FACILITATION (FAL) DIVISION — TWELFTH SESSION

Cairo, Egypt, 22 March to 2 April 2004

Agenda Item 2: Facilitation and security of travel documents and border control formalities
2.4: Advance passenger information (API)

THE CANADIAN ADVANCE PASSENGER INFORMATION PROGRAM

(Presented by Canada)

1. INTRODUCTION

1.1 This paper describes Canada's experience in implementing its Advance Passenger Information (API) program. The program's objective is to identify and target high-risk travellers before they arrive at the Canadian border.

1.2 Canada implemented API for the air mode on 7 October 2002, making it mandatory to provide API data on international air travellers and crew members aboard flights destined to Canada, prior to their arrival. API implementation was accelerated from a two-year period to only eight months as a result of the events of 11 September 2001. Given that many commercial air carriers were already providing API data under a voluntary program in the United States, the take-up rate was very high, with approximately 70 per cent of the carriers transmitting API data to Canada within the first three months of operation.

1.3 At this time, Canada is receiving API data for only the air mode. Future expansion to other modes of transport will be determined after consultations with key stakeholders have taken place and funding has been secured.

2. DISCUSSION

2.1 API data is captured by airlines at passenger check-in by swiping the machine-readable zone of the travel document or by keying the data. It is then provided to the Canadian authorities after the flight departs for Canada.

2.2 In order to support global system interoperability, Canada's mandatory API data set conforms to the joint World Customs Organization (WCO)/International Air Transport Association (IATA) Guideline on API. In addition, Canada has made system changes to accept the nationality of the passport holder in the form of the Alpha-3 Codes specified in the ICAO Doc 9303.

2.3 Canada’s mandatory API data elements are:

Full name;
Date of birth;
Gender;
Citizenship or nationality;
Type of travel document, the country of issue and the number;
Reservation record locator, if any; and
Flight manifest data, which can vary from carrier to carrier.

2.4 **Legislative authority**

2.4.1 Canada’s legislative authority for the API program, a joint initiative between the Canada Customs and Revenue Agency (CCRA) and Citizenship and Immigration Canada (CIC), is derived from the *Customs Act* and the *Immigration and Refugee Protection Act.* The CCRA’s *Passenger Information (Customs) Regulations* prescribe that commercial carriers and charterers, travel agents, and owners and operators of a reservation system are required to provide the Minister of National Revenue with, or provide access to, specific information on all passengers and crew members en route to Canada at the time of their departure.

2.4.2 Similarly, Section 269(1) of CIC's *Immigration and Refugee Protection Regulations* states the regulatory requirement for transporters to provide API details to CIC.

2.4.3 Given that Canada’s regulations have made the provision of API data mandatory, an Administrative Monetary Penalty regime for API non-compliance has been established.

2.5 **Canada's technical solution**

2.5.1 Canada contracted with SITA, a telecommunications service provider for the airline industry, to develop software and provide secure network access to airline reservation system and departure control systems. Contractual obligations include:

a) developing API messaging software;

b) implementing a secure network access between airlines and the CCRA; and

c) certifying and encrypting airline API messages prior to transmitting them to CCRA systems.

2.5.2 Canada's API system is known as PAXIS (Passenger Information System). PAXIS has two components, the Data Acquisition Solution (DAS) and Passenger Analysis (PA). The DAS is a customized version of SITA's iDetect software, while the PA component of PAXIS is a mainframe application that was developed in-house by the CCRA. Both components are fully owned by the CCRA and operated with the CCRA's secure environment in Ottawa. CIC acts as a user of the system, and must abide by the security provisions and standards put forth by the CCRA regarding PAXIS.

2.5.3 PAXIS has been designed to accept API data via electronic data interchange (EDI), email or the Internet — in either the U.S. EDIFACT or UN EDIFACT standard. Once the API data is received, PAXIS conducts automated queries against CCRA and CIC enforcement databases, and displays the results for review and analysis by authorized customs and immigration officers. API data is stored in the PAXIS database and available to selected users for a maximum period of six years.

2.6 **Current status**

2.6.1 As of 15 October 2003, Canada is receiving API data from 99% of commercial air carriers providing service to Canada. Not all compliant carriers send API data for every flight, nor for all passengers and/or crew members for each flight. The CCRA is actively working with carriers to achieve 100% compliance.

2.7 Passenger name record (PNR) data

2.7.1 On 8 July 2003, Canada began the collection and analysis of Passenger Name Record (PNR) data, as an expansion of the API program. PNR data resides in air travel reservation systems and contains a non-exhaustive list of data respecting the traveller and associated travel plans. Examples include trip itinerary, the date the ticket was purchased, seat assignment and method of payment. Although a PNR record is non-exhaustive, Canada decided to limit the collection of PNR data to 38 specific elements. As of 8 December 2003, eleven carriers were providing PNR data and we anticipate bringing on six air carriers every six weeks until implementation is complete.

