# Application of Advance Passenger Information (API) and Passenger Name Record (PNR) security systems by using travel information

**July, 2022**

**State Customs Committee of Azerbaijan**
**Kanazawa University, Japan**

**Authored by Rovshan Namazov**

# ABSTRACT

National security has always been a top priority for governments, and it has been a core responsibility of law enforcement officers. Certainly, the definition of national security encompasses several key areas, and it is without question that effective national security highly depends on and would be beyond the realm of possibility without integrated and coordinated border security and management.

It is crystal clear that data is a very critical resource for law enforcement agencies, and it has more value if law enforcement agencies receive the necessary data in advance. The receiving advance data of travellers enable law enforcement agencies to analyze more detailed information on time and conduct well-timed operations to detect and prevent any kind of attempted travel to, or entry into their territories of criminals or foreign terrorist fighters. The transmission of advance data or in other words, the exchange of data between law enforcement agencies or between the government and third parties is one of the key parts of the discussion, particularly the data transmission from the airline industry to the law enforcement agencies. In this regard, this article aims to identify the necessary conditions and environment for the effective application of Advance Passenger Information (API) and Passenger Name Record (PNR) systems and to share more information about the systems applied internationally.

The study mainly focuses on how to use the passenger data by law enforcement agencies in the most effective way by avoiding institutional drawbacks and implementing necessary action plans. This article suggests that the effective application of Advance Passenger Information (API) and Passenger Name Record (PNR) systems requires a comprehensive approach, not only legally or technically.

# TABLE OF CONTENTS

## Contents

# GLOSSARY OF TERMS

**Advance passenger information (API) —** Information of an air passenger collected at check-in or at the time of online check-in. It includes biographic data of the passenger, ideally captured from the Machine Readable Zone (MRZ) of their travel documents, as well as some information related to their flight (Commission, Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), 2020);

**API Batch —** An electronic communications system whereby required data elements are collected and transmitted to border control agencies prior to flight departure or arrival and made available on the primary line at the airport of entry (ICAO, Annex 9 to the Convention on International Civil Aviation, 2017);

**Computer reservation system (CRS) —** Computer reservation systems, or central reservation systems (CRS), are computerized systems used to store and retrieve information and conduct transactions related to air travel, hotels, car rental, or other activities;

**Departure control system (DCS) —** Automates processing an airline's airport management operation, which includes managing the information required for airport check-in, printing boarding cards, baggage acceptance, boarding, load control and aircraft checks;

**Global Distribution System (GDS) —** A computerized reservation system for reserving airline seats, hotel rooms, rental cars, and other travel-related items;

**Interactive API System (i-API) —** An electronic system that transmits, during check-in, API data elements collected by the aircraft operator to public authorities, who within existing business

processing times for passenger check-in, return to the operator a response message for each passenger and/or crew member (Commission, Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), 2020);

**Passenger Information Unit (PIU) —** Units established or designated within the law enforcement authorities dealing with terrorist offences and serious crimes at State level that collect, store and process API and PNR data;

**Passenger Name Record (PNR) —** A record of each passenger's travel details which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities. Air carriers shall transfer PNR data 24 to 48 hours before the scheduled flight departure time and immediately after flight closure (i.e. once passengers have boarded the aircraft). PNR data have to include API data if collected by the air carriers (Commission, Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), 2020);

**Single Window —** A facility that allows parties involved in trade and transport to lodge standardized information and documents with a single-entry point to fulfil all regulatory requirements. If information is electronic then individual data elements should only be submitted once (Commission, Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), 2020);

# INTRODUCTION

Protecting the borders from the threats such as terrorists, criminals, illegal movement of weapons, drugs, and contraband, as well as facilitating the seamless and lawful movement of people across the borders is quite significant to national security, economic prosperity and sovereignty of the nations.

Broadly speaking, border risk priorities ranges for each country and each operation is based on risk analysis and uniquely tailored to the circumstances identified by law enforcement agencies. The scope of threats ranges from terrorists who may have weapons of mass destruction to transnational criminals smuggling drugs or counterfeit goods, to unauthorized migrants intending to enter the country. However, there is one truth that a top priority mostly for all law enforcement agencies is to keep terrorists and their weapons away from their borders while facilitating the legitimate travelling of passengers and vehicles.

The border activities against the potential threats are differing from the availability of various types of borders – air, land, sea, and railway. Implementation of effective border management and security activities particularly presents unique challenges at the air borders. Because of that, the huge volume of arrivals and exits and high frequency of the flights make it very hard to detect risky passengers on time at the airport by law enforcement agencies, while ensuring the smooth movement of legitimate passengers.

