



**Privacy Impact Assessment Update
for the
Advance Passenger Information System
(APIS)**

DHS/CBP/PIA-001(g)

June 5, 2015

Contact Point

Robert Neumann

Office of Field Operations

U.S. Customs and Border Protection

(202) 344-2605

Reviewing Official

Karen L. Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is updating the Privacy Impact Assessment (PIA) for the Advance Passenger Information System (APIS) in order to provide notice of an Intelligence Community (IC) pilot leveraging APIS data shared under the terms of a Memorandum of Agreement (MOA) between DHS and the National Counterterrorism Center (NCTC), and in further support of the Department's mission to protect the United States from potential terrorist activities.

Introduction

The Aviation and Transportation Security Act of 2001¹ and the Enhanced Border Security and Visa Entry Reform Act of 2002² together mandated the collection of certain information on all passengers and crew members who arrive in or depart from (and, in the case of crew members, overfly) the United States on a commercial air or sea carrier. The information required to be collected and submitted to APIS can generally be found on routine entry documents that passengers and crew members must provide when being processed into or out of the United States. APIS information includes, but is not limited to, full name, date of birth, citizenship, passport/alien registration card number, travel document type, passport number, expiration date and country of issuance (if passport required), alien registration number, country of residence, passenger name record locator number, and U.S. destination address (when applicable). APIS information is collected in advance of a passenger's departure from or arrival to (and in many cases, prior to departure for) the United States. APIS information is also collected for each individual aboard a private aircraft arriving in or departing from the United States.

The purpose of this collection is to identify high-risk passengers and crew members who may pose a risk or threat to vessel or aircraft safety or to national security, while simultaneously facilitating the travel of legitimate passengers and crew members. This information collection also assists in expediting processing of travelers at ports of entry, resulting in a significant time savings. This IC pilot is consistent with the original purpose for the collection of APIS data.

Pursuant to the National Security Act of 1947, as amended,³ NCTC "serve[s] as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support." In

¹ Pub. L. No. 107-71.

² Pub. L. No. 107-173.

³ 50 U.S.C. § 404o.



order to enhance information sharing, the President issued Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*,⁴ which provides that the Head of each agency that possesses or acquires terrorism information shall promptly give access to that information to the Head of each other agency that has counterterrorism functions. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004⁵, as amended, places an obligation on U.S. Government agencies to share terrorism information with the IC, including NCTC. In certain instances, DHS shares the entire dataset with an IC member in order to support the counterterrorism activities of the IC and to identify terrorism information within DHS data.

In 2011, DHS began sharing the entire APIS dataset with NCTC under a Memorandum of Agreement (MOA). In 2013, DHS and NCTC entered into a new APIS MOA that supersedes the 2011 MOA and documents an increase in the temporary retention period NCTC was granted under its then newly expanded authority to hold and analyze U.S. Person information.⁶ The APIS MOA permits NCTC to use APIS information to facilitate NCTC's counterterrorism efforts and aligns with DHS's mission to prevent and deter terrorist attacks. The APIS MOA includes a number of safeguards, detailed below in the Privacy Impact Analysis section under "External Sharing and Disclosure," to ensure the data is only used for the purposes explicitly permitted under the APIS MOA, APIS PIA NCTC Update,⁷ and the DHS/CBP-005 Advance Passenger Information System System of Records Notice (SORN).⁸

The Intelligence Advanced Research Projects Activity (IARPA) in the Office of the Director of National Intelligence (ODNI) collaborates across the IC to research and develop programs in four research areas: 1) "Anticipating Surprise" develops technologies that provide decision makers with timely and accurate forecasts for a range of events; 2) "Incisive Analysis" seeks to maximize insight from collected information in a timely fashion; 3) "Safe & Secure Operations" endeavors to counter new capabilities implemented by our adversaries that could threaten our ability to operate freely and effectively in a networked world; and 4) "Smart Collection" strives to dramatically improve the value of collected data from all sources. As part of its research, IARPA developed the Security and Privacy Assurance Research (SPAR)

⁴ Exec. Order No. 13888 Further Strengthening the Sharing of Terrorism Information To Protect Americans (October 25, 2005), available at <http://www.gpo.gov/fdsys/pkg/WCPD-2005-10-31/pdf/WCPD-2005-10-31-Pg1592.pdf>.

