PHASE I REPORT OF THE INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)–WORLD CUSTOMS ORGANIZATION (WCO) JOINT WORKING GROUP ON ADVANCE AIR CARGO INFORMATION (JWGACI)

Contents

Purpose

1. The purpose of this document is to report on the objectives and requirements for the use of Advance Cargo Information (ACI)[1] in the civil aviation security context as assessed by the JWGACI in accordance with its ToR (Annex A) and to obtain the endorsement of the AVSEC Panel and the Technical Experts' Group on Air Cargo Security (TEGACS).
2. As the requirements of civil aviation in respect of ACI relate entirely to data available before loading, this report will generally refer to Pre Loading ACI (PLACI) rather than to the ACI data required, often pre-arrival, by Customs and other agencies for wider risk assessment purposes.
3. Unless otherwise specified, references to cargo in this report should be understood as referring to both cargo and mail.

Outcome of JWGACI meetings

4. The JWGACI has met twice to date, in Singapore (August 2014) and Geneva (December 2014), and has considered:

   - existing regulatory frameworks for the current and possible future use of ACI (WCO's SAFE Framework of Standards and ICAO's Annex 17 to the Chicago Convention;
   - existing aviation security risk mitigation measures;
   - current PLACI pilots for aviation security as well as the set of joint principles developed by Canada, the European Union (EU) and the United States (US), on the timelines, data elements, filing options, risk mitigation measures etc. for PLACI;
   - Universal Postal Union's (UPU) Advance Electronic Information (AEI) model for providing postal data at global level;
   - the views of industry and regulators on using PLACI for aviation security purposes;
   - the need to assess the impact of the implementation of PLACI systems by multiple States on transfer processes and multi-leg shipments;
   - differences between air cargo and postal[2] documentation; and

[1] 'Advance Cargo Information' (ACI) is an approach where a data set providing information about an international movement of cargo is used for conducting risk assessments to address a range of threats, including safety and security.

[2] In particular, postal shipments will not be accompanied by a HAWB and MAWB, but do have a unique identifier which can be used in the same way as a HAWB or MAWB to identify a shipment.

- draft principles and model for the use of PLACI in aviation security submitted by Singapore for consideration during Phase 2[3].

5. Customs authorities have been using ACI, based on the provisions set out in the WCO's SAFE Framework of Standards,[4] for a number of years as an essential tool in the process of targeting shipments[5] for security and other purposes. For aviation security, the focus is the 'bomb in the box' threat, for which only PLACI is relevant. It is on this that the JWGACI has focussed.

6. The possible use of PLACI as part of AVSEC's multi-layered air cargo security risk based approach was given added impetus in the wake of the October 2010 incidents involving improvised explosive devices (IEDs) concealed in computer printers. It was considered in addition to other ICAO measures for strengthening the security of the air cargo supply chain, as mandated through Amendments 13 and 14 to Annex 17 of the Chicago Convention, which became applicable in July 2013 and November 2014, respectively. Determining how electronic PLACI can be used to support risk management in air cargo security was also included as one of the areas on which ICAO and WCO were committed to working together by their respective Secretaries-General[6].

7. Canada, the EU and US launched the pilot projects to establish how such a system might work in practice. These involved different business models but had similar results. It was generally recognised that, for States wishing to adopt PLACI as part of their regulatory framework, there was a need to adopt a common approach and principles, in the interests of avoiding duplication and/or conflicting requirements that could add to costs or result in operational challenges for industry.

8. Industry representatives voiced support for the use of PLACI for air cargo security purposes. They also emphasised the need for global standards for data submission elements, timelines, formats and communication and security mitigation protocols to be vital to operability. There should be sufficient flexibility to accommodate diverse business models and the use of PLACI should be optional, as not all States would have the capacity to implement it.

9. The JWGACI noted the following challenges common to the pilot projects:

   - ensuring data quality in terms of accuracy and adequacy;

   - maintaining operational feasibility, by keeping the number of requests for extra data at a manageable level[7];

   - establishing clear lines of communication, properly targeting requests for information and providing prompt responses;

[3] Initial discussions around these draft principles included the issue of whether cargo could still be loaded on board an aircraft even when concerns have been raised in relation to PLACI, but not yet resolved. This could include missing data.
[4] http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/safe_package.aspx
[5] It has to be noted that this kind of advance electronic cargo information is usually submitted prior to arrival by air, road and rail and prior to loading for containerised maritime cargo.
[6] Joint Communiqué of the ICAO-WCO Joint Conference on Enhancing Air Cargo Security and Facilitation, 6 July 2012, Singapore, sub-paragraph xii on page 3.
[7] However, such requests would be limited if all required data elements were provided promptly.

- resource implications for States implementing ACI and/or responding to referrals, as well as capacity development;

- communicating relevant information on alerts to governmental bodies; and

- how to take into account existing measures designed to secure the supply chain.

10. The group noted that the three pilot projects and WCO's SAFE Framework of Standards review proposal identified the '7 + 1' initial data set for beginning the risk assessment process for air cargo security (name of consignor, address of consignor, name of consignee, address of consignee, number of pieces in the consignment, description of contents, weight, plus the house and/or master air waybill number[8]). This data, when subjected to a risk analysis process against a profile established by Customs and aviation authorities, is considered useful for conducting risk assessment and in the management of risk.

11. Over the course of the pilot activities, it has been demonstrated that the 7 + 1 data elements were usually available early[9] in the supply chain and before a consignment was loaded on to an aircraft. When the data provided was incomplete or insufficiently precise, additional information was requested. The industry stressed the importance of ensuring that unnecessary delays are prevented and also expressed concerns that regional variations on the data set required might lead to problems in interoperability.

12. It was noted that there were broad similarities between the potential use of PLACI and the use of Advance Passenger Information and Passenger Name Record systems in respect of aviation security.

13. Some terms are defined or used differently in Annex 17 to the Chicago Convention as compared to the WCO SAFE Framework of Standards. The most significant are shown at Annex B. The JWGACI Members decided that this could probably be dealt with by adopting cross references, but that amendments could be considered later if difficulties arose.

14. The most effective approach to aviation security is multilayered, as terrorist and criminal networks evolve in response to the controls put in place by governments and industry and it will always be necessary to adjust and vary security measures in order to maintain, and where possible raise, levels of effectiveness. Pre-loading ACI represents a tool that can help to differentiate high-risk shipments from the rest so that resources can be targeted with maximum efficiency.[10]

15. Although the WCO's SAFE Framework of Standards is not mandatory, 94% of WCO Members have signalled their support and are already in the process of implementing it. The synergies between the content and purpose of Customs' and AVSEC rules, and the evidence of the pilots, indicate that AVSEC needs can be accommodated within existing Customs' platforms and security mechanisms. This would lead to

[8] For postal shipments, see footnote 2.
[9] It should however be noted that due to factors like geography or supply chain characteristics the information may be available only shortly before loading.
[10] The 7 + 1 elements do not directly correspond to the ICAO definition of high-risk cargo. The ICAO definition requires that the shipment come from an unknown entity or that it show signs of having been tampered with in addition to other risk factors, unless there is specific related intelligence.

economies in time and equipment, and bring together the two main global sets of regulations governing cargo movements. Industry would therefore benefit from the elimination, or avoidance, of duplicate requirements.

16. Electronic exchanges are increasingly common as a business tool. They are already widely used by the aviation industry to transmit data on passengers and air cargo. Operational trials using PLACI are being conducted in the Canada, EU and US, with a move towards legislation. The Universal Postal Convention has been amended to allow the requirement of ACI in respect of mail (Article 9). While it is clear that electronic systems cannot be counted on at all times and in all places, and there must always be provision for alternatives, there are strong arguments to suppose that they can contribute positively to both security and facilitation.
17. It is important to note that the benefits could be lost if the different schemes and approaches currently being trialled are not sufficiently harmonised and interoperable. ICAO, WCO, UPU and their members and industry partners should therefore continue to work closely together to optimise the potential gains from PLACI.

Summary of expected benefits

18. In summary, the possible benefits of adopting a PLACI system were seen as follows:

- Additional layer of security, increasing effectiveness of a multilayered system and risk-based approach;
- Focus on and easier identification of high-risk shipments
- Avoidance of unnecessary delays for low-risk air cargo shipments
- Meeting the needs of Customs and aviation security through a single, joint process, avoiding duplication
- Flexibility to adapt to diverse supply chain models providing comparable outcomes
- Facilitation of movements of cargo throughout global supply chains, which are complex, cross-border, and multi-modal

Reports from the pilot projects

19. The three PLACI pilot projects being conducted by Canada, the US and the EU have much common ground. All three utilise the 7 + 1 data set as a baseline, and in addition take into account AVSEC screening results when appropriate. All three report that 7+ 1 data is generally available prior to loading and provides a sufficient basis for conduct a first layer of security risk analysis**. (**Data was provided to regulatory authorities by express couriers, postal operators, air carriers and freight forwarders according to the different business models.)

20. The data is usually transmitted electronically (i.e. using a standard message format and a system that can accept these messages) and an electronic system is widely seen as a pre-requisite for future implementation. Once received, the data is risk assessed by Customs and aviation security authorities on the basis of security risk rules. In addition, intelligence and historical data, previous incidents and the perceived threat to aviation are considered as part of the risk profile. The risk assessment process may result in no further action, a request for further information and/or additional screening or, in cases of imminent aviation security threat, a Do Not Load (DNL) message.

21. The provision of the data and the communication of the resulting risk assessment were provided as early as possible. This practice minimised the potential disruption to legitimate trade. The three pilots concluded that the PLACI assessments provided an additional layer of security.

22. The most significant challenges identified by the pilots are:

    - establishing adequate IT systems;
    - ensuring that the data is of sufficient quality;
    - overcoming challenges associated with sharing intelligence and information; and
    - allowing for different business models including multi stop routes and multi modal shipments.