The International Civil Aviation Organization (ICAO) has reported 4.3 billion passengers globally carried by air transport on scheduled services in 2018, a 6.1% increase over 2017. It is estimated that the global volume of air passengers grows at a rate between 5% and 7% every year and could reach 7.2 billion by 2036 (Commission, European Commission, 2020).

Certainly, the pandemic plunge in air traffic since 2019 and right after wide-scale lockdown measures, border closures, travel restrictions and strict quarantine rules dramatically reduced the international passenger traffic. ICAO reports that as seat capacity fell by 50% in 2020, passenger totals dropped by 60% with just 1.8 billion passengers taking to the air during the first year of the pandemic, compared to 4.5 billion in 2019 (ICAO, 2021). The pandemic is going to be over and following ICAO, in an optimistic scenario, passenger traffic is expected to recover to 86% of its 2019 levels by December 2022, based on 73% international traffic recovery and 95% domestic (ICAO, 2022).

The modern world is developing and witnessing many large-scale events and conferences and first and foremost tourism development is a key strategy of each country. With the dramatic growth in passenger numbers on scheduled and charter flights across the world on one hand and the increasing trend of terrorism and other transnational crimes on the other, it is difficult to ignore the threats against the airline industry and passengers. This continuous growth has greatly increased the workload of border agencies (customs, border service, immigration, police, etc.) and additionally, it requires certain proactive measures aiming at speeding up border controls while combating irregular immigration and ensuring internal security, like the processing of Advance Passenger Information (hereafter API) and Passenger Name Records (hereafter PNR).

## ADVANCE PASSENGER INFORMATION (API) DATA

Advance Passenger Information (API) is information about air passengers collected at check-in or at the time of online check-in. It includes biographic data of the passenger, ideally captured from the Machine Readable Zone (MRZ) of their travel documents, as well as some information related to their flight. Namely, API data is the set of data consisting of the details of

the flight by the aircraft operators and the biographic data of a passenger or crew member available on his or her travel document collected by air carriers during check-in and, complemented with travel route information, transmitted by these carriers to the border control authorities of the country of destination. According to the International Air Transport Association (IATA), over 90 countries now require airlines to send API before the flight's arrival (IATA, 2022). More countries are planning to introduce similar requirements soon.

In general, API data includes:

- Flight information;
- Scheduled departure date and time;
- Scheduled arrival date and time;
- Airport information;
- Number of passengers;
- Surname;
- First name;
- Middle name;
- Date of birth;
- Gender;
- Citizenship or nationality;
- Passport number;
- Country of passport issuance.

API data elements are transmitted by the airline companies to the law enforcement agencies of the arrival country during check-in, more clearly prior to the flight departure and the time or

frequency of the data transmission requirements can be different under the established procedures between the governments and airline companies.

It is important to note that countries should limit their data requirements to the minimum necessary and according to national legislation. Principally, API data can be divided into two main categories:

**Non-interactive Batch Style API Systems** - It is a simple form of API to implement and the data are transmitted as a single data file or batch. The definition of API Batch is an electronic communications system whereby required data elements are collected and transmitted to border control agencies prior to flight departure or arrival and made available on the primary line at the airport of entry (ICAO, Annex 9 to the Convention on International Civil Aviation, 2017). Non-interactive batch style API data is covering all passengers and, in many cases, all crew members on board a specific flight are gathered during the check-in process and then transmitted in a single manifest message at or immediately following flight reconciliation or departure (WCO/IATA/ICAO, 2014).

**Interactive API System (i-API) –** It is an electronic system that transmits, during check-in, API data elements collected by the aircraft operator to public authorities, who within existing business processing times for passenger check-in, return to the operator a response message for each passenger and/or crew member. i-API allows government and carriers to take precautionary activities interactively and reduce any potential risks prior to travel. Implementation of i-API systems is more complex than non-interactive batch style API systems in terms of cost and time. Governments should establish best practices when working with individual carriers and service providers, to ensure adequate network protocols are available. Therefore, formulation of certain action plans and comprehensive analysis is the key part of general the implementation process.

# PASSENGER NAME RECORD (PNR) DATA

PNR data – is a record in the database of a computer reservation system (CRS) that contains the itinerary for a passenger or a group of passengers travelling together. More precisely, it is a record of each passenger's travel details which contains the information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities. PNR data have to include API data if collected by the air carriers (Commission, Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), 2020).

