Privacy Impact Assessment Update
for the

Arrival and Departure Information System – Information Sharing Update

DHS/CBP/PIA – 024

March 7, 2014

Contact Point
Matt Schneider
Assistant Director,
DHS/CBP/OFO/PPAE Entry/Exit Transformation Office
Dr. Kenneth N. Clark
Director
DHS/I&A/Information Sharing and Intelligence Enterprise

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)[1] is updating the Privacy Impact Assessment (PIA) for the Arrival and Departure Information System (ADIS) last published on August 1, 2007, to provide notice of a change in the National Counterterrorism Center's (NCTC) temporary retention of ADIS information to three years for U.S. Person information and 10 years for non-U.S. Person information due to the March 2012 approval of *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Data sets Containing Non-Terrorism Information (2012 NCTC AG Guidelines).*

Overview

ADIS is a system that aggregates certain records from a number of border crossing and immigration systems. It was created to identify individuals who were lawfully admitted to the United States but subsequently overstayed their permission to remain. This is accomplished by tracking entry and exit encounters during a variety of DHS's interactions with the public, such as the immigrant and non-immigrant pre-entry, entry, and exit processes. Specifically, DHS aggregates filtered data from CBP Nonimmigrant Information System (NIIS),[2] Advanced Passenger Information System (APIS),[3] CBP Border Crossing Information System (BCI),[4] CBP TECS,[5] U.S. Immigration and Customs Enforcement (ICE) Student Exchange Visitor Information System (SEVIS),[6] U.S. Citizenship and Immigration Services (USCIS) Computer Linked Information Management System (CLAIMS 3),[7] NPPD/OBIM Automated Biometric Identification System (IDENT),[8] and other data that is relevant to the Department's overstay mission and as described in more detail in the general ADIS PIA.[9]

---

[1] The Arrival Departure Information System (ADIS) transitioned from National Protection and Programs Directorate (NPPD), Office of Biometric Identity Management (OBIM) to Customs and Border Protection (CBP) on Saturday January 18, 2014. The functionality remains the same, but ownership of the program and technology has shifted.
[2] DHS/CBP-016 - Nonimmigrant Information System (NIIS), December 19, 2008, 73 FR 77739.
[3] DHS/CBP/PIA – 006 Advanced Passenger information System (APIS) and DHS/CBP-005 - Advance Passenger Information System (APIS), November 18, 2008, 73 FR 68435
[4] DHS/CBP/PIA – 009 TECS System: CBP Primary and Secondary Processing (TECS) and DHS/CBP-007 Border Crossing Information (BCI) System of Records, July 25, 2008, 73 FR 43457
[5] DHS/CBP/PIA – 009 TECS System: CBP Primary and Secondary Processing (TECS) and DHS/CBP-011 - U.S. Customs and Border Protection TECS, December 19, 2008 73 FR 77778
[6] DHS/ICE/PIA – 001 Student and Exchange Visitor Information System (SEVIS) and DHS/ICE-001 Student and Exchange Visitor Information System, January 5, 2010, 75 FR 412
[7] DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) and DHS/USCIS-007 Benefits Information System, September 29, 2008, 73 FR 56596.
[8] DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) and DHS/NPPD-004 DHS Automated Biometric Identification System (IDENT), June 5, 2007, 72 FR 31080
[9] DHS/NPPD/PIA-005 Arrival and Departure System (ADIS) and DHS/NPPD-001 Arrival and Departure Information System (ADIS) May 28, 2013, 78 FR 31955.

DHS uses ADIS to collect arrival and departure records and statuses of all aliens traveling to and from the United States, including information on Lawful Permanent Residents (LPRs), Refugees, and Asylees. ADIS data may also be used in connection with issuing certain DHS credentials, such as trusted traveler cards.

Terrorism Information Sharing.

NCTC "serve[s] as the central, 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."[10]

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004[11] requires U.S. government agencies, including DHS, to share Terrorism Information with the Intelligence Community (IC), including NCTC. To enhance information sharing among federal agencies, the President issued Executive Order[12] 13388 (EO 13388) in 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. In certain instances, DHS shares an entire dataset (or a substantial subset thereof) with NCTC (or other IC partners), so NCTC can identify Terrorism Information within DHS data to support its counterterrorism activities.