23. A comparatory matrix and full details of the three pilot projects can be found in Annex C. A set of joint principles was also developed by the pilot entities. This is included at Annex D.

24. Trials have also been conducted in respect of postal operations. The advance electronic information (AEI) postal model is a collective work that has been developed and discussed since early 2013. This model has been presented and modified through working groups such as the UPU Customs, Postal Security and Transport Groups, WGACS, TEGACS, IATA/UPU Contact Committee, WCO/UPU Contact Committee and in consultation with IATA.

25. The EU postal pilot confirmed the use of electronic CN23 data and relevant UPU messaging standards. The postal model is based on existing processes and EDI messages that have been agreed to by posts, airlines and customs. These messages include ITMATT, PREDES, CUSRSP, CUSITM, and CARDIT. Postal

items are recognised by the use of a unique identifier standardised by the UPU. The UPU has also developed a Customs Declaration System (CDS) which, associated with the IPS (International postal system), assist its members in meeting the requirements of AEI, which also uses these messages in its flow. A diagrammatical representation of the AEI postal model is as per Annex E, Fig. 1.

Note: The air cargo industry has many business models. The flow charts in Annex E (Figs. 2 and 3) also set out the basic operating processes for the two primary non-postal models, express and general cargo.

Recommendations

The JWGACI recommends:

1. **That the AVSEC panel and TEGACS endorse the concept of PLACI as an additional layer in the management of air cargo security risk and the continuing work of the JWGACI into Phase 2.**

2. **That during Phase 2, the JWGACI develop a model for the use of PLACI, for States which wish to adopt such a system.**

3. **That in developing this model, the JWGACI will take into account the preliminary draft Proposed Principles and Model for Pre-loading Advance Cargo Information attached as Annex F.**

4. **That where PLACI is adopted, there should be a harmonised global approach with avoidance of duplication.**

ANNEX A – TERMS OF REFERENCE

ICAO-WCO Joint Working Group On Advance Cargo Information

I. Scope of the Work

1. The Joint Working Group will progress in two distinct phases. The first phase will assess the needs and determine the objectives of the use of Advance Cargo Information (ACI) in a civil aviation security context, while the second phase will focus on the practical and technical ways to implement the use of ACI, as per the outcomes of Phase 1.

II. Phase One: Assessment

2. The working group will:
   - in the light of ongoing Customs pilots on advance information and discussions/reports of WCO Technical Experts Group on Air Cargo Security (TEGACS) and ICAO Aviation Security Panel Working Group on Air Cargo Security (WGACS) meetings, identify and assess the mutual benefits and challenges with regard to the use of ACI in a civil aviation security context;
   - determine to which purpose and in which context ACI would be useful in a civil aviation security context;
   - assess the economic and operational impact (to both industry and governments) of the use of ACI in a civil aviation context; and
   - consider the impact of not using ACI in an aviation security context.

   Allocated time: six to eight months

3. Deliverables: a written report will be produced, including summary information on:
   - overview of pilots;
   - operational functioning of pilots (data elements, time limits for data submission, as well as response times);
   - key similarities and differences between pilots;
   - benefits and challenges identified for aviation security, Customs, airlines, and other supply chain entities;
   - identified applications for civil aviation security and proposed use and processes;

- identified prerequisites and conditions for the efficient and operational use of ACI in a civil aviation security context (operational and technical conditions, constraints and impacts, time limits, response time, etc.);

- determined respective roles and responsibilities of Customs and aviation security in the context of the use of ACI in a civil aviation security context; and

- determined expected outcomes and deliverables of Phase II.

III. Phase Two: Concept of Operations

4. In light of outcomes of the first phase and ongoing developments, the working group will:

   - consider how and whether ACI could complement existing or future civil aviation security tools;

   - determine the technical and practical ways to implement and administrate the use of ACI in a civil aviation security context;

   - determine how Customs and civil aviation authorities might be able to support each other with regard to the use of ACI, aiming to improve air cargo security; and

   - determine whether and how outbound (Customs/civil aviation) and inbound (Customs/civil aviation) authorities can communicate and make determinations jointly or in support of each other.

   Allocated time: to be determined at the end of Phase I.

   Deliverable: development of a more detailed concept of operations. Detailed deliverables will be determined at the end of phase one.

IV. Rationale

5. As part of their cooperative efforts, ICAO and WCO will evaluate possible enhancement of synergies between their instruments, tools, and programmes. For instance, risk assessment decisions made on the basis of early supply chain information may enhance security without impeding trade or facilitation.

6. One of the objectives is to harmonize tools, including existing ones, so as to enhance efficiencies within the secure supply chain and to consider the need for standardised data, joint risk criteria/mitigation through risk management, intelligence, and threat information sharing.

7. The potential use of ACI, by Customs and civil aviation authorities jointly, for the identification of high-risk cargo, is to be assessed by the group.

V. Detailed elements to be analyzed and treated for the purpose of the Working Group objectives (non-exhaustive):

a) presentation and analysis of the outcomes of ongoing trials on advance cargo information, including current level of implementation and results;

b) data elements collected:

- minimum key data elements derived from the ongoing pilots/study to be considered and discussed for possible risk assessment within an aviation security context;
- when, where, how, and between whom these data elements are collected and shared; and
- potential impact data elements to be collected may have on industry IT systems and costs (messages transmission, re-programming of systems, training, other);

c) overview of the risk assessment process:

- who carries out the assessment, when, and where; and
- process and implications of different risk analysis and judgments;

d) advantages and challenges;

e) regulatory requirements including impacts on other existing regulations;

f) administrative requirements;

g) technical requirements:

- how is the information provided from the air cargo supply chain?;
- how is the information shared? Customs traditionally uses electronic methods, often real time, whose practicality needs to be assessed for aviation security purposes; and
- in the aviation security environment, the carrier or the regulated agents generally carry out the security operations and take the final decision on the security status of cargo. Customs might need to share the ACI with them directly, or through the national aviation security authorities;

h) personnel requirements:

- resources available;
- training; and
- operational requirements; and

i) oversight mechanisms

VI. Team Members

- Co-Chairpersons;

- 8 representatives of WCO Members (including regional representatives and members undertaking pilots/study);
- 8 representatives of ICAO Members;
- ICAO and WCO Secretariats;
- 6 representatives of relevant stakeholders.
- A meeting/consultation of State members only may be organized if/when needed.
- The composition of the working group is to be coordinated jointly by the ICAO and WCO Secretariats.

VII. Working Mode

- Conference calls will be held at regular intervals;
- Mailing list of the participants will be used for discussions and sharing of documents;
- http://wco.webex.com will be activated for arranging teleconferences;
- ICAO and WCO Secretariats will maintain meeting/discussion notes;
- brief summary of the discussions will be provided to the TEGACS and the WGACS;
- ICAO and WCO Secretariats will have joint consultations as often as needed, including for the preparation of the agenda and working papers; and
- on an exceptional basis, physical meetings will be held when needed.

VIII. Decision Making Process

- Discussion summaries and potential results or conclusions will be presented to the TEGACS for further discussions and possible endorsements where relevant; and
- The working group will also report to the ICAO Aviation Security (AVSEC) Panel through the WGACS for further discussion and endorsement.
- Outcome of the Joint Working Group to be presented and reported to the AVSEC Panel through the WGACS, the Committee on Unlawful Interference and the ICAO Council for endorsement.
- Outcome of the Joint Working Group to be presented and reported to the SAFE Working Group, Policy Commission and Council Sessions for endorsement.

IX. Timelines

- January 2014 – Draft terms of reference presented to TEGACS;
- March 2014 – Information Paper presenting the terms of reference to the AVSEC Panel;
- May 2014 – Update on terms of reference to TEGACS; and
- 1st semester 2014 – Setting up of Joint Working Group.

ANNEX B - Comparison of terms used in SAFE and ANNEX 17

	WCO	**ICAO**
Advance Cargo Information	SAFE Framework of Standards, Pillar 1, para 1.3.3 Advance cargo information or advance cargo declaration (Pillar 1, Standard 1, paragraph 1.3.3) is the declaration to be submitted electronically by the carrier or his/her agent to the Customs at expert and/or at import. For all other modes and shipments, it should be lodged prior to the arrival of the means of transport at the Customs office at export and/ or import. For security purposes, Customs should not require more than the details listed in the SAFE Framework of Standards (FoS Annex II.NB new paragraph 1.3.4 and 1.3.10 are now being proposed to be introduced into the SAFE FoS for Air cargo Security purposes and suggest that a limited number of data elements should be submitted by an entity in the air cargo supply chain such as, but not limited to, the carrier, freight forwarder, integrator, postal operator or their agent as soon as the information becomes available but no later than prior to loading onto the aircraft.	Annex 9 4.17 To promote trade facilitation and the application of security measures, Contracting States shall, for the purpose of standardisation and harmonisation of electronic data interchange, encourage all parties concerned, whether public or private, to implement compatible systems and to see the appropriate internationally accepted standards and protocols.

Facilitation	WCO glossary of international Customs terms Simplification and harmonisation of international trade procedures, including activities, practices and formalities involved in collecting, presenting, communicating and processing data required for the movement of goods in international trade.	Annex 9 Facilitation is the efficient management of border control processes, to expedite clearance (of aircraft, passenger/crew, baggage, cargo) and prevent unnecessary delays.
High risk cargo	SAFE Framework of Standards, Annex 1 High risk cargo is that for which there is inadequate information or reason to deem it as low-risk, that tactical intelligence indicates as high risk, or that a risk-scoring assessment methodology based on security-related data elements identifies as high risk.	Annex 17 Cargo or mail presented by an unknown entity or showing signs of tampering shall be considered high risk if, in addition, it meets one of the following criteria: a) Specific intelligence indicates that the cargo or mail poses a threat to civil aviation; or b) The cargo or mail shows anomalies that give rise to suspicion; or c) The nature of the cargo or mail is such that baseline security measures alone are unlikely to detect prohibited items that could endanger the aircraft.
Risk management	SAFE Framework of Standards, Annex 1 The systematic application of management procedures and practices which provide border inspection agencies with the necessary information to address movements or consignments which represent a risk.	Annex 9 The systematic application of management procedures and practices which provide Customs with the necessary information to address movements or consignments which present a risk.