⁵ Pub. L. No. 108-458.

⁶ GUIDELINES FOR NCTC ACCESS, RETENTION, USE, AND DISSEMINATION OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION (March 2012), available at <http://www.dni.gov/files/documents/CLPO/NCTC%20AG%20Guidelines.pdf>.

⁷ DHS/CBP/PIA-001(f) APIS NCTC Update (June 5, 2013), available at <http://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

⁸ DHS/CBP-005 Advance Passenger Information System System of Records Notice (SORN), 80 FR 13407 (March 13, 2015), available at <https://www.federalregister.gov/articles/2015/03/13/2015-05798/privacy-act-of-1974-department-of-homeland-security-united-states-customs-and-border-protection>.



program, which allows an information sharing exchange that minimizes the risk of disclosure of private information while also facilitating lawful access to threat information needed to protect the nation.

During the pilot, the Parties will test SPAR's ability to both encrypt DHS's APIS data in a DHS-controlled enclave, and encrypt NCTC's queries against the data, while producing analytically useful encrypted results. This should enhance privacy by preventing one participant from seeing the information furnished by the other, whether as raw data, query terms, or query results, before they are associated together as a match to a valid counterterrorism query. During the pilot, query results will be validated by DHS, NCTC, and IARPA. If successful, this pilot may be an important step in reducing the need for DHS or others to engage in multiple bilateral bulk sharing arrangements.

DHS and NCTC will leverage a subset of data already shared under the APIS MOA in a pilot arrangement to test SPAR's ability to maintain or enhance security and privacy protections in information sharing efforts. Under the pilot, and as outlined in a Letter of Intent (LOI) between DHS, NCTC, and IARPA, DHS will make this subset of APIS data available to IARPA for the sole purpose of testing the SPAR technology. This PIA does not alter the protections covered in APIS NCTC Update PIA.⁹

Reason for the PIA Update

CBP is updating the existing APIS¹⁰ PIA to account for the short-term, limited sharing of APIS data with IARPA and routine sharing enhancements: specifically, the appropriate hosting and controlled use of APIS data in a DHS-controlled classified environment via encryption and policy-based access rules. These enhancements will not alter the information sharing principles expressed in the APIS MOA or APIS NCTC PIA Update.¹¹ DHS has entered into a LOI with NCTC and IARPA in order to ensure that APIS data can be appropriately hosted and controlled in the classified cloud environment. DHS, NCTC, and IARPA have placed specific safeguards in the LOI to ensure that the data is used appropriately and in accordance with the existing SORN, DHS/CBP-005 Advance Passenger Information System System of Records.¹²

⁹ DHS/CBP/PIA-001(f) (June 23, 2011).

¹⁰ The existing DHS/CBP/PIA-001 APIS was first published on March 21, 2005, and updated subsequently on August 9, 2007, September 11, 2007, November 18, 2008, February 19, 2009, and June 23, 2011.

¹¹ DHS/CBP/PIA-001(f) (June 23, 2011).

¹² DHS/CBP-005 Advance Passenger Information System System of Records Notice (SORN), 80 FR 13407 (March 13, 2015), available at <https://www.federalregister.gov/articles/2015/03/13/2015-05798/privacy-act-of-1974-department-of-homeland-securityunited-states-customs-and-border-protection>.



Privacy Impact Analysis

The System and the Information Collected and Stored within the System

There is no change in the collection of APIS records.

Uses of the System and the Information

There are no changes to the uses of the information.

Retention

The DHS retention period for APIS has not changed. The information initially collected by APIS is used for traveler processing purposes and is retained in APIS for no more than twelve months.

Pursuant to the LOI, IARPA will retain APIS records for up to one year in order to test SPAR in support of the mission of DHS. The one year temporary retention period commences when DHS delivers the APIS information to IARPA. DHS will mark records with a “time-to-live” date, which will specify when the APIS information will be deleted from IARPA servers. NCTC will purge all APIS records queried from IARPA servers not determined to constitute terrorism information no later than the time-to-live date. This process will be audited as required under the LOI.