PNR data is used by law enforcement authorities, and other public authorities competent for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crimes, and protecting the vital interests of persons.

The PNR data can contain some more sensitive personal data and the set of data required from the carriers can be varied according to the legislation of each country.

PNR data may include many separate data elements. However, the airline industry is not able to collect all the required data because of the costs and time issues. In this regard, the content of PNR data and the amount of data would be different according to the arrangements between the airlines and governments. Generally, PNR data includes, but is not limited to the following:

- PNR locator code[1];

[1] An airline's reservation system automatically generates a unique record locator whenever a customer makes a reservation or booking, commonly known in the industry as an itinerary. When an itinerary is entered into the reservation system it is commonly known as a passenger name record (PNR);

- Date of reservation;
- Dates of intended travel;
- Ticketing information;
- Travel agency information;
- Seat information;
- Check-in information;
- Baggage information;
- Phone number, mail address, payment details and some other sensitive data can also be required.

Mostly, two possible methods of PNR data transfer are used:

The first one is called a ‘pull’ method, where competent authorities of the governments requiring the PNR data can access the air carrier's reservation system and can get a copy of the required PNR data.

The second one is called a ‘push’ method, where air carriers transfer the required PNR data to the relevant authority of the country requesting the data. This method requires ensuring a high level of data protection.

In terms of creating and transferring the PNR data, when a passenger books an itinerary, the travel agent or travel website user will create a PNR in the computer reservation system it uses. This is typically one of the large global distribution systems (GDS), such as Amadeus, Sabre, or Travelport (Apollo, Galileo, and Worldspan) but if the booking is made directly with an airline the PNR can also be in the database of the airline’s computer reservation system (CRS). This PNR is called the master PNR for the passenger and the associated itinerary. The PNR is identified in the particular database by a record locator.

Regarding the frequency and timing of PNR data transfer, airlines and States determine the frequency and timing of the data transfer, taking into consideration the limitations and capabilities of aircraft operators' systems.

In this regard, the transmission time and frequency of PNR data highly depend on the requirements of the national legislation of the arrival country. In general, the PNR data is transmitted twice from the aircraft operators to law enforcement agencies, 72 hours or 48/24 hours before the scheduled time of flight departure and immediately after the flight from the airport of the departure country. However, in accordance with the requirements of the national legislation, the PNR data transmission can be requested up to 6 (six) times from the carriers until the flight will be finalized upon flight closure.

It is widely known and recognized that effective border management highly depends on the application of modern facilitation tools and profiling systems, such as API and PNR systems, which help law enforcement agencies to improve the overall security of their air borders by obtaining relevant passenger data from the carriers in advance.

In this regard, the development of law enforcement agencies' capability to use passenger data and to detect and interdict risky passengers on time requires a comprehensive and systematic approach, namely effective implementation of API and PNR systems requires the countries to be ready for legally, institutionally, operationally and technically.

## LEGAL READINESS

Legal readiness and having a strongly complied legal basis is the first key pillar of the implementation process of API and PNR systems. At first, the availability of appropriate legislation adjusts and reinforces collaboration matters on data transmission between the airline

industry and governments. The stipulation of certain articles in national legislation on data transmission issues (set of data, format, frequency, time etc.) makes clear the format of cooperation and create legal obligations as well as penalty mechanisms between the parties. In as much as, airline companies are sometimes not willing to transmit the passenger data in advance to law enforcement agencies of the arrival country, and it creates additional difficulties for law enforcement agencies to require the data from the carriers in advance if there is no legal obligation between the parties.

On top of that, one of the important aspects of API and PNR systems is the consideration of data protection mechanisms and this issue need to be legally adjusted before the application of the systems. Legislation on data protection must be enacted in countries to protect the individual's right to privacy and allow individuals to exercise their rights relating to the use of their personal data. Certainly, each country has its own legislation and data protection mechanisms vary from country to country. However, there is a common provision of such legislation. Such as, personal data (WCO/IATA/ICAO, 2014):

- should be obtained and processed fairly and lawfully;
- should be stored for legitimate purposes and not used in any way incompatible with those purposes;
- should be adequate, relevant and not excessive in relation to the purposes for which they are stored;
- should be accurate and, where necessary, kept up to date;
- should be preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which that data is stored.