Security	SAFE Framework of Standards, Pillar 1, Section 3 Introduction It (the Customs to Customs Pillar) provides an effective mechanism (measures) for securing the international trade supply chain against the effects of terrorism and other forms of transnational crime.	Annex 17 Safeguarding civil aviation against acts of unlawful interference. The objective is achieved by a combination of measures and human and material resources.
Screening	SAFE Framework of Standards, Annex 1 Screening means evaluation of information and intelligence relating to goods and means of transport in a risk assessment process (manual, automated or otherwise).	Annex 17 The application of technical or other means which are intended to identify and/or detect weapons, explosives or other dangerous devices, articles or substances which may be used to commit an act of unlawful interference.

ANNEX C - Reports of the three pilot projects

Pilot Details	United States – ACAS	Canada – PACT	European Union - PRECISE
# of States in Pilot / Total States	1/1	1/1	8/28
Status	• Continuously ongoing from December 2010 • CBP intends to continue the pilot until full mandatory implementation	• Raw data transmissions began in February 2013 • Pilot extended to March 31, 2015.	• Express Pilot 2012 • 4 month desktop exercise with conventional carriers 2013
Regulatory timeline & status	• Notice of Proposed Rulemaking (NPRM) expected in 2015. Final Rule and implementation expected by 2016.	Pending	UCC Regulation to enter into force in 2016, with practical implementation expected in the following years.
Risk assessment data elements	• Consignor[11] Name/Address • Consignee Name/Address • Cargo Description • Piece Count • Total Weight • Consignment identifier (generally known as "7+1")	• "7+1" mandatory as an initial data set • "+1" optional - Canada proposes to adopt an optional "e-CSD"[12] data element to indicate screening has been performed	"7+1"
Submission time	As early as possible in the supply chain	As early as possible in the supply chain	As early as possible in the supply chain

[11] In the United States, the "consignor" is referred to as the "shipper"
[12] The e-CSD, electronic consignment security declaration, is a harmonized ICAO/IATA message designed to replace paper documentation of required screening information

Number and type of participants	• 17 Operational o 4 Express carriers o 6 Passenger carriers o 7 Freight forwarders • 33 Pre-operational[13] o 1 Express carrier o 17 Passenger carriers o 6 Heavy all-cargo carriers o 9 Freight forwarders	• 7 Passenger carriers • 2 Freight Forwarders • Expansion under considerations	• 4 Express carriers • 10 Conventional carriers • 8 Freight forwarders
Inclusion of mail/postal operators	Preparatory work has been completed to enable an AMAS (Air Mail Advance Screening) pilot project to be launched, in the near future. Willing postal operator and carrier participants are being identified.[14]	Postal Mail Targeting is not part of PACT. Postal Mail Targeting is underway under a separate initiative.	EU Postal Pilot with 8 EU Member States and their Postal Operators since 2012; Phase 1: transmission of electronic CN 23 data from 1) non-EU postal operator to EU postal operator 2) from EU postal operator to customs Phase 2: air carrier involvement (ongoing)
Inbound messages	• Delivered via existing CBP/carrier or CBP/forwarder communication links. • A number of messaging formats may be used including “industry-standard” IATA Cargo IMP Cargo XML , or modified CBP “CAMIR”.	• Air waybills received in two PACT-dedicated email accounts (one for CBSA, one for TC) • Message formats include FWB, FHL, and customer service bulletins	*Currently under discussion in EU feasibility study*

[13] “Pre-operational” indicates that a participant is either transmitting to the production environment for data quality analysis or transmitting to the certification system for testing – these are the two steps immediately prior to “operational”.

[14] Unlike the inbound cargo pilot projects, which can be conducted by the implementing country alone with the participation of willing carriers, mail pilots require the additional participation of other country postal operators, as the origin post is the data transmitter to the host country post, who then provides the data to the host country customs authority.

Targeting	• Shipment data is submitted to the Automated Targeting System (ATS), a rule-and weight-set based system that vets shipments against multiple reference sources. • Shipments may be reviewed manually by a National Targeting Center (NTC) officer based on ATS results or other criteria.	• Shipments reviewed manually based on risk indicators and manually against multiple reference sources • TC officers and CBSA National Targeting Centre (NTC) officers perform targeting independently, with TC officers embedded at NTC	Proposed concept: 1. Automated risk analysis by EU Customs IT system, if hit: 2. Manual risk analysis by customs officers Development of harmonised EU risk aviation security risk criteria by customs, civil aviation, and interior authorities
System responses	• Automated messages indicate acknowledgment of submission or submission error, followed by one of the following: assessment complete, a referral (data or screening)[15], or a Do Not Load hold[16] (DNL). When referral resolution protocols are completed, releases of screening/ data referrals are sent. • Data and screening referrals are also delivered via e-mail. • DNL holds also trigger a telephone response protocol.	• No automated system response due to lack of automated targeting system[17] • Requests for Information (RFI) and Requests for Confirmation of Screening are sent by officers via email • Requests for Screening (RFS) are sent by officers via email but also include follow-up telephone response; • Do Not Load (DNL) notification not being tested under the PACT pilot	*Currently under discussion in EU feasibility study*

[15] A referral or DNL holds is not issued based on ATS results alone, but only after manual review by an NTC officer.
[16] Since the inception of the ACAS pilot in December 2010, no shipment has received a Do Not Load hold.
[17] Solutions for an automated targeting system are being explored as part of the pilot extension to March 31, 2015

Referrals and resolution protocols	Upon receipt of a shipment referral (data, screening, DNL), the ACAS data filer must acknowledge the referral to the National Targeting Center by message or e-mail, and follow the appropriate resolution protocol elaborated in the ACAS Standard Operating Procedures.	Upon determining an RFI or RFS is required, officers follow the appropriate resolution protocol elaborated in the PACT Internal Standard Operating Procedures.	Three referral tests conducted in 2014 with traditional carriers, freight forwarders and express couriers. Referrals – Types tested: • Request for more information • High risk cargo screening • DNL Findings: Customs were able to get necessary the additional information and to locate the shipment within a reasonable time frame
Mitigation Strategies and Resolution Response Protocols		4 Levels of Mitigation: Level 0 – no further action required, shipment proceeds as normal, no messages Level 1 – Request For Information (RFI) – via email, does not mean shipment needs to stop, response from carrier/freight forwarder expected Also includes request for screening confirmation – has screening been applied, and if so what type and at which station? Level 2 – Request For Screening – official requests for screening from GoC. Shipment can still proceed as normal. Level 3 – Do Not Load – not being tested at this time in Canada.	Four scenarios: • No further action required • Request for more information • High risk cargo screening • DNL

ANNEX C cont.

Pilot projects

A. Canada

Section 1: Pilot Information

Background

1. The Pre-Load Air Cargo Targeting (PACT) Pilot is a joint initiative between the Canada Border Services Agency (CBSA) and Transport Canada (TC). Launched on October 1st, 2012, the PACT pilot consists of joint targeting activities, where Canada Border Services Agency and Transport Canada officers work in cooperation to risk assess cargo data submitted by volunteer air carriers and freight forwarders in advance of loading.
2. Under the Pilot, volunteer air carriers and freight forwarders provide air cargo data at the earliest point possible prior to the cargo being loaded onto aircraft destined to Canada. Once data is received, Canada Border Services Agency and targeters conduct risk assessment activities on the cargo data received for indications of risk to aviation security. When risk is identified, targeters work with volunteer participant air carriers and freight forwarders to mitigate the risk through a series of actions including:
    - Level 0: Data is reviewed, no further action required;
    - Level 1: Request for Information (RFI) – additional information is required and can include a request for confirmation of screening already conducted;
    - Level 2: Request for Screening (RFS) – additional screening is required in addition to the screening method already applied; and
    - Level 3: Do Not Load (DNL) – issued only in extreme circumstances.
3. Due to a number of limiting factors, the scope for the PACT pilot has remained passenger flights inbound to Canada only. The voluntary participants currently include seven air carriers (Air Canada, KLM Royal Dutch Airlines, British Airways, Cathay Pacific, Lufthansa, Japan Airlines, and Air France) and two freight forwarders (Kuehne & Nagel and DB Schenker). All-cargo, express, and post/mail were not included in the scope of the pilot.
4. The pilot concept and design has drawn on the experiences and best practices of the US Air Cargo Advance Screening (ACAS) pilot project and utilizes similar strategies to mitigate risk to air cargo destined for Canada from offshore. The pilot also shares best practices with the European Union's Pre-loading Consignment Information for Secure Entry (PRECISE) pilot.

Components

5. The original concept of the PACT included stakeholder participants providing a subset of available cargo data at the earliest point possible, but no later than prior to loading at the last port of departure. This subset of data would include any of the information currently required by Canada Border Services Agency (4 hours prior to arrival) under the Advance Commercial Information (ACI) program. The sub set of data would then be risk assessed using Canada Border Services Agency existing automated targeting systems. It was determined, however, that due to Canada Border Services Agency and industry IT systems limitations, that data could not be either transmitted by the carrier or received by Canada Border Services Agency in its existing format without costly investment on both sides.
6. As a result, an alternative was established whereby industry participants are currently transmitting pre-load cargo data to Canada Border Services Agency and Transport Canada via email (and flat file attachments), which is then targeted manually by Canada Border Services Agency and Transport Canada officers. A solution to enable automated targeting is under development as manual targeting is not an ideal option for moving forward.
7. Message formats currently received via email from air carriers and used for targeting purposes include master airway bills (FWB); consolidation messages or house airway bills (FHL); and customer service bulletins as attachments to emails. Due to the format of submission, targeters are able to see anywhere from 7 to 30+ data elements including items such as shipper name and address through to handling messages and screening codes.

