it is transmitted *before a shipment is loaded* on an aircraft at the last point of departure to the destination country.

Information related to *safety and revenue* is provided *before the shipment arrives* at the destination country's border, ideally where possible in a single transmission. This allows border authorities to perform 'pre-arrival processing' under Art. 7.1 of the World Trade Organisation's Trade Facilitation Agreement (TFA), that is, to determine the admissibility of a shipment before it is in the authority's territory for customs and related purposes.

Lastly, in many countries, additional revenue-related data can be provided *after the arrival of the shipment* -- for final clearance purposes. Technically, this is no longer 'advance information' but information that supports the segregation of two customs processes, release and clearance, as recognised under Art. 7.3 of the TFA. The goods are thus released, formalities completed, and duties and taxes can be secured and collected later. Data for national statistics purposes can also be sent post-arrival.

Each transmission serves a specific purpose, i.e. security or safety or revenue related, and each contains different kinds and levels of quality of data, for a reason.



## **PRE-LOADING**

**Pre-loading' advance cargo information (PLACI) is submitted as soon as it becomes available in order to mitigate potential risks to aviation security.**

Since 2010, border authorities in a few countries have considered requesting pre-loading advance electronic information to detect or to identify the possibility or risk of an improvised explosive or incendiary device ('a bomb in a box') before it is loaded on an airplane.

The USA started testing this through its ACAS pilot, which has since become a permanent programme. The UK has recently started its own PREDICT pilot and the EU intends to start its programme by 2021. International standards clearly indicate that these are *optional, additional* layers of security. Not all countries are encouraged to develop such programmes. It is up to each country to make a decision depending on its own threat and risk analysis, meaning how exposed they are to terrorism threats in the cargo and mail channels.

The US ACAS pilot has allowed regulators and industry to test data in order to determine what is available, when, and whether it is fit for purpose. As a result, the data fields to be transmitted for this purpose have been codified in an international standard – the World Customs Organisation's SAFE Framework of Standards. They are known as the **PLACI '7+1' data**.

Annex III of the WCO SAFE Framework of Standards calls for the transmission of a shipment identifier plus the following seven data fields:

- Consignor, name
- Consignor, address
- Consignee, name
- Consignee, address
- Number of packages
- Total gross weight
- Brief cargo description (so called 'raw' description as provided by the shipper/sender).

The rationale for sending these 7+1 data fields (and not any other ones) is twofold. First, they are available very early in the process, whereas other data fields are only available later on. Secondly, intelligence experts have tested these data fields through the ACAS pilot in the USA and determined that that they were fit for purpose. In other words, these '7+1' data, when contrasted with available intelligence, proved sufficient to determine the presence of an aviation security risk.

The '7+1' data are submitted by the express operator exactly as provided by the shipper, (so-called 'raw data'). Security authorities, including Customs, see value in the fact that the data is not altered or processed as they would be when provided for Customs clearance purposes. Raw data can provide intelligence traces or patterns that can support specially trained analysts in their assessment of a potential security risk, and a security risk alone. For these reasons, '7+1' data are

not fit for traditional Customs risk assessment and clearance purposes. (Again, not all countries are encouraged to develop such programmes.)

Aviation security risks must be mitigated before a flight departs. This is done by applying various layers of security.

Under the Chicago Convention on International Civil Aviation, all outbound cargo must be subjected to security controls, which are defined in Annex 17 to this international treaty. The submission of pre-loading data for security risk assessment is as an *optional, additional layer* of security. It has been developed jointly by the international bodies governing air cargo security (ICAO) and customs (WCO). Governments choose whether to apply this additional layer depending on their own threat and risk assessment. To satisfy the accuracy of the PLACI '7+1' data and to verify the screening status of a shipment, "requests for information (RFI)" and "requests for screening (RFS)" can be issued by the government to the air carrier or the person filing as the case may be<sup>2</sup>.

In the event of an imminent threat to aviation being detected, the authorities will initiate so-called Do Not Load (DNL) protocols, including a DNL message to the air carrier. The DNL protocol would trigger an immediate emergency response in order to deal with the threat (a 'bomb in a box'). The consequences of a DNL cannot be underestimated. It would mean closing an airport – with all traffic in and out of that airport being stopped for several hours. The airport may also need to be evacuated completely.

It is for this reason and the significant economic consequences of a "false positive" DNL that these protocols must not be used for any purpose other than aviation security.

Other risks, such as revenue, drugs, firearms, illicit trade, intellectual property right violations, etc can be mitigated effectively prior to or on arrival. They do not require immediate responses at the time of flight departure. Trying to use PLACI referral protocols, including Do Not Load, to detect and mitigate non-security risks is unnecessary. Most importantly, it can distract targeting officers from detecting true security risks and lead to complacency amongst all involved in managing the execution of a DNL.

Data other than the '7+1' data should not be required for security assessment purposes. Adding data fields that usually support revenue and safety risks (such as the HS code, country of origin, customs value or whether any of the parties are private citizens or a corporation) will have the same unintended consequences.