Internal Sharing and Disclosure

There are no changes for internal sharing and disclosure.

External Sharing and Disclosure

DHS entered into an LOI with NCTC and IARPA in order to test appropriate hosting and controlled use of APIS data in a DHS-controlled classified environment that would facilitate use as described in the APIS MOA. DHS entered into the APIS MOA with NCTC in order to facilitate NCTC’s counterterrorism efforts and to identify terrorism information within APIS. This sharing is conducted pursuant to routine use H of the APIS SORN,¹³ which states that DHS may share APIS information with “a federal, state, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive,” and routine use P of the APIS SORN, which states that DHS may share APIS information with “appropriate federal, state, local, tribal, or foreign

¹³ DHS/CBP-005 Advance Passenger Information System System of Records Notice (SORN), 80 FR 13407 (March 13, 2015), available at <https://www.federalregister.gov/articles/2015/03/13/2015-05798/privacy-act-of-1974-department-of-homeland-securityunited-states-customs-and-border-protection>.



governmental agencies or multilateral governmental organizations when CBP is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law.”

IARPA participants will not disclose APIS information nor remove it from a DHS-controlled environment. NCTC analysts may run queries against APIS information held in the IARPA servers hosted in a DHS-controlled Virtual Private Cloud (VPC). When APIS information is determined to constitute terrorism information, NCTC will include DHS on the distribution of the lead or finished intelligence product, so that DHS may use this information to support its mission to prevent and deter terrorist attacks. NCTC will review, retain, and disseminate APIS records it has determined to constitute terrorism information in accordance with procedures approved for NCTC by the Attorney General in accordance with Section 2.3 of Executive Order 12333,¹⁴ and additional terms specified in the APIS MOA.

The LOI is subject to the strict safeguards in the APIS MOA to protect PII provided to NCTC. These protections include training to be provided to NCTC users on the appropriate use of PII. DHS/CBP will provide annual and periodic training to appropriate NCTC personnel on the proper interpretation of the information contained in APIS and on the proper treatment of information from certain categories that require special handling, such as asylum and refugee information. The APIS MOA stipulates that NCTC may not disseminate to third parties information derived from APIS information, unless that information is identified as terrorism information.¹⁵ NCTC will maintain an electronic copy and accounting of the APIS information that is disseminated, including to whom the information is disseminated and the purpose for the dissemination. Additionally, the APIS MOA allows DHS to assign an on-site oversight representative to NCTC to provide intelligence, data stewardship, privacy, civil rights, and civil liberties oversight of the handling of DHS information by NCTC.

Notice

The APIS SORN was last published in the *Federal Register* on March 13, 2015¹⁶ and remains accurate and current. Routine Uses H and P cover this sharing.

¹⁴ Exec. Order No. 12333 United States Intelligence Activities, 46 Fed. Reg. 59941 (Dec. 4, 1981), available at <http://www.archives.gov/federal-register/codification/executive-order/12333.html>.

¹⁵ APIS may contain some information controlled by regulations related to asylum information. The MOA establishes procedures for NCTC’s dissemination of asylum information in APIS that has been identified as terrorism information.

¹⁶ DHS/CBP-005 Advance Passenger Information System System of Records Notice (SORN), 80 FR 13407 (March 13, 2015), available at <https://www.federalregister.gov/articles/2015/03/13/2015-05798/privacy-act-of-1974-department-of-homeland-security-united-states-customs-and-border-protection>.



Individual Access, Redress, and Correction

There are no changes to APIS access, redress, and correction procedures.

Technical Access and Security

There are no changes to technical access and security procedures for APIS.

Technology

There are no changes to APIS technology.

Responsible Officials

Robert Neumann
Office of Field Operations
U.S. Customs and Border Protection
U.S. Department of Homeland Security

John Connors
CBP Privacy Officer
U.S. Customs and Border Protection
U.S. Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office

Karen L. Neuman
Chief Privacy Officer
U.S. Department of Homeland Security