What has been tested?

8. The PACT is currently completing an evaluation of the past 2 years of pilot data. During this evaluation, the pilot work, including targeting efforts continues. Some of the initial findings are listed below:

    - **Data availability and data quality:** Initial findings confirm that, in most cases, the minimum data elements (shipper name/address, consignee name/address, piece count, weight, and air waybill number) required for effective risk analysis are available prior to loading of cargo and often days before. Due to PACT's alternative format for data submission it has been shown that aside from the initial data elements required for targeting, there are many other data elements—at times over 30— also available that are very useful at providing the risk picture needed to either mitigate or identify risk. These additional data elements (e.g. screening codes, routing) form an integral part in the overall risk picture of a shipment, and are often the data elements requested when issuing an RFI – Request for Information, to the carrier or freight forwarder.

    - It should be noted that in situations where the data is absent or of insufficient quality, it becomes much more difficult to mitigate risks. When accurate and additional supporting data elements are provided, the risk mitigation activities are

expedited by not having to request additional information from carriers and freight forwarders. A key piece of information that we have discovered be readily available is the “handling codes”, which are normally part of the electronic Consignment Security Declaration (e-CSD). These codes provide information on how (and if) the cargo was screened or accepted by a regulated agent/known consignor.

- **Messaging/referrals:** Despite the lack of an automated system for risk assessment and mitigation messaging, the pilot has been successful in establishing communication with industry participants both in receiving advance cargo data and in sending referrals to participants when further information or screening is required.

- The current process of requesting more information from a participant includes a standard email form that identifies an RFI - Request for Information or an RFS – Request for Screening, by including the details of the shipment (i.e. air waybill number) as well as the type of information that is being requested. These standard messages are sent to the identified point of contact for the stakeholder. If a response is not received, the targeter will reach out by telephone.

- Messaging and referrals for PACT typically follow a progression, where Level 1 RFI _ Request for Information is the initial contact, Level 2 RFS – Request for Screening is used when risk cannot be mitigated with additional information and Level 3 DNL - Do Not Load message for cargo that poses an imminent threat. It should be noted that during this phase of the pilot, Level 3 DNL – Do Not Load message has been tested by means of Table Top Exercise only and operationally remains out of scope. No Level 3 DNL – Do Not Load messages have been issued as a result of the PACT pilot.

- **Risk Assessment:** The PACT pilot has begun to develop and test a specific risk assessment process that includes risk based rules/algorithms, analysis of submitted information against intelligence and historical data, practical examples from previous incidents including previous enforcement history, as well as knowledge of the aviation environment and relevant threat/risk assessments.

- During this risk assessment process it was found that security screening codes were frequently included with the initial set of advance cargo data received from participants. Further, within the context of the mitigation process, when return messaging was sent to industry requesting further information about a particular shipment, responses from industry often included an e-CSD. This form contains important security information which proved very useful for mitigating possible high risk cargo or confirming high risk cargo screening.

- **Table Top Exercise**: As part of the PACT pilot activity, a Table Top Exercise was completed that provided all stakeholders and participants the opportunity for a face to face walk through of various scenarios. These scenarios simulated a live environment and provided for group discussions between the Canada Border

Services Agency, Transport Canada and industry, thus allowing all involved to learn from each other and identify issues that can be addressed at the earliest point possible.

Benefits

9. From an aviation security perspective, the PACT pilot has demonstrated that targeting and risk analysis could be used as an additional layer of aviation security, specifically for inbound air cargo. Through the joint activities conducted it has been proven that cargo data is available, a risk assessment can be conducted and communication protocols can be achieved so that a shipment can in most cases be isolated and screened in accordance with direction from the regulating authority, and in partnership with industry.
10. Consequently, what the pilot has realized is that information (through risk assessment) that could potentially identify a high risk shipment or more specifically an incendiary explosive device (IED) in a shipment, is available before loading onto an aircraft. The opportunity to prevent an attack is possible through this type of program, and as such supports the mandate of an aviation security regime.
11. From a national security perspective, it has been noted that the receipt of data in the pre-load time frame has proven ability to push the border out and mitigate risk at the earliest point possible. While the focus of the pilot remains on imminent threats to aircraft, there are ancillary benefits to the protection of Canada's national security by being able to conduct risk assessment activities at an earlier point in time.
12. The other additional discovery has been that it has been noted that there is the ability on the part of industry to send customs currently prescribed pre-arrival trade data prior to loading, as opposed to prior to arrival. The additional potential benefit of this is for trade chain partners (e.g., air carriers, freight forwarders) to respond to other types of information requests and data clarification issues before the cargo arrives in Canada. Additionally, these earlier reporting timeframes could also provide customs authorities with more time to respond to other threats (e.g. criminal, health, etc.) at the port of arrival.
13. A significant and noteworthy benefit or success of this pilot has been the demonstration of excellent cooperation and coordination between industry stakeholder participants and Canada Border Services Agency/Transport Canada officials. Since the beginning of the pilot, stakeholders have been very active and supportive of the pilot, both through regular communication and membership in the PACT Working Group.

Challenges

14. The PACT pilot is not devoid of its challenges. The two most prevalent challenges to date have centered on information sharing and the use of an automated system. There are currently some legal and legislative impediments that limit the amount and type of information that can be shared between Transport Canada and Canada Border Services Agency. The ability to share intelligence and tactical information

between departments is key to the success of PACT and is an ongoing issue that has been identified as a priority.

15. The alternative data submission designed for PACT is not feasible for the long term. The absence of an automated system, including automated risk scoring, has limited pre-load targeting abilities and has placed a small burden on the industry participants.

16. Additional challenges for the PACT pilot moving forward will be dependent on expansion of the current pilot scope and transition to a PACT standard program. The pilot has been fortunate to have had only 7 participants comprised of passenger carriers only. Future iterations of the pilot will include expansion to other business models including express couriers and cargo freighters. Adding these business lines will help with the identification of owners of the data, at which point in time and offering accessible filing options for industry.

Section 2: Discussion Items

a) Required components:

Processes and systems

17. Due to large volumes of advance cargo data, the use of an automated targeting system is critical for risk assessment and return "real-time" mitigation messaging. Though automated targeting could not be tested during the PACT pilot, short and long-term solutions for an automated system are under development.

Data elements

18. Explanation of how we came up with 7+1 and why these are considered as sufficient:

- In trying to keep the impact on industry minimal, the pilot has agreed that, to date, the 7+1 data elements are sufficient ***as an initial data set*** for beginning the risk assessment process. However it should be noted that through the PACT pilot it has been determined that the additional air waybill data is extremely useful in mitigating risk and when it is received as part of the data submission it can often eliminate needless communication and burden on industry with the need for requesting further information through an RFI – Request for Information. Specifically, the screening code and or acceptance messaging that is included in an e-CSD has proven very useful.

- When return messaging is sent to industry participants requesting further information about a particular shipment, it has been proven useful for mitigation purposes to request the optional inclusion of the e-CSD attached to the shipment in question.

- Unless proven otherwise, these should be accepted as minimum data elements

- As per above, 7+1 data elements are sufficient ***as an initial data set*** for risk assessment, though further information may be requested during the risk assessment process. Complete and accurate information is essential in the risk mitigation process, and access to more information can help in this process.

Intelligence required

19. Intelligence is a key factor that forms part of the air cargo risk assessment process. Information sharing regulations that enable communication between departments and potentially other countries is critical in making robust assessments and in executing risk mitigation procedures.

Importance of data quality

20. Complete and accurate information can help mitigate potential high risk shipments. It should be noted that in situations where the data is absent, insufficient or incomplete, it becomes much more difficult to mitigate risk. Since the initial data set of required data elements is currently limited to 7+1 it becomes increasingly important to have complete and accurate data submissions.

Risk assessment processes

21. Under the PACT pilot, targeters manually review advance cargo data for indications of high risk cargo. Based on various risk indicators determined through a risk assessment process targeters will escalate a shipment that presents potential risk. Once a shipment has been elevated or identified, progressive mitigation strategies are employed. These include:

    (0) **No further intervention required**, shipment proceeds as normal

    (1) **Request for Information:** return messaging to industry requesting further information or clarification about the cargo data, including any available security screening codes or information. These requests are sent when the data is insufficient to form a risk picture.

    (2) **Request for Screening:** return messaging to industry requesting further screening of the cargo shipment. These requests are sent when there is sufficient data to form a risk picture and the shipment presents with high risk to aviation security.

    (3) **Do Not Load:** directive to industry not to load the cargo shipment on aircraft (NOTE: the “Do Not Load” mitigation has not been used under the PACT pilot).

22. In reviewing advance cargo information, targeters follow a sequence of steps, beginning with an initial triage of shipments. At this point, targeters identify possible high risk shipments based on the initial information received. If a determination is made that further information is required on a particular shipment, communication is established with the industry participant. The new information, once received, is reviewed by targeters to determine whether this is sufficient to mitigate the risk. If a determination is made that the shipments still presents a high risk to aviation security, a tactical response is initiated in the form of a request for screening.

23. Targeters review the results of this screening to determine whether this is sufficient to mitigate the risk. The final mitigation measure—which is not being tested during the pilot phase—would be a “Do Not Load” notification to the air carrier. This notification would theoretically be sent to an air carrier when the aviation security authorities determine that the shipment poses an imminent threat to aviation security, based on a variety of risk indicators.