In short, pre-loading advance information protocols should be used for the purpose they were designed for: detecting a 'bomb in a box'.

---

<sup>2</sup> For further information please refer to the ICAO/WCO Joint Guiding Principles for Pre-Loading Advance Cargo Information (PLACI).



## **PRE-ARRIVAL**

### **'Pre-Arrival' electronic data is sent later in the process to facilitate release.**

Pre-Arrival information has been in place in many countries for over 10 years. Since its adoption in 1999, the Revised Kyoto Convention – an international treaty that harmonises customs procedures – has promoted the concept of pre-arrival data submission for risk assessment purposes in order to facilitate the immediate release of goods on arrival. In 2005, another international protocol, the World Customs Organisation's SAFE Framework of Standards, introduced pre-arrival data submission focusing on safety risks. For long-haul flights the data is submitted 4 hours prior to arrival; for short-haul flights, at the time of wheels-up.

Either as part of the customs clearance process or as part of the pre-arrival risk assessment, GEA members send electronic cargo information in advance to border authorities at destination countries. In many cases, this data is also sent to countries through which they may transit.

Unlike PLACI data, pre-arrival data is no longer 'raw', and may contain much more information than the data requirements defined in the '7+1' data, (movement-related data, simple HS code, goods description, country of origin, etc.) It has been processed by in-house customs specialists, or even our own customs clearing agents, and is specifically prepared to meet regulatory entry requirements and expedite the shipment's release. In some cases, collecting this information requires additional contacts with customers, which takes more time.

Using this information, border authorities can assess whether the goods present a risk (for instance, undervaluation or any type of illicit trade) before the goods arrive in their territory. If the analysis shows the likely presence of such a risk, the shipment can be selected on arrival for documentary or physical inspection.

If, however, the analysis shows that the shipment is of low risk, it can be cleared and released immediately on arrival (in the most advanced economies, customs duties and taxes can be paid later based on supplementary information provided after the release of the goods). This is a tremendous facilitative measure which allows customs to focus their limited resources on those shipments that pose a risk whilst avoiding unnecessary delays and the associated costs to legitimate trade.

Standard 3.12 of the Revised Kyoto Convention and Art. 10.1 of the Trade Facilitation Agreement state clearly that authorities must restrict their interventions, including data collection and goods inspection at import, to those only necessary to support proper risk-based customs controls.

Whilst pre-arrival data sets contain much more information than a pre-loading transmission, it is important to make sure that each specific data field serves a risk-assessment purpose, and that the receiving authorities are in a position to process them efficiently.

## **POST-ARRIVAL**

### **Post-arrival information completes clearance**

Art. 7.3 of the Trade Facilitation Agreement and Standards 3.13 and 3.14 of the Revised Kyoto Convention provide for the possibility of separating the release of a shipment by Customs from the final determination of the duties and taxes due for said shipment.

In practice, this means that an incomplete or simplified declaration is submitted prior to arrival of the goods in order to have the goods released (which some countries call *prior release* or *conditional release*). Supplementary information required to support foreign trade statistics and the final determination and collection of duties and taxes is provided later on, often 7 to 10 days after release (and as legislated or otherwise agreed with the relevant regulatory authority) or on a monthly or bi-monthly basis for trusted operators.

Determining the shipment's customs value often requires more time and additional information from either the shipper or the consignee. Allowing for the submission of additional information or updating already submitted data after the release of the goods facilitates this process and helps manage compliance and meeting the importer's fiscal obligations.

The separation of release from clearance is secured by a financial guarantee (such as a customs bond) to ensure that the government's financial and fiscal interests are protected.

In addition, a post-clearance audit process provides additional control capabilities for Customs to satisfy its revenue and compliance concerns.

The time between release and clearance can also be used for sampling and testing in case authorities have to take samples for safety or revenue purposes.

The compliance level of the operator – for instance, where it holds authorized economic operator (AEO) status - should determine, too, the level of simplification it benefits from, including the amount of guarantee to be provided (if not waived altogether). This would provide the operator with an economic incentive to keep a high compliance level, as it would make it more competitive.

## Summary & Recommendations

Advance cargo information can serve a multitude of purposes:

- facilitation of legitimate trade, and
- the detection of various types of risks and threats.

It is important that all border agencies coordinate their risk assessment activities and design their risk assessment specifically according to threat. That means that *data requirements and timings of transmission should be limited to the specific need*.

Defining the necessary data -and data quality- must depend on the purpose of the data submission and the associated risk assessment. In other words, data provided for aviation security risk assessment prior to loading must meet data quality requirements for this very purpose, and for this purpose only.

Safety risk assessments require more time, more data (of a different type and quality), and are ideally dealt with prior to arrival.

For revenue and other government purposes such as foreign trade statistics, pre-arrival data might be used. Where a financial guarantee is provided, it should be possible to submit or update data after the release of the goods.

Mixing up these processes would not only blur the lines and make them less efficient, but would lead to unintended consequences, such as unnecessarily slowing down the flow of legitimate trade.

Geneva, January 2020