Privacy Impact Assessment Update
for the

Advance Passenger Information System (APIS)

DHS/CBP/PIA – 001(f)

June 5, 2013

Contact Point
Robert Neumann
Office of Field Operations
U.S. Customs and Border Protection
202-344-2605

Reviewing Official
Jonathan R. Cantor
Acting 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 the expansion in the National Counterterrorism Center (NCTC)'s "temporary retention" of APIS information due to the March 2012 release of the *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Data sets Containing Non-Terrorism Information* (AG Guidelines).

Introduction

The Aviation and Transportation Security Act of 2001 and the Enhanced Border Security and Visa Reform Act of 2002 together mandated the collection of certain information on all passenger 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 passenger and crew members must provide when being processed into or out of the United States. The APIS information includes full name, date of birth, citizenship, passport/alien registration card number, passport/alien registration card country of issuance, passport expiration date country of residence, passenger name record locator number, and U.S. destination address (when applicable). The 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 perform law enforcement queries and 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.

Pursuant to the National Security Act of 1947, as amended, the National Counterterrorism Center (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," 50 U.S.C. § 404o. In order to enhance information sharing, the President issued Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (October 27, 2005), 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 2004 (Pub. L. No. 108-458), as amended, places an obligation on U.S. government agencies to share terrorism information with the Intelligence Community (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 Understanding (MOU). In 2013, DHS and NCTC entered into a new Memorandum of Agreement (MOA) that supersedes the 2011 MOU and documents an expansion of routine sharing with NCTC. The MOA permits NCTC to use APIS information to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. The MOA includes a number of safeguards to ensure the data is only used for the purposes explicitly permitted under the MOA, this PIA, and the DHS/CBP-005 Advance Passenger Information System of Records Notice (SORN), 73 FR 68435, November 18, 2008.[1] The MOA also limits the amount of time the information is maintained at NCTC, ensures proper information technology security is in place during and after transmission of the APIS information to NCTC, requires training for staff accessing APIS, and provides for routine reporting and auditing of NCTC's use of the information.

Reason for the PIA Update

CBP is updating the existing DHS/CBP/PIA-001 APIS[2] to provide notice of an expansion in NCTC's 'temporary retention' of APIS information.[3] Under Executive Order 12333, *United States Intelligence Activities* (December 8, 1981), as amended, IC elements are required to have guidelines approved by the Attorney General of the United States for the collection, retention, and dissemination of information concerning United States Persons (U.S. Persons).[4] These guidelines outline temporary retention periods during which an IC element must determine whether it can continue to retain U.S. Person information, consistent with Executive Order 12333 and the purposes and procedures outlined in its guidelines.

---

[1] Available at: http://edocket.access.gpo.gov/2008/E8-27205.htm.
[2] 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.
[3] The purpose of this 'temporary retention' period is to allow NCTC sufficient time to determine whether the U.S. Person information it receives from other federal departments and agencies is terrorism information.
[4] NCTC's Guidelines use the definition of U.S. Person provided in Executive Order 12333, which states that a U.S. Person is "a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." *See* Executive Order 12333, Section 3.5(k).

In March 2012, the Attorney General of the United States approved *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Datasets Containing Non-Terrorism Information* (AG Guidelines).[5] These Guidelines establish an outside limit of five years for NCTC's temporary retention of U.S. Person information obtained from the datasets[6] of other federal departments and agencies. The purpose of this temporary retention period is to allow NCTC sufficient time to determine whether the U.S. Person information it receives from other federal departments and agencies is terrorism information.[7] The AG Guidelines allow NCTC to retain all information in the datasets it receives for the full temporary retention period,[8] whereby the information may be "continually assessed" against new intelligence to identify previously unknown links to terrorism.[9] NCTC may only retain U.S. Person information within such datasets beyond the temporary retention period if the information is "reasonably believed to constitute terrorism information."[10] In light of the new AG Guidelines, NCTC requested that DHS re-evaluate its information sharing and access agreements with NCTC, including the 2011 MOU to share APIS information.

The AG Guidelines preserve the Department's authority to negotiate with NCTC the terms and conditions of information sharing and access agreements relating to, among other things, "privacy or civil rights or civil liberties concerns and protections."[11] One such protection is the amount of time NCTC may retain DHS records that do not constitute terrorism information. With this in mind, DHS developed a Data Retention Framework of Factors to

---

[5] *See* NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

[6] In the context of DHS's information sharing relationship with NCTC, a "dataset" refers to a collection of information about a set of individuals that DHS has gathered during its routine interactions (e.g., screening travelers, reviewing immigration benefit applications, issuing immigration benefits) with the public. Consequently, DHS datasets contain information about individuals who have no connection to terrorism. A dataset may constitute all the records in a Privacy Act System of Records, or a portion of the records therein.

[7] NCTC's AG Guidelines use the statutory definition of "terrorism information" in Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, which states "the term 'terrorism information'—(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to: (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and (B) includes weapons of mass destruction information." 6 U.S.C. § 485(a)(5).

[8] As noted later in the PIA, the Guidelines allow departments and agencies to negotiate the terms and conditions of information sharing and access agreements. Through these negotiations, departments and agencies may establish temporary retentions period that are less than the five year outside limit established by the AG Guidelines. DHS's agreement with NCTC for APIS information establishes a temporary retention period of one year for reasons explained later in the PIA.