Concerning the international obligation on States to implement API and PNR systems at a national level, the International Civil Aviation Organization (ICAO) has already elevated the deployment of API capacity initially as a recommended practice and followingly, accepted as a Standard in Annex 9 to the Chicago Convention. On 23 October 2017, a standard was established under Annex 9 — Facilitation, regarding the use of Advance Passenger Information (API) systems by the ICAO's Member States, and recognized that many ICAO's Member States have yet to implement this standard.

Article 9.5 clearly states that each Contracting State shall establish an Advance Passenger Information (API) system and Article 9.6 stipulates that the API system of each Contracting State shall be supported by appropriate legal authority (such as, inter alia, legislation, regulation or decree) and be consistent with internationally recognized standards for API. In addition to that, the obligation to develop the capability to collect, process and analyze, PNR data should become a standard according to the Amendment 28 to the Annex 9[2].

Another great sample of international obligation, the UN Security Council Resolution 2178 (2014)[3] was adopted and the resolution clearly states that the Member States must ensure that any measures taken to counter terrorism comply with all their obligations under international law, in particular international human rights law, international refugee law, and international humanitarian law, underscoring that respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures, and are an essential part of a successful counter-terrorism effort and notes the importance of respect for the rule of law to effectively prevent and combat terrorism. Additionally, it has been stressed in the resolution that foreign terrorist fighters increase the intensity, duration and intractability of

[2] See the link: https://acsa.cocesna.org/en/adopcion-de-la-enmienda-28-del-anexo-9/
[3] See the link: https://daccess-ods.un.org/tmp/7334761.02352142.html

conflicts, and also may pose a serious threat to their States of origin, the States they transit and the States to which they travel.

In connection with these provisions, the UN Member States are called upon to require that airlines operating in their territories provide advance passenger information to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, and further calls upon Member States to report any such departure from their territories, or such attempted entry into or transit through their territories, of such individuals to the UN Security Council Committee, as well as sharing this information with the State of residence or nationality, as appropriate and in accordance with domestic law and international obligations.

The UN Security Council Resolution 2396 (2017)[4] is another obligation that was put in place for States to implement a Passenger Name Record (PNR) system in the fight against terrorism and serious crime. Chapter VII, "Border security and information sharing", calls upon the Member States to prevent the movement of terrorists by effective national border controls and controls on the issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents and urges the Member States to expeditiously exchange information, through bilateral or multilateral mechanisms and in accordance with domestic and international law.

Moreover, resolution double stresses that in furtherance of paragraph 9 of resolution 2178 and the standard established by ICAO that its Member States establish advance passenger information (API) systems as of October 23, 2017, Member States shall require airlines operating in their territories to provide API to the appropriate national authorities, in accordance with

[4] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/25/PDF/N1746025.pdf?OpenElement

domestic law and international obligations, in order to detect the departure from their territories, or attempted travel to, entry into or transit through their territories.

However, the latest and most important part of this resolution was an obligation about the PNR data collection. Article 12 clearly states that the UN Member States shall develop the capability to collect, process and analyze, in furtherance of ICAO standards and recommended practices, passenger name record (PNR) data and to ensure PNR data is used by and shared with all their competent national authorities, with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offenses and related travel.

Further, calls upon Member States, the UN, and other international, regional, and sub-regional entities to provide technical assistance, resources and capacity building to Member States in order to implement such capabilities, and, where appropriate, encourages Member States to share PNR data with relevant or concerned Member States to detect foreign terrorist fighters returning to their countries of origin or nationality, or travelling or relocating to a third country, and also urges ICAO to work with its Member States to establish a standard for the collection, use, processing and protection of PNR data.

Furthermore, the UN Security Council Resolution 2482(2019)[5] states that implement obligations to collect and analyze Advance Passenger Information (API) and develop the ability to collect, process and analyze, in furtherance of International Civil Aviation Organization (ICAO) standards recommended practices, Passenger Name Record (PNR) data and to ensure PNR data is used by and shared with competent national authorities, with full respect for human rights and fundamental freedoms, which will help security officials make connections between individuals

[5] See the link: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/224/98/PDF/N1922498.pdf?OpenElement

associated to organized crime, whether domestic or transnational and terrorists, to stop terrorist travel and prosecute terrorism and organized crime.

WCO/IATA/ICAO (2014) API guidelines are also one of the main international regulatory instruments on API and joint recommendations by the World Customs Organization (WCO), International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO) are quite useful and productive in this regard.