Roles and responsibilities

24. The PACT pilot roles and responsibilities stem from the mandates and authorities of CBSA and TC. At the macro level, as the civil aviation authority Transport Canada is the department responsible for preventing and managing security risks in all modes of transportation, including aviation. Transport Canada is working to make further improvements for a secure Canadian aviation system that is protected against unlawful interference, terrorist attacks or use as a means to attack our allies. As the customs administration CBSA is responsible for overseeing the management of the border, focusing its efforts on clearance of people and goods. In the air mode, the Agency employs various mechanisms to help identify threats to Canada’s border security, including the use of advance commercial information to risk assess cargo prior to arrival in Canada. The use of ACI pre-load has been ongoing in the maritime mode since 2004.
25. Under the current PACT model air cargo manifest (waybill) data is received at the earliest point possible. This data is generally a flat file of raw manifest data that includes all data elements the air carrier requires to issue the waybill. This information is received via email to both the CBSA and Transport Canada, where targeters will triage the information using a risk analysis process. The risk analysis and targeting is performed by Transport Canada and Canada Border Services Agency with a specific aviation security lens leveraging expertise, indices and intelligence information from both departments.
26. Throughout this process when a shipment is identified as high risk to aviation security, a PACT officer will contact the air carrier to request additional Information (RFI). Upon receipt of additional information and risk remains unmitigated, further mitigation steps, including RFS – Request for Screening and DNL – Do Not Load messages will be made by Transport Canada, as the department responsible for Aviation Security."

Standardization

27. Canada believes a key success factor to implementing aviation security Advanced Cargo Information type program (similar to PRECISE or ACAS) as a component of a national air cargo security program is to also strive to achieve international consistency. This includes:

    - Working with key partners to align concepts and processes to achieve a global standard to the extent possible.

- Where possible, support efforts for international cooperation and harmonization amongst Customs Administrations, Civil Aviation Authorities and agencies responsible for air cargo/airport security.

- Participate in global standardization efforts by participating in international discussions organized through the efforts of the World Customs Organisation (WCO) and International Civil Aviation Organization (ICAO).

- Continue to work closely with the global air cargo industry to further explore how to implement and operate these types of programs without impeding the flow of trade while providing a real security benefit.

B. European Union

Background:

28. EU Customs authorities have the mandate to control the flow of goods entering into the EU. In 2006 the EU Customs Legislation was changed in order to address safety and security concerns. One of the components was the introduction of the requirement for traders to provide customs authorities with advance cargo information through the lodging of an electronic declaration (the so called Entry Summary Declaration - ENS) for goods prior to import to the European Union. The ENS requirement entered into force on 1 January 2011. In the air mode of transport the ENS has to be submitted 4 hours before the arrival of the plane at the first airport in the EU for long-haul flights or at "wheels up" for short-haul flights.
29. After the Yemen Incident the EU Air cargo security action plan highlighted weaknesses of the EU advance cargo information system as regards data quality and timely availability and gave the mandate to EU Customs to test an additional layer of data requirements before loading in the air mode.
30. Whilst EU customs' first intention was to shift the timeline of the submission of the ENS from pre-arrival to pre-loading, first discussions with trade showed that it would be very challenging to submit the whole data set to Customs at that early stage. Therefore the EU tested the submission of a reduced set of 7+1 data, following the US ACAS approach, beginning with the express couriers (2012), followed by postal operators (start in 2012) and the traditional air cargo business model – PRECISE (2013).

Express Courier Pilot

31. As first pilot activity in response to the EU Air Cargo Security Action Plan, the express courier pilot, conducted in 2012, assessed the feasibility of data submission prior to loading taking into account the US ACAS approach. 4 Member States (Belgium, France, Germany, and the United Kingdom) and 4 express couriers services (DHL, FEDEX, TNT, and UPS), represented by the EEA, actively participated in the pilot.

32. The scope of the pilot was to address security related risks that would require intervention prior to loading of cargo on an aircraft and were thus focused on explosive and incendiary devices. The evaluation of the express courier pilot showed that the set of 7+1 data tested (so-called 'raw data') can be made available early and is sufficient for a first layer of security risk analysis for air cargo.

EU PRECISE

33. Based on the findings of the express courier pilot, the EU decided to assess the feasibility of gathering pre-loading information and the appropriateness of the so-called 'raw data approach' in the traditional air cargo business model (air carriers, freight forwarders). Due to the limited time frame, it was decided that this exercise should take the form of a desktop study, referred to as EU PRECISE ("Pre-loading consignment information for secure entry").

34. The participants were from 8 Member States (Belgium, France, Germany, Italy, Luxemburg, Netherlands, Sweden, United Kingdom), 8 airlines (Air France, British Airways, Air Canada, Cargolux, Delta, KLM/Martinair, Lufthansa Cargo, SAS, Singapore Airlines, Alitalia), 8 freight forwarders (DHL Global Forwarding, Expeditors, TFL Overseas (representing several French freight forwarders), DB Schenker, Anama, Kühne + Nagel, Logwin Air Ocean, Interline Luftfracht) and further stakeholders (Cologne Bonn Airport, AOC Fiumicino, Cargonaut, ground handlers) actively participated in the study. The study was supported by 6 trade associations (IATA – AEA/ FIATA – CLECAT / TIACA and EEA).

35. As in the express courier pilot, the study showed that the set of 7+1 data elements was sufficient for a first layer of security risk analysis in the traditional air cargo business model. Data can be made available early by using industry standards reproducing HAWB information.

36. The study allowed gaining a solid understanding about the fundamental features of the traditional air cargo business model including the process flows and the roles of the main parties. The study led to identifying different options for pre-loading data submission that take account of the diversity of the general cargo business model and the different capacities of the involved supply chain parties.

EU Postal Pilot

37. The EU also assessed implementation options for introducing advance electronic data submission requirements for goods moved under the UPU. 8 Member States (Belgium, Denmark, France, Germany, Italy, Spain, Sweden and United Kingdom), and their respective Postal operators (B-Post, Post Denmark, La Poste, Deutsche Post, Poste Italiane, Correos, Swedish Post and Royal Mail) and 2 non-EU Posts (United States' Postal Services (USPS) and Canada Post) and the International Postal Corporation (IPC) as well as Kahala Post Group (KPG)/Australia Post, PostEurop, IATA / AEA actively participate in the Pilot.

38. The pilot allowed gaining a full understanding about the fundamental features, imperatives and specificities of the Postal Model for goods moved under the UPU. The pilot confirmed the use of the electronic CN23 and the relevant UPU messaging standards (ITMATT, CUSITM) and the specific mail data flows (i.e. between origin and destination posts, first, and between destination post and Customs in the destination MS, second).

Components - Operational approach

39. In the **EU express pilot** industry participants (DHL, FEDEX, TNT, and UPS) provided Customs with access to their systems that contain information on consignments pertinent to the security risk analysis. The pilot tested the quality and availability of "raw data" for selected consignments and could cover all goods. Selection parameters focussed on e.g. operators' business products, origin, short/long haul and distance to the depot (first service centre). Pilot processes were either based on historical or "real-time" data and included access to imaging information.

40. The **PRECISE study**, although intended to be conducted without real time processes, closely reached 'real time' levels. EU Member States analysed real cargo information (IATA CARGO IMP messages as FHL, FWB, XFZB) from former flights or by automatically sending a copy of the forwarder message to customs (MS analysed thousands of shipments). EU Member States analysed data already available in the supply chain, either by extracting data from operators systems or after receiving data Information currently available in ICS was also used, together with documentation available at arrival.

41. In the **EU Postal Pilot** two data transmission flows, which take account of the specificity of the postal business model, were tested: the first data flow was the inter-postal data transmission between the Post in the country of origin and the Post in the country of destination. The second data flow was the data transmission from the Post in the country of destination to the competent office of the Customs of that country. Regarding the first flow, data was provided by two non-EU Posts: USPS and Canada Post to specific EU Posts. The **message standards** for the electronic data transmission are the relevant UPU messaging standards; notably the ITMATT (the UPU messaging standards for the inter-postal exchange of item level data.) For the second flow between EU Posts and MS Customs, the ITMATT message was converted into an ICS test format as a 'light' ENS (referred to as "ENS-P").

42. The pilot activities were carried out in close coordination with international partners, especially the USA and Canada who have been conducting similar pilots, ACAS (US) and PACT (CAN) and with relevant international organisations (WCO/UPU/ ICAO).

43. Three referral tests, each one with airlines, freight forwarders, and express couriers were conducted in 2014. In each of the tests, the PRECISE group risk-analysed ca. two dozens of shipments, based on information available in the optical archives or tracking systems of the respective operators. Once a consignment was selected for further action 3 types of referrals were initiated (see under "what has been tested")

What has been tested?

Data availability

44. In all business models the 7+1 data can be made available early to customs by the operator system or by using industry standards reproducing HAWB information or the data is available on the CN 23 customs declaration.

Data quality

45. The set of 7+1 data tested in the pilots is sufficient for a first layer of security risk analysis as it contains the motivators behind the transaction (data elements "shipper, consignee"), and the nature of the goods shipped (data element "goods description, weight, number of pieces").

Referral Protocols

46. In the referral test the following referral types were initiated:

- Additional information like scanned invoice/packing list/AWB etc.
- High risk cargo screening results/additional high risk cargo screening
- Do not load

47. In all tests the PRECISE group was able to get all necessary information about the selected shipments within a reasonable time frame and in addition to locate all shipments that it asked for. The real-time processes that were tested worked very well in general.

Benefits and challenges

48. The benefits are first regarding "Security"- an additional layer of risk analysis (bomb in the box) and second regarding "Facilitation"- an earlier submission of data, a faster processing better data quality and fewer rejection of data, faster processing while using existing processes and structures and avoid duplication.

49. The most important challenges will be the Cargo movements on multi-stop routes, multi-modal cargo and that the Implementation (in EU) will require major changes to the Customs IT system. Furthermore technical and human challenges on operational legal and resources could appear and EU system architectures (such as ICS control system or Automated Import System) need to be upgraded.

Distinction between pre-arrival, pre-departure, and pre-load data

50. In the EU the following distinction applies:

- pre-loading data (tested during the pilots, legislative proposal pending): cargo information submitted before loading, aimed at immediate threats to air cargo security e.g. explosive device concealed in cargo,.