2.8 Partnership with the United States

2.8.1 Following the events of 11 September 2001, Canada and the United States committed under the *Canada-U.S. Smart Border Declaration* to "develop a border that securely facilitates the free flow of people and commerce, and that reflects the largest trading relationship in the world". More germane to this paper, Canada and the United States agreed to share API data on high-risk international travellers on a case-by-case basis.

2.8.2 Canada's PAXIS and the United States' API system will conduct automated risk-scoring of the PNR data to determine what information can be shared. This determination will be based on established risk management criteria that are common to both countries.

2.8.3 Canada is establishing a National Centre of Expertise to oversee the sharing of information and provide greater strategic coordination to detect and interdict high-risk inadmissible people and illegal or controlled goods. This centre will respond to the USA's requests for information, engage in strategic and operational intelligence gathering, and conduct trend analysis.

2.9 Protecting travellers' privacy

2.9.1 PAXIS and all the data stored in its database are designated "Protected", in accordance with Government of Canada Security Policy. Access to the data is controlled by user IDs and passwords, and is limited to a small number of authorized officers who are responsible for the transactions they complete. PAXIS has the ability to audit all transactions and show the relationship between the user, terminal, and data.

2.9.2 The Office of the Privacy Commissioner of Canada (OPC) did not have any privacy concerns regarding the implementation of the API program. However, Canada's implementation plan for PNR, which met with the OPC's approval, required strict administrative guidelines around the collection, retention and use of PNR data, which exceed the requirements of the *Customs Act* and the *Privacy Act*. The main safeguards are:

a) All information that is not required for customs or immigration purposes will be purged, including information on meals and health.

b) Like API data, PNR data will be retained for six years. However, the access and use of PNR data will become progressively more restricted during the six-year period.

c) For the first 72 hours, PNR data will be used by customs and immigration officers to assess risk.

d) From 72 hours to two years, the PNR data will be on a "no-name" basis and used by intelligence and targeting officers. The information can be re-identified with the traveller's name only when necessary for customs purposes or in relation to an immigration investigation.

e) During this two-year period, PNR data can be shared with other agencies or departments for non-customs purposes if a warrant has been obtained.

f) From two to six years, PNR data will only be available on a depersonalized basis. Access will only be provided if authorized by the Commissioner of the CCRA or the Deputy Minister of CIC, and it will only be provided where there are reasons to suspect that the name or identifying data elements are necessary to identify high-risk persons who pose a risk to the security of Canada.

g) During this final period, information can only be shared with agencies that have a national security or defence mandate.

2.9.3 Canada has been discussing privacy concerns at the international level. European airlines have stated their concern of a potential conflict between Canada's privacy laws and the privacy legislation of the country where they are located. Although the European Commission has ruled that Canada's *Personal Information Protection and Electronic Documents Act* meets the rigorous standards set out in the relevant European Directive, we continue to meet with the European Commission with a view to obtaining an adequacy finding that would allow European airlines to provide Canada with PNR data relating to European passengers.

3. **CONCLUSION**

3.1 A number of lessons can be learned from Canada’s experience in implementing its API program. First, is the importance of ensuring that legislative authority is in place to receive and use the data. The time and effort required to draft and obtain approval of supporting legislation and regulations can be considerable and, in Canada’s case, required coordination between two different government agencies.

3.2 Secondly, privacy and human rights issues should figure prominently in all planning and decision-making—ideally from the moment a country decides to develop an API program. Operational policies and system controls that provide safeguards governing the access, use and disclosure of the data are vital to the success of the program.

3.3 Thirdly, data standardization is essential. Although many carriers were already able to transmit API data in a non-standard EDI message format, Canada held firm in requiring that API data be transmitted using the U.S. EDIFACT standard. Since then, changes have been made to the PAXIS system to also receive API data in the UN EDIFACT standard.

3.4 Finally, it is important to provide carriers with options for complying with the requirement to provide API data. Not all carriers have automated systems that can transmit data using EDI. When the API program was first implemented, non-automated or low-volume carriers were sending the API data via facsimile or email. All risk assessment of this data was, by necessity, manual. Since then, Canada has worked with SITA to develop Internet data acquisition solutions that enable carriers to transmit API data to the PAXIS system—using an Excel spreadsheet, email, or through a graphic user interface (GUI) that is available on the CCRA’s website.

4. **ACTION BY THE DIVISION**

4.1 The Division is invited to note the information provided and recommend inclusion of appropriate sections in ICAO guidance material.

— END —