## CARRIER ENGAGEMENT AND DATA TRANSMISSION

The arrangement and transmission of high-quality data between the air carriers and law enforcement agencies is an essential part of API and PNR implementation process. However, even the legal adjustments are in place, the close cooperation with the air transport industry to ensure collaboration and technical connectivity is quite significant to obtain the data appropriately and on time.

In general, countries use their own developed technologies to support the transmission of the data on crew and passengers by carriers, or they use third-party business providers in return for paying some annual service fees. Both approaches have pros and cons.

The first scenario is that countries choose their way to develop some technologies and directly arrange the connectivity between the airline companies and law enforcement agencies. In the case of the one-to-one relationship between the commercial airline carrier and the government, they need to contact and consult individually with each airline company and sign separate contracts regarding the data transmission. The whole aspects of the data exchange process, including format, frequency, time, commitments, responsibilities and so on, are reflected in the content of the contract and this is an effective way to avoid any misunderstanding or confusion between the parties during the transmission process.

Another advantage of this scenario is that the responsible government agency from the transmission process is not obliged to pay any annual service fee to any third parties, and it automatically eliminates future dependency as well. However, in order to pursue the first scenario and to be successful, high technological capacity and high-calibre manpower resources are necessary for those countries.

The disadvantage factor of the first scenario is that the process is quite long, exhausting and time-consuming. By the reason of that, the responsible government agency needs to consult with each airline company separately and there are several technical and administrative issues that need to be agreed upon and integrated between the parties and the whole process can take several months or years.

Regarding the second scenario, there are several commercial air carriers that provide information to a participating country on behalf of the carriers in accordance with applicable legislation. The advantage of this scenario is that the service providers transmit the required information in an approved format in a short time. In addition to that, the responsible government agency gains significant time by avoiding consultation and some other redundant stages to ensure data transmission. Some airline companies host the data from the carriers and then convert it to the relevant format required by the participating country and transmit it, some acquire the data from the carrier's system and format it and transmit it to the Single Window of the respective government. Some third-party service providers are:

- SITA;
- Amadeus;
- Travelsky.

To sum up, the general advantage of the second scenario is high-quality service, high-quality data, standing clear of exhausting and complicating negotiation processes and the last but not the least, gaining time. The disadvantage could be paying annual fees to the service providers and somehow, being dependent on solving technical issues in connection with data transmission.

There is another third scenario which is about the transmission of API data by e-mail. In point of fact, this scenario is not so highly recommended and there are several disadvantages. Firstly, e-mail format is not a professional and secure way to transmit the data and particularly, the PNR data cannot be transmitted through the e-mail by the commercial air carriers. Another challenge, law enforcement agencies will not be able to process and analyze the data on the risk management system and consequently, the received data by e-mail will be useless for the government agency. The reason is that the format transmitted through the e-mail, can not be converted and processed by the risk management program efficiently and this creates numerous problems in targeting and profiling processes.

## RISK MANAGEMENT TOOLS

Law enforcement agencies play an essential role in ensuring that legitimate travel meets regulatory requirements and complies with national legislation. The economic growth and social development, particularly the impressive progress in the tourism sector bring lots of benefits which governments and people can reap this benefit and enjoy on one hand, on the other hand, it puts hard work and responsibility on law enforcement agencies to manage and apply new approaches on their tasks against the new challenges and threats.

The emerging challenges at the borders urge the governments to seek and apply more professional and systematic approaches in managing known and unknown risks. Certainly, the application of a systematic and technological approach is also essential in ensuring the facilitation

of legitimate travel and avoiding redundant controls on passengers. It is crystal clear that both facilitation and control measures can be achieved by the application of a holistic risk-based compliance management approach.

Border law enforcement agencies are certainly applying risk management techniques to determine where the greatest areas of risk exposure exist and seek the best methods to manage the risks appropriately. At the operational level, law enforcement agencies are encouraged to implement risk-based control procedures based on intelligence information and robust analysis.

In respect to this, the availability of a risk system is very significant which allow law enforcement to assess, profile and target the people and means of conveyance that cross international borders and to determine what levels of intervention may or may not be required.

The processing of API and PNR data, deployment of the technical solution and application of an effective risk management system is one of the key stages of the general implementation process. It is quite apparent that without the tools, the data is useless and a huge volume of data can't be managed. Poor data governance creates inefficiency, inaccuracy and extra workload across the law enforcement departments and systems.

In this regard, the emerging risks urge law enforcement officials to perform promptly and adequately while managing the collection and targeting processes of API and PNR data. By integrating the API and PNR data into the risk management system, law enforcement agencies are seeking to identify high-risk passengers as quickly as possible in travel and conducting proactive measures to prevent inadmissible passengers into their countries.