- pre-arrival data (mandatory since 2011): Entry summary declaration, i.e. cargo information submitted electronically by traders prior to arrival of goods in the EU, aimed at other risks with regard to risk management and supply chain security

- Customs declaration: to be lodged to the customs office where the goods were or will shortly be presented, in order to place goods under a given customs procedure

- pre-departure declaration (export): cargo information submitted electronically by traders prior to departure of goods from the EU. For this the customs export declaration is used with regard to risk management and supply chain security.

Roles and responsibilities (between customs and aviation security)

51. The findings of the EU pilots suggest the following concept:

- Customs receives the pre-loading data and conducts the "first layer" of risk analysis aiming at an immediate risk for aviation security (based on risk criteria developed jointly with AVSEC).

- During risk analysis customs consults AVSEC authorities, if necessary, in one case or the other.

- If the risk analysis reveals a significant aviation-security related risk Customs issues a request for a referral – by using the existing processes and mechanisms of AVSEC such as the High risk cargo screening (the definition by AVSEC of High risk cargo will be used here).

Required components: Processes and systems

52. In the EU there is an electronic Customs advance cargo information system in place, the Import Control system (ICS). However, major system upgrades will be necessary to implement the changes resulting from the pilots. Those are being currently assessed in an implementation feasibility study.

Data elements: Explanation of how we came up with 7+1 and why these are considered as sufficient

53. After the Yemen Incident, EU Customs intended to shift the timeline of the submission of the Entry Summary Declaration (ENS)[18] from pre-arrival to pre-loading. However, first discussions with trade showed that it would be very challenging to submit the whole data set to Customs at that early stage. The ACAS pilot in the US that worked with a reduced data set of 7+1 elements showed positive results.

54. Therefore the EU tested the ACAS 7+1 data elements in the different air cargo business models, beginning with the express couriers in 2012 and extending it to postal operators and the traditional air cargo business model (airlines and freight forwarders). The pilots/study focused on the feasibility of the pre-loading submission of the 7+1 data, a subset of the ENS. However, the necessary subsequent submission of the rest of the ENS to Customs within the currently applicable time-limit, i.e. 4 hours before arrival, was taken into account as well.[19]

55. Whereas the first (pre-loading) data set is necessary to address immediate air cargo security risks (bomb in the box) the subsequent data set (pre-arrival) is used to address other safety and security risks, as currently. The EU pilots demonstrated that the data tested was sufficient for a first layer of risk analysis aimed at immediate air cargo security risks (bomb in the box). See proposed text for SAFE review 2015.

56. It is the operators' responsibility and risk to make available the data early enough in order to avoid any potential disruption of processes.

Intelligence required

57. Intelligence is important factor that will come in via the risk management process (risk rules). A common set of security risk criteria needs to be developed jointly by Customs, Aviation Security and Interior authorities with elements pertaining to the specific threats to the air cargo transport mode.

Importance of data quality

58. Modern Customs security risk management systems rely on accurate data to make informative decisions on cargo clearance procedures and grant facilitation to traders. It is crucial that Customs gets the right data, at the right time, from the right person in order to conduct effective risk assessment which allows for trade facilitation. For example, with regards to the specific data elements "consignor/shipper" and "consignee" information about the real supply chain parties motivating the transaction and movements of goods is required whereas information about logistic providers is not sufficient.

[18] See above page 1,2

[19] Different options were tested during PRECISE with regards to persons submitting the first and second data sets, as well as the submission of the complete data set before loading.

Risk assessment processes

59. EU Customs authorities conduct risk management to systematically identify and mitigate different kinds of risks in the international supply chain in order to protect the security and safety of EU residents and the protection of the financial and economic interests of the EU.

60. The aim is to manage risks in an optimal way, for example: the security risk of an explosive device or threat posed by a highly infectious disease needs to be addressed prior to loading; prohibited, smuggled or dangerous goods need early intervention, but can be controlled upon arrival on EU territory or at the place of unloading; some risks such as product safety can be dealt with at the time of clearance; financial, commercial policy and other risks can be addressed at the time of clearance, as well as post-clearance through audit controls. Therefore the pre-loading advance cargo information which is subject of the EU Air Cargo pilots is intended for targeting exclusively “a bomb on the plane”, i.e. immediate threats, e.g. explosive devices concealed in cargo.

61. In the EU Customs Risk Management is implemented by collecting data and information, analysing and assessing risk, assessing the level of risk, prioritizing of risk and prescribing most appropriate customs action. The EU Common Risk Management Framework (CRMF) sets out EU-wide common criteria to identify risks, common conditions for trusted traders and pre-arrival/pre-departure security risk analysis based on electronically submitted cargo information.

62. Conceptually with regards to air cargo security related risk analysis – depending on the risks detected - there are three scenarios:

    - Scenario 1: Automated (IT based) Risk analysis, no risk found, quick response time;

    - Scenario 2: if IT based hit, additional manual analysis by customs required;

    - Scenario 3: if air cargo risk related risk it found (through risk analysis, intelligence, etc.), additional analysis by customs and consultation of other authorities necessary
      Due to the need of sufficient time for the risk analysis before loading of a consignment the overriding principle must be that the trader will provide the data as soon it is available

63. Defining AVSEC and Customs roles and responsibilities

    In general terms the cooperation between Customs and AVSEC authorities will focus on the development of joint risk criteria and referral protocols, the consultation during risk analysis and the use of AVSEC definitions/mechanisms by customs.

    Link to secure supply chain systems.

Standardization

64. Highlight where we see the need for short vs. medium-term possibilities for a global model, and interoperability.

C. United States

Background

65. The Air Cargo Advance Screening (ACAS) pilot was launched in December 2010 in response to an October 2010 incident where concealed explosive devices were discovered in cargo on board aircraft destined for the United States. This incident demonstrated the significance of advance information in identifying and disrupting the attempts of terrorists to exploit the global supply chain. The ACAS pilot is a partnership between United States Customs and Border Protection (CBP), the Transportation Security Administration (TSA), and industry partners.

66. In the air mode of transportation, CBP regulations implementing the requirements of the Trade Act of 2002 (19 C.F.R. § 122.48a) already required the electronic transmission of advance air cargo information (also known as the air manifest) for cargo security and safety from air carriers and/or other eligible filers four (4) hours prior to arrival of the aircraft for aircraft departing for the United States in any foreign area in North America (north of the equator), to include the Caribbean and Bermuda. Aircraft departing from North America are required to provide the required data elements no later than the time wheels are up on the aircraft. Targeting of high-risk cargo is conducted with the advance air cargo information for all national security threats at both the national and port levels. The joint CBP-TSA ACAS pilot uses existing customs infrastructure for the specific scope of identifying high-risk air cargo prior to departure from a last point of departure (LPD) to the United States, with the sole aim of preventing the carriage of explosives in air cargo.

Description of Pilot

67. In the ACAS pilot, volunteers in the air cargo industry, specifically air carriers, express consignment couriers and freight forwarders, provide a subset of the Trade Act of 2002 data elements (ACAS data elements) as early as possible before cargo is loaded onto an aircraft. Identifying high-risk shipments as early as possible in the air cargo supply chain prior to loading provides targeters an opportunity to conduct a comprehensive review of cargo data without unduly impacting the flow of commerce into the United States. ACAS allows receipt of advance security filing cargo data as a means to target U.S.-bound cargo shipments that may be high-risk and require additional physical screening under the appropriate regulatory framework and protocols.

68. The ACAS data elements consist of the shipper name, shipper address, consignee name, consignee address, piece count, weight, cargo description, and air waybill number. These data elements must be on the shipment level, also known as the house waybill level. These data elements were chosen because they are available to air carriers and other participants early in the lifecycle of a cargo transaction and allow the ACAS risk assessment to be completed early enough in the supply chain to enhance security while minimizing disruption to the flow of goods.

69. Participants are encouraged to send data as early as possible to avoid disruptions to cargo movement before loading of cargo at the last foreign port of departure to the United States should action be required.

70. Electronic messages with the ACAS data elements are sent the National Targeting Center – Cargo (NTC-C) in advance of the cargo loading on aircraft departing for the United States. This data is reviewed jointly by CBP and TSA personnel to identify high-risk air cargo. ACAS will return message acknowledgements to the submitter as well as any holds on the shipment.

71. The pilot examines (1) the ability of the participants to provide the ACAS data elements earlier in the supply chain, specifically prior to loading of the cargo no later than the last foreign port of departure; (2) whether the data elements are sufficient for a risk assessment of the shipment; and (3) the ability of the participants to respond to holds, particularly Do Not Load holds.

Roles and Responsibilities

CBP	**Joint**	**TSA**
Employ existing electronic data interchange capabilities	Target ACAS shipments at NTC-C	Establish protocols for ACAS screening and Do Not Load holds by carriers at LPDs
Employ existing automated targeting system/tool	Initially developed rule sets for ACAS pilot use	Update Standard Security Programs with ACAS requirements

Utilize intelligence and existing law enforcement	Engage with pilot participants and manage stakeholder communications	Engage with foreign counterparts and carriers on screening requirements

ACAS and the Secure Supply Chain

72. The use of ACAS to target high-risk cargo does not negate the security processes and procedures already in place through the implementation of a secure supply chain. Rather, ACAS provides an additional layer of security encompassing the entire supply chain. ACAS operating procedures continue to be developed to fully integrate participants from all levels of the supply chain as well as account for mutual recognition of national cargo security program protocols.

Risk Assessment Process

73. Using advance shipment information submitted through the Automated Targeting System (ATS), combined with risk-based targeting algorithms, targeters analyze international inbound air cargo shipper and shipment information against intelligence and other available historical data to identify shipments, prior to loading, that may pose an elevated risk to aviation. Such shipments can then be segregated for enhanced screening measures, or may otherwise be prohibited from being transported on board aircraft bound for the United States. Submitting pre-loading data directly supports risk-based decision making to determine the appropriate level of screening for particular cargo shipments internationally.