[9] *See* NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

[10] *See* NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

[11] *See* NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

determine appropriate temporary retention periods for DHS datasets on a system-by-system basis. This Framework includes factors related to the sensitivity of a dataset and operational considerations. Factors related to the sensitivity of a dataset include: the circumstances of collection, the amount of U.S. Person information in the dataset, and the sensitivity of the particular data fields (e.g., sensitive personally identifiable information) that are requested. Operational factors include: the mission benefits to DHS, the mission benefits to NCTC, and any limitations for the DHS data steward (e.g., DHS's own retention period for the dataset). Using the Data Retention Framework of Factors, DHS and NCTC agreed to a one year temporary retention period for all APIS information provided to NCTC. This temporary retention period matches DHS's own retention period for APIS information.

The 2013 MOA documents NCTC's expanded temporary retention period and augments the privacy protections of the 2011 agreement with NCTC. The MOA augments privacy protections related to transparency, redress, and oversight. To promote transparency, the MOA requires DHS and NCTC to develop public PIAs that provide notice regarding the existence and contents of the MOA and to cooperate to promote transparency through efforts such as joint presentations to Congress and the DHS Data Privacy and Integrity Advisory Committee. With respect to redress, the MOA requires NCTC to establish a redress mechanism for individuals whose PII has been retained as terrorism information. The redress process will direct any request for correction or redress to DHS for resolution, as appropriate. For any records corrected by DHS through this process, NCTC will correct those records in its possession when it receives a notification of the correction from DHS. To increase oversight, DHS and NCTC have refined the quarterly reporting requirements regarding NCTC's use and retention of the DHS information. Additionally, the 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.

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 entry screening purposes and is retained in APIS for no more than twelve months.

Pursuant to the MOA, NCTC will now be allowed to temporarily retain APIS records for up to one year in order to identify terrorism information, in support of its counterterrorism mission and in support of the mission of DHS. NCTC previously retained APIS records for 180 calendar days. The one year temporary retention period commences when DHS delivers the APIS information to NCTC. When NCTC replicates APIS information, the records will be marked with a "time-to-live" date, which will specify when the APIS information will be deleted if it is not identified as terrorism information. NCTC will purge all APIS records not determined to constitute terrorism information no later than one year from receipt of the record from DHS. This process will be audited as required under the MOA.

Since NCTC's AG Guidelines allow information to be "continually assessed" during the temporary retention period,[12] NCTC may retain all APIS information for one year, regardless of whether NCTC has made a terrorism information determination about a particular APIS record, as it is possible that new intelligence or terrorism information will identify previously unknown terrorism information within that APIS record. NCTC may retain APIS records determined to constitute terrorism information in accordance with NCTC's authorities and policies, applicable law, and the terms of the MOA.

Internal Sharing and Disclosure

No changes have been made to internal sharing.

External Sharing and Disclosure

DHS has entered into an updated MOA with NCTC in order to facilitate NCTC's counterterrorism efforts and to identify terrorism information within APIS. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. This sharing is conducted pursuant to routine use H of the APIS SORN, 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

[12] *See* NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

applicable national security directive."

A material condition for DHS's sharing APIS information with NCTC is that the sharing must provide real and ongoing value to both NCTC's and DHS's missions. NCTC replicates APIS information into its Counterterrorism Data Layer (CTDL) to support its counterterrorism efforts. The CTDL provides NCTC analysts "with the ability to search, exploit, and correlate terrorism information in a single environment."[13] For example, NCTC analysts may run queries against APIS information in the CTDL to identify terrorism information within APIS. 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, and additional terms specified in the MOA.

DHS/CBP/PIA – 001(e)[14] noted that "NCTC will process all APIS records within [the temporary retention period] to determine whether a nexus to terrorism exists." This requirement proved to be enormously challenging, and the parties have agreed in the updated MOA to continue exploring improved methods for creating a practicable solution to provide more direct support to DHS's mission to prevent and deter terrorist attacks. Within a year of its signature, the new MOA requires DHS and NCTC produce a joint report regarding the prioritization of screening, Terrorist Identities Datamart Environment (TIDE) enhancement, and the analytic initiatives that leverage NCTC's holdings and provide value to the Department and the Intelligence Community. DHS and NCTC will provide interim reports quarterly to the Deputy Secretary of Homeland Security, Director of NCTC, DHS Under Secretary for Intelligence and Analysis, DHS Chief Privacy Officer, DHS Officer for Civil Rights and Civil Liberties, the DHS General Counsel, and the Office of the Director of National Intelligence (ODNI) Civil Liberties Protection Officer.

The MOA has strict safeguards 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 MOA stipulates that NCTC may not disseminate to third parties information derived from APIS

---

[13] *See* "Information Sharing Environment Annual Report to the Congress: National Security Through Responsible Information Sharing," dated June 30, 2012. Available at: http:// http://ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2012.pdf.

[14] Published on June 23, 2011.

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 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 November 18, 2008, 73 FR 68435, and remains accurate and current. Routine Use H covers this sharing.

Individual Access, Redress, and Correction

No changes have been made to access, redress, and correction procedures. However, CBP is updating the address to which individuals should submit their requests for access, redress, and correction.

DHS allows persons, including foreign nationals, to seek administrative access under the Privacy Act to certain information maintained in APIS. Requests for access to PII contained in APIS that was provided by the commercial air or vessel carrier or private pilot regarding the requestor may be submitted online at: https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002
Fax Number: (202) 325-0230

Technical Access and Security

No changes.

[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.

Technology

No changes.

Responsible Officials

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

Laurence Castelli
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

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. Department of Homeland Security