In general, each country uses different threat and risk assessment methodologies, intelligence and targeting technologies, namely risk management systems to identify potential threats that pose a risk to the security of the country and the safety of people.

Regarding the risk management products dedicated to the processing and profiling of API and PNR data, there are some famous systems along with national products:

- United Nations "goTravel";
- WCO "Global Travel Assessment System (GTAS);
- USA "ATS-G";
- SITA "Border control";
- IDEMIA "Traveler Analytics Suite";
- WCC Group "Hermes";
- National systems;

Generally speaking, some systems have been developed by international organizations and deployed freely in their Member States, and some systems have been developed by private companies and offered to the countries in return for the package fee. The systems are designed to enable organizations to seamlessly capture, generate and analyze big data from multiple sources and provide smart analytics for efficient risk assessment at the border.

Undoubtedly, there are certain differences among the systems, in terms of functionality, documentation processes, the scope of the support package, payments, services, responsibilities and commitments between the signatories, quality, and so on.

**United Nations "goTravel"**[6] **–** The United Nations Office of Counter-Terrorism (UNOCT) Countering Terrorist Travel Programme (CTTP) aims at building the capacity of UN Member States to prevent, detect and investigate terrorist offences and related travel by using Advance Passenger Information (API) and Passenger Name Record (PNR) data in line with Security Council Resolutions 2178, 2396 and 2482.

[6] See the link: https://www.un.org/cttravel/goTravel

The UN Office of Information and Communications Technology (OICT) is one of the implementing partners under the UN Office of Counter-Terrorism (UNOCT) capacity building Countering Terrorism Travel Programme.

"goTravel" is a United Nations-owned software solution derived from the Travel Information Portal (TRIP), developed by The Netherlands. The UN received full ownership of the TRIP solution at the margins of the high-level segment of the 73rd session of the UN General Assembly and intends to further develop and deploy it to Member States also offering ongoing support while supporting the enhancement of their capacity to use API/PNR data to detect terrorists and serious criminals and their travel movements in compliance with Security Council resolutions 2178, 2396 and 2482.

"goTravel" supports the end-to-end process for law enforcement to obtain passenger data from (airline) carriers and conduct targeted analysis as well as share the findings of their data assessment. Member States adopt the UN-owned "goTravel" solution to enable the automated analysis of large data volumes on passengers in all inbound and outbound traffic. goTravel currently supports air travel data collection/analysis/dissemination.

Possible expansion of "goTravel" scope to maritime, international high-speed rail and coach information is under consideration. Expected data volumes to be analyzed exceed several million records per year for any medium-size country. Automated analysis and watch list matching are instrumental to enabling the establishment of intelligence packages for transmission to competent authorities for their action on the ground, as relevant.

The "goTravel" software solution is provided to the Member States free of charge and is deployed within Member States administrations, and no data is managed by the United Nations. Countering Terrorist Travel Programme support package for the Member States includes full

support on legislative compliance, technical application and integration, carrier engagement and connectivity and capacity-building activities on improving profiling and targeting capabilities. The main functionalities of the system include:

- Perform as a single window accepting multiple data transfer standards including receiving API/PNR data from carriers in PNRGOV EDIFACT, PNRGOV XML or UN/EDIFACT PAXLST;
- Allow configuration of rule-based risk indicators and watch lists, and list the records that are matching against those rules;
- Perform an assessment of passengers prior to their scheduled arrival/departure (matching with risk indicators, watch lists and Interpol databases);
- Manually query API/PNR data for the purpose of helping competent authorities during ongoing investigations;
- Automatically notify competent authorities when goTravel identifies passenger data requiring further examination;
- Enable analysts to reveal relationships between objects such as passengers, phone numbers, credit cards, etc. and visualize connections on graphs;
- Use network analysis to identify formally unknown relationships.

The core benefits of the system include:

- Support global WCO/IATA/ICAO standards and recommended practices for API and PNR;
- Complies with ICAO Chicago convention SARPs (Standards and Recommended Practices);

- Enable privacy protection;
- Support the integration of a data sharing module to share data within the national competent authorities and with other goTravel instances in other countries;
- Enable the establishment of intelligence packages that can then be disseminated for law enforcement action;
- Support the operationalization of best practices in terrorist travel detection from a number of countries;
- Allow the targeting of "known and unknowns" by combining API/PNR data;
- Support configuration as per Member States legislation and needs.