Outcomes

74. To date the ACAS pilot has shown that industry is capable of submitting advance electronic information for air cargo prior to loading the cargo onto aircraft destined to or transiting through the United States at the LPD. ACAS data is regularly submitted well in advance of departure, sometimes even days in advance, which supports the feasibility of the pre-departure submission time frames. The pilot participants' submission of this information prior to loading has allowed CBP and TSA to target, identify, and mitigate any risk with the least impact practicable on trade operations.

Pilot Components

75. In establishing a pilot similar to ACAS, many issues must be addressed and considerations made including authorities, IT and communications infrastructure, resources and operations. CBP and TSA continue to consider the components outlined below.

    - **Authorities**: Customs and civil aviation security agencies can utilize authorities of each agency in order to establish a pre-departure advance cargo information (ACI) pilot. In the case of ACAS:

CBP

a. Authority to mandate submission of advance electronic air cargo information for national security purposes, to include the anti-terrorism mission; and

b. Authority to search all persons, baggage, and merchandise arriving in the Customs territory of the United States.

TSA

c. Authority to mandate screening of air cargo bound for the United States per the 9/11 Act screening requirements.

d. Authority to ensure compliance of security measures through assessments and inspections at LPDs to the United States as well as U.S. carriers wherever they operate.

76. Information technology (IT)/system requirements: ACAS is able to largely utilize an existing technology/communications infrastructure already in place for customs targeting, but considerations were made to enable earlier data exchange for the pilot.

- Electronic Data Interchange Capabilities
- Automated Risk Management/Targeting System

Resources requirements

77. The resource requirements are:

- Facility for national targeting
- Trained analysts/officers/inspectors to target for high-risk air cargo
- Program managers (s) to manage policy and trade outreach on both the customs and transport/aviation security side
- IT team
- Personnel for engagement with foreign government partners

Benefits and Challenges

78. Benefits of the ACAS pilot include:

- Greater ability to identify high- and low-risk cargo prior to loading of aircraft destined to the United States;
    - Prior to the ACAS pilot, there was no visibility or data to determine high-risk cargo before its departure to the United States due to limitations in existing advance electronic data requirements. Data submitted by pilot participants have improved capabilities to target high-risk cargo earlier in the supply chain.
    - The identification of high-risk cargo also enables the U.S. to meet Annex 17 requirements regarding the treatment of such cargo.

- Greater ability to inform foreign partner countries of shipments posing an immediate threat to their country;
- Ability to communicate with air carriers and forwarders when there is actionable intelligence that a shipment poses an immediate threat to aviation security;
    - Prior to the ACAS pilot, CBP did not have 24/7 contact information of air carriers and forwarders that can be reached and utilized in case of an emergency.
- Ability to mitigate any potential risks that the NTC-C identifies;
    - Prior to the ACAS pilot, there was not a communication mechanism or protocols to mitigate a threat if high-risk is identified prior to the aircraft's departure to the United States.
- Streamlined Department of Homeland Security responses to aviation security threats by (1) recognizing TSA screening protocols for high-risk cargo as a way to mitigate high-risk ACAS shipments, and (2) co-locating TSA inspectors with CBP targeters in the NTC-C for ACAS targeting operations.
- ACAS provides an additional layer of security as a part of the strategy to meet the 9/11 Act mandate for air cargo screening which is based upon the secure supply chain approach and requirements in U.S. Standard Security Programs.

79. Challenges faced throughout the ACAS Pilot consist of the following:

- Understanding the complexities of varying business models of the air cargo industry when importing into the United States required investing significant time and effort cooperating with air industry partners.
- Compelling all participants to become operational and all of the air industry to participate on a voluntary basis.
- Determining response protocols, screening requirements, and/or Do Not Load procedures for high-risk cargo identified at the LPD or before cargo reach the LPD. Such protocols will eventually need to be enveloped into Standard Security Programs.
- Understanding oversight of the involvement of overseas freight forwarders who are not regulated by either CBP or TSA.

ANNEX D - Joint principles from the pilot projects

80. The pilot activities in US (ACAS), EU (PRECISE) and Canada (PACT) were carried out in close coordination with each other. A comparison between the key findings of the pilots showed that all share the same general principles which are reflected in the following list of Joint Principles on Advanced Electronic Data in Air Cargo Security:

- Data = set of key data elements relating to:
    - Persons motivating the transaction
    - Goods
    - + Consignment Identifier

- Data submission to customs as early as possible, but not later than before loading onto the aircraft
    - Data submission
    - By the most appropriate source
    - With the least impact on the supply chain
    - Taking into account different business models and filing options
    - Ensure data quality

- Security risk analysis before loading onto the aircraft
    - Based on air cargo security specific risk criteria – to be developed jointly with other competent authorities, e.g. Customs, Civil Aviation and Interior Authorities
    - To identify and mitigate “high risk cargo”
    - To prevent explosives posing an immediate threat to be loaded on
    - board of the aircraft

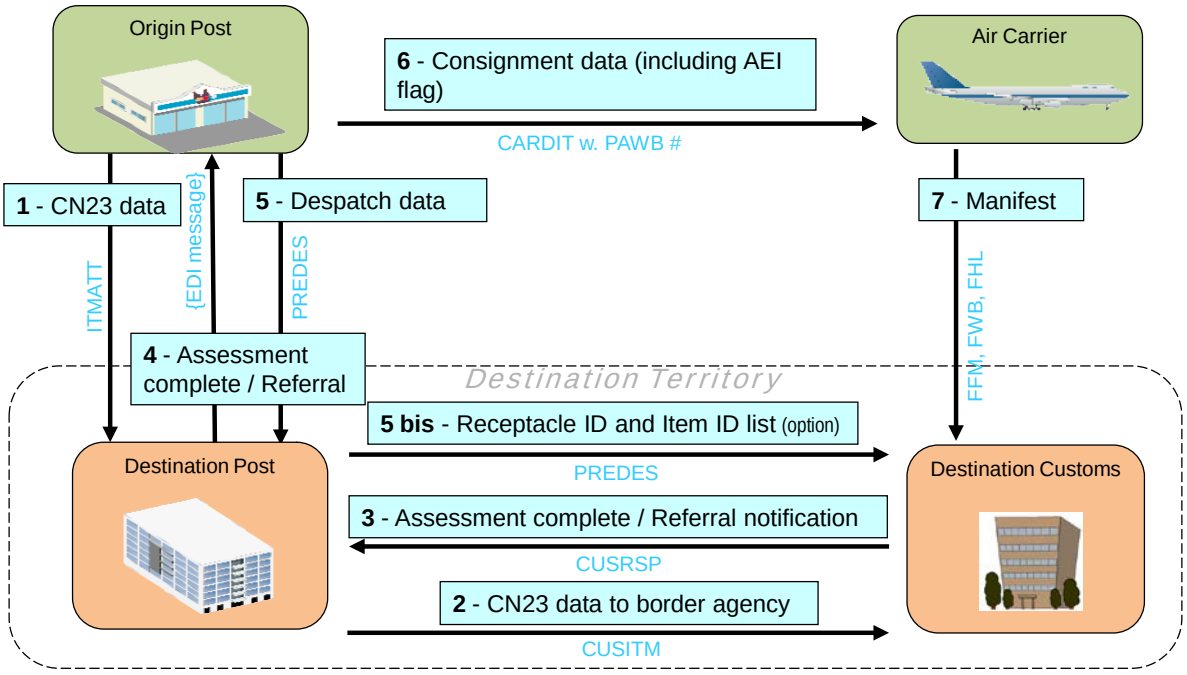
- Risk mitigation measures include:
    - Data quality
    - High risk cargo screening (ICAO rules as minimum standard)
    - Do Not Load
    - Key goals regarding legislative rulemaking:
    - Avoid conflicting rules for trade
    - Strive for global standards

- Ensure coherency and alignment between Customs and Civil Aviation Security Legislation to the fullest extent possible
    - Include in WCO SAFE and ICAO framework

ANNEX E – Flow charts

Fig. 1

Advance Electronic Information flowchart (Single global postal model)



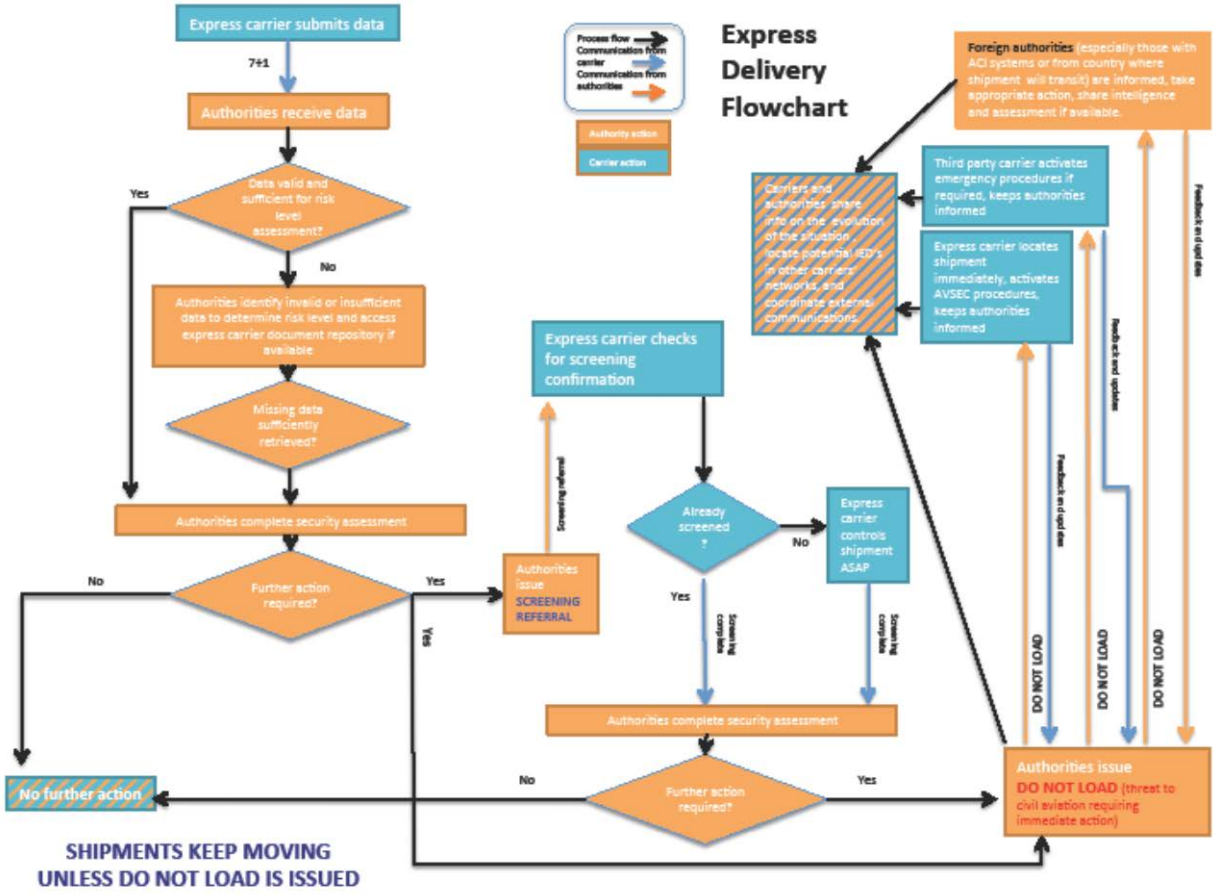
AEI Postal model v3.2 20141106

Note:
Steps 1 through 4 constitute the pre-loading (actually pre-handover) ACI model. Steps 5 bis through 7 constitute the pre-arrival phase, to allow authorities to locate a consignment in case of intelligence received after the initial risk assessment was completed, and conduct other customs risks assessment. Steps 5 and 6 are current processes, although additional elements need be added in the message for step 6.

ANNEX E

Fig. 2

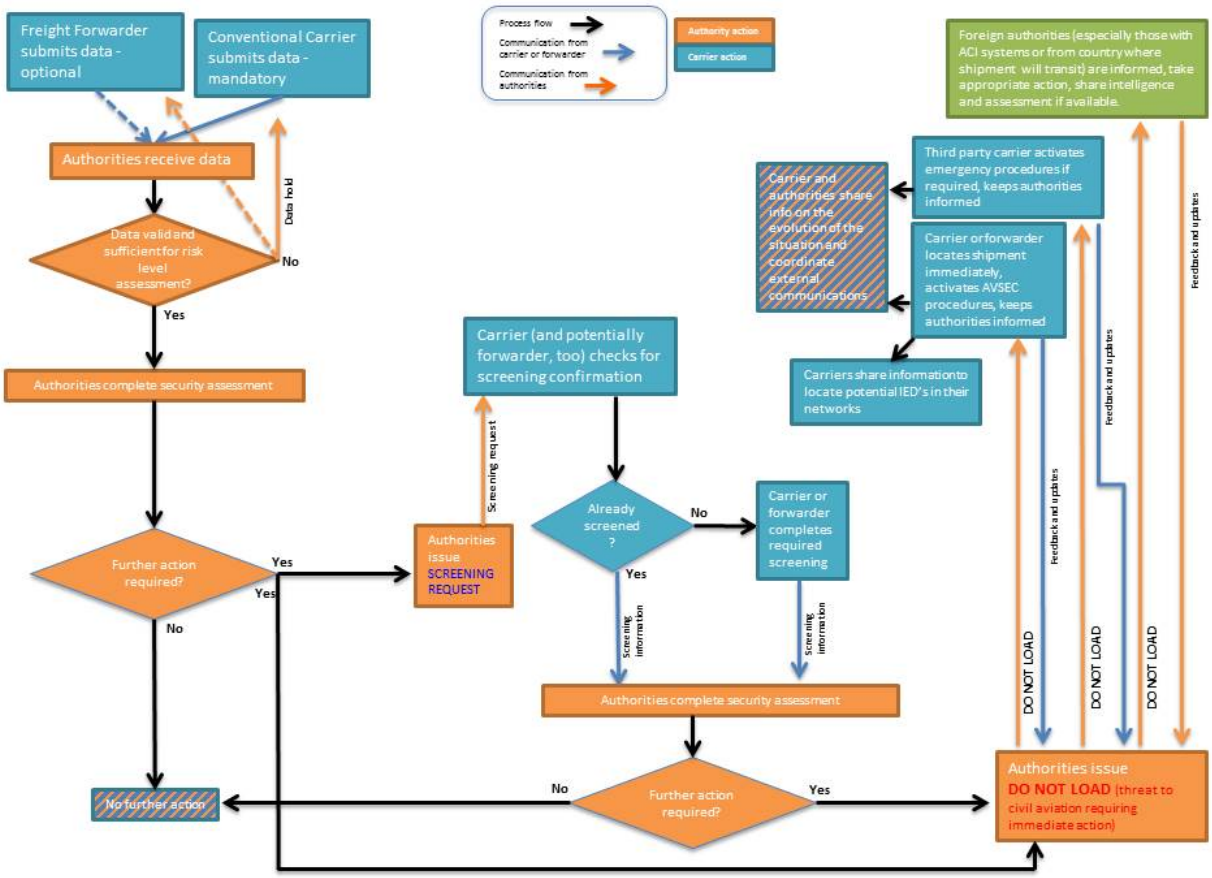
Express cargo flow chart



ANNEX E

Fig. 3

General cargo flow chart



ANNEX F

Proposed Principles and Model for Advance Cargo Information to Address States' Aviation Security requirements

Principles

1. The use of ACI for Customs purposes is recommended in the WCO's SAFE Framework of Standards. In the civil aviation context, the use of advance cargo information (ACI) lies in assessing the aviation security risk to a State. It follows that the parties who have responsibility for aviation security should be consulted on the use of ACI for AVSEC purposes.

2. Requiring submission of ACI for aviation security purposes should not be mandatory for States.

3. Should States decide to require and use ACI for aviation security purposes, a harmonised approach should be adopted, in view of the cross-border, inter-connected, and often multi-modal nature of air cargo flows.

4. The use of ACI is one additional layer of a multi-layered approach to aviation security and a total supply chain security approach.

5. Cargo movements should continue through the supply chain unless there is a clear and present threat of an act of unlawful interference that warrants a 'do not load' (DNL) order for a particular consignment.

6. States should abide by the principles of international co-operation in aviation security (as adopted by the 38th ICAO Assembly) and the Customs-to-Customs pillar in the WCO's SAFE Framework of Standards in the use of ACI for aviation security purposes.

Proposed model

As a start, the proposed model for ACI in an aviation security context that is set out below, has deliberately been kept simple so that we will be able to test and identify issues that need to be resolved before the model is expanded further up and down the supply chain. To this end, it would also be desirable to continue to take into account the experience and lessons from the ongoing pilots, both from the regulators and industry entities involved.

For a start, the model proposes that we consider the following for implementation:

- Should a State choose to implement ACI, action taken on the basis of ACI should be taken in a way that does not conflict with existing legal frameworks that the States in question are party to, including bilateral and multilateral agreements.[20]

- States adopting ACI should establish a risk assessment process for the analysis of ACI data that ensures that aviation security risk is taken into account. This could

[20] States here refers to all States in whose airports the consignment is scheduled to arrive, as well as the State requesting the submission of ACI.

include a joint risk assessment process between AVSEC authorities, Customs, and other relevant authorities as the State deems fit.

- Entities responsible for submitting ACI to the relevant regulator(s) can include air carriers and freight forwarders. The air carrier is regulated by the State of arrival through the aircraft operator security programme.

- States adopting ACI should require the submission of the following data elements (commonly known as the '7+1' that have been tested with the industry) to initiate a risk assessment for aviation security purposes.

  i) Shipper name
  ii) Shipper address
  iii) Consignee name
  iv) Consignee address
  v) Number of pieces
  vi) Gross weight
  vii) Commodity description (raw/as received; box 3 in the CSD template[21])
  viii) House Airway Bill (HAWB) number (box 2 in the CSD template)

  The submission of further information, if available, may facilitate a more robust and efficient risk assessment.

- Submission of ACI for aviation security purposes should be done pre-loading (i.e. before the consignment is loaded onto an aircraft) and as soon as possible once data is available.

- Mitigating measures following the submission of ACI should be considered in the context of measures taken to secure the entire supply chain, such as Regulated Agent, Known Consignor, and/or Account Consignor status; security controls already applied; security status assigned to the consignment; etc. Much of this information is already captured in the CSD template.

Other factors to be considered in future work of the JWGACI include:

- Whether submission of ACI is to be done electronically (for speed) or if paper submissions are allowed

- Linking ACI to other air cargo security information currently required and being transmitted, e.g., security status; CSD

- Access to ACI submitted to the destination State, by the departure State

- How to deal with multi-stop routes; transfer and transit cargo

- Related to the above, whether ACI data should be transmitted along the chain from regulator(s) to regulator(s), or if a separate submission must be made to every State in the route

[21] Consignment Security Declaration (CSD) template, Appendix 33, Amendment 1 to the 8th Edition of the ICAO *Aviation Security Manual* (Doc 8973)

- How to deal with code-share and inter-lining operations

- How to deal with multi-modal operations, especially when cargo is transferred from a non-air mode to the air mode at short notice

- How to deal with mail

- SOPs for requests for additional information; requests for mitigation measures; DNL orders; etc., between the destination State and the air carrier, as well as the destination State and the State of intended departure (the ‘host State’, where the consignment would be physically located at that point in the supply chain).