A maintenance fee will be charged for the provision of expertise, including the deployment, installation and maintenance support to countries that adopt the solution. This cost-recovery model is based on a Memorandum of Agreement (MoA) / Service Level Agreement (SLA) with the Member States adopting the goTravel solution.

For the initial two years from the date of the signature of the MoA/SLA, all new releases and updates of the goTravel software and related support services are free to the recipient Member State as they are covered under the United Nations Countering Terrorist Travel Programme.

Should the country using goTravel decide to continue to use the software beyond the initial 2 years' period, it can opt in to a non-profit partnership with all other participating states sharing the costs of maintenance, software updates and 3rd level ICT support.

Up to now, more than 50 Member States applied to the United Nations to adopt the "goTravel" risk management system as a solution to process and profile API and PNR data effectively and statistics show that the number of applications to adopt the system will increase continuously.

The advantage of joining the UN Countering Terrorist Travel Programme (CTTP) is not only limited to supporting Member States with the implementation of API and PNR systems, it also includes active participation in the UN events related to counter-terrorism and border security. Fundamentally, this is a golden opportunity for the UN Member States to enhance the possibility of exchanging knowledge and best practices with other member countries.

**The World Customs Organization "Global Travel Assessment System (GTAS)"**[7] - is an open-source web application for improving border security by processing API and PNR data to check and profile commercial air travellers. It enables government agencies to automate the identification of high-risk air travellers in advance of their intended travel and it is a free software tool for improving travel safety.

GTAS also was developed with the purpose of appropriately implementing the requirements and standards of the UN Security Council Resolutions 2178, 2396, 2482 and certainly Chicago Convention Annex 9.

In terms of functionality, GTAS is also an effective API/PNR profiling system with a rich feature set and a track record for success. The system is free and no paid licenses are required and the WCO Member States can deploy the system on their own internal platforms. The system is open-source and all the human-readable source code is available on GitHub[8] and the system is deployed behind a host country's firewall on their own intranet. It offers complete transparency into how the application works, so it gives confidence that the data is secure. GTAS features include creating flight grids for a real-time view of critical flights and passenger information, a

[7] See the link: https://us-cbp.github.io/GTAS/

[8] GitHub is a code hosting platform for version control and collaboration. It lets you and others work together on projects from anywhere;

priority vetting list for high-risk passengers, passenger details view and link analysis, sharing data automatically or manually with other partner agencies, and so on.

**IDEMIA "Traveler Analytics Suite"**[9] – IDEMIA is a French business company, famous for the development of technologies backed by the latest advancements in biometrics, cryptography, systems, data analytics, and smart devices.

IDEMIA Traveler Analytics Suite (IDEMIA TAS)[10] – is a sophisticated and automated risk assessment solution designed to detect persons of interest and identify suspicious patterns, all in full compliance with legal requirements as well as EU recommendations and privacy regulations. The system is one of the effective API-PNR solutions with its ability to manage massive amounts of data from multiple sources, which allows law enforcement agents to run pre-travel passenger risk analyses, screen national and international databases in real-time, develop risk profiles, spot suspicious behavior, and more. As an example, the French government is one of the users of IDEMIA TAS and in early 2014, the French government selected IDEMIA to design and roll out the API-PNR system, in compliance with the law, E.U. recommendations and privacy requirements. The system helps to collect passenger data simultaneously from up to 230 airlines with secure real-time data sharing between government agencies. This represents 70 passenger information units and more than 200 secured workspaces. According to the IDEMIA's report, more than 100 million passengers have already used IDEMIA API/PNR system in France and more than 30 international airlines and 13 cruise ship companies transmit the passenger data in Argentina in the frame of API and PNR.

[9] https://www.idemia.com/

[10] See the link: https://www.idemia.com/idemia-supports-french-law-enforcements-efforts-fight-organized-crime-and-illegal-immigration

IDEMIA Traveler Analytics Suite risk assessment solution support package includes support on legislative and regulatory compliance, secured and flexible data collection, help to design risk profile models to detect any pattern of interest and provides dashboard tools to turn data into actionable intelligence.

As can already be seen from the various examples of the products offered by international organizations and commercial companies, each system has advantages and disadvantages in terms of functionality, documentation processes, technical options etc. The general idea is that the market now is more accessible to the products for countries to conduct their effective border risk management process to prevent threats on time if they have no possibility or potential to develop their own national risk management solutions. However, it is crystal clear and certain that a comprehensive action plan for the implementation of an API and PNR transmission and processing system must be guided by the application of an effective risk system.

## PASSENGER INFORMATION UNIT (PIU) ESTABLISHMENT AND TARGETING

Law enforcement officials are at the frontline in combat against illegal activities at the border and prevent any threats that pose risk to national security. In this regard, the building of law enforcement capacity and the necessary infrastructure is a core component of the API and PNR establishment process. Simply, effective analysis of passenger data and implementation of operational activities will be resulted in detecting, investigating and prosecuting terrorist offences and serious crimes. The essence of this policy is to target criminals and crime networks, and application of preventive measures by applying the best experiences.

In this regard, the establishment of the Passenger Information Unit (PIU) or in other words, the Passenger Targeting Centre is a summit of the API and PNR implementation stages. PIU is a

division that collects and processes passenger data on people entering and leaving the country. The availability of PIU enables law enforcement agencies to work together and apply effective cooperation with all the other stakeholders for preventing, detecting, investigating and prosecuting terrorist offences.

In general, PIU operates 24/7 and functions as an intelligence-led unit to collect passenger data from the carriers through a single window. The opportunity to work on risk systems and access to watch lists and databases in PIU enables law enforcement agencies to conduct more effective targeting by using data and intelligence to identify known and unknown high-risk travellers in advance and on time.

Another important benefit of PIU is to facilitate cooperation between intelligence and law enforcement agencies while conducting an operational activity. PIU also plays a coordination role and provides operational staff in the field with access to intelligence that enables better and more effective operational activity.

Normally, PIU is a platform for multi-agency cooperation and the list of PIU agencies ranges from country to country on the basis of their border structure and risk priorities. In general, PIU includes authorities from the following border agencies:

- Customs;
- Border Service;
- National Security Service;
- Immigration;
- Police;
- Other related law enforcement agencies.

PIU provides an ample opportunity to manage the data effectively, conduct effective risk management and targeting, demonstrate a holistic approach across the border, ensure data protection mechanisms accordingly and build tight collaboration between stakeholders as a part of a cross-governmental implementation approach.

In a summary, the PIU benefits are specific for each country and highly depend on risk priorities and sharing of responsibilities among the law enforcement agencies. However, the core essence is that API and PNR implementation process could remain imperfect without having an effective PIU. The availability of PIU is an added value to the whole implementation process through better border management, effective cooperation and enhanced link between intelligence and targeting activities.

## CONCLUSION

In summary, effective implementation of API and PNR systems requires governments to apply a comprehensive approach by considering the legal, technical, operational and cooperation sides of the implementation stages. The transmission of high-quality data from the carriers to law enforcement agencies, the establishment of closer cooperation between stakeholders and the application of effective targeting by using intelligence and risk management tools help border officials to identify high-risk travellers on time, prevent serious crimes and facilitate movement of legitimate passengers across the borders. The effective processing and profiling of API and PNR data play a crucial role in ensuring national security and appropriate implementation of the concept of integrated border management. The development of cooperation among all relevant authorities and agencies involved in border management extremely enhances the data and information sharing practice and a risk-based data-driven approach in operational activities.

# BIBLIOGRAPHY


Affairs, M. a. (2020, May 06). *Migration and Home Affairs*. Retrieved from https://ec.europa.eu/home-affairs/whats-new/evaluations-and-impact-assessments/border-and-law-enforcement-advance-passenger-information-api-revised-rules_ga

Commission, E. (2020). *Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive).* Brussels: European Commission.

Commission, E. (2020, June 5). *European Commission*. Retrieved from Migration and Home Affairs: https://ec.europa.eu/home-affairs/whats-new/evaluations-and-impact-assessments/border-and-law-enforcement-advance-passenger-information-api-revised-rules_en

IATA. (2022). *Passenger facilitation*. Retrieved from https://www.iata.org/en/programs/passenger/passenger-facilitation/passenger-data/

ICAO. (2017). *Annex 9 to the Convention on International Civil Aviation.* ICAO.

ICAO. (2021, January 15). Retrieved from https://www.icao.int/Newsroom/Pages/2020-passenger-totals-drop-60-percent-as-COVID19-assault-on-international-mobility-continues.aspx

ICAO. (2022, January 17). Retrieved from https://www.icao.int/Newsroom/Pages/2021-global-air-passenger-totals-show-improvement.aspx

WCO/IATA/ICAO. (2014). *Guidelines on Advance Passenger Information (API).*