Executive Order 12333 (EO 12333)[13] requires that IC elements have guidelines approved by the United States Attorney General (AG) for the collection, retention, and dissemination of information concerning United States Persons (U.S. Persons).[14] These AG-approved guidelines typically outline temporary retention periods during which an IC element must determine whether it can continue to retain U.S. Person information, consistent with EO 12333 and the purposes and procedures outlined in the guidelines.

In 2010, consistent with EO 13388 and the IRTPA, DHS began sharing the entire ADIS dataset with NCTC for counterterrorism purposes under a Memorandum of Understanding (MOU). At that time, NCTC was operating under AG-approved guidelines from November 2008,[15] which permitted NCTC to retain U.S. Person information for no longer than 180 days.

---

[10] National Security Act of 1947, as amended, 50 U.S.C. § 3056.
[11] Pub. L. No. 108-458, 118 Stat. 3638 (2004), as amended, 6 U.S.C. § 485.
[12] Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (October 27, 2005).
[13] Executive Order 12333, *United States Intelligence Activities*, as amended (Dec. 4, 1981).
[14] 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).
[15] For information on the 2008 NCTC AG Guidelines, please see the "Background and Summary" section of "Information Paper: Description of Civil Liberties and Privacy Protections Incorporated in the Updated NCTC

Under the 2010 Agreement, DHS allowed NCTC to retain non-U.S. Person information for 75 years.

In March 2012, pursuant to EO 12333, the Attorney General approved updated *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Datasets Containing Non-Terrorism Information* (2012 NCTC AG Guidelines).[16]

The 2012 NCTC AG Guidelines establish an outside limit of five years for NCTC's temporary retention of U.S. Person information obtained from the datasets of other federal departments and agencies, including datasets that have no apparent association with derogatory data about an individual. The purpose of this retention period is to allow NCTC to continually assess the information that NCTC holds to determine if it constitutes Terrorism Information, including identifying connections among pieces of data that may have previously been unrecognized or unknown.[17]

In this context, a "dataset" refers to information about a set of individuals that DHS has gathered during its routine interactions with the public[18] (e.g., screening international travelers at the border, reviewing immigration benefit applications, and issuing immigration benefits or other credentials). Many DHS datasets contain information about individuals who may have no connection to terrorism. The 2012 NCTC AG Guidelines preserve DHS's authority to negotiate with NCTC the terms and conditions of information sharing and access agreements, concerning, among other things, "privacy or civil rights or civil liberties concerns and protections." One of these protections about minimizing the length of time NCTC may retain and continually assess DHS records that have not been previously identified as Terrorism Information.

Under the 2012 NCTC AG Guidelines, NCTC is authorized to retain U.S. Person information within these datasets beyond the temporary retention period only if the information

---

Guidelines," dated January 2013, from the Civil Liberties and Privacy Office of the Office of the Director of National Intelligence. Available at: http://www.nctc.gov/docs/CLPO_Information_Paper_on_NCTC_AG_Guidelines012213.pdf.

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

[17] *See id.* at p. 9. NCTC's AG Guidelines use the definition of "Terrorism Information" set forth 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).

[18] More generically, a dataset may constitute all the records in a Privacy Act System of Records, or a portion of the records therein.

is "reasonably believed to constitute terrorism information."[19] Information may be "continually assessed" against new intelligence, including derogatory information from other parts of the IC, or data that was previously perceived to be unconnected, to identify previously unknown links to terrorism.[20] This can occur when an analyst (1) queries NCTC's data holdings and retrieves ADIS information responsive to the query or (2) reviews and confirms potential matches between ADIS and derogatory data that are generated through the automated comparison of ADIS data with NCTC's holdings.

As a result of the 2012 NCTC AG Guidelines, NCTC asked DHS to re-evaluate all of its information sharing and access agreements, including the retention periods in the 2010 MOU, to allow NCTC to retain U.S. Person information for longer than 180 days.

The Revised DHS-NCTC Information Sharing Agreement.

In undertaking this re-evaluation, the Department adopted a retention framework (Framework) that considered the datasets as a whole. This approach included assessing the sensitivity of each dataset and its operational purpose. Factors related to sensitivity include the circumstances of collection, the amount of U.S. Person information in the requested dataset, and the sensitivity of Personally Identifiable Information (PII) in the dataset. Operational factors include the mission benefits to DHS and NCTC, and limitations on the use and retention of the data faced by DHS (e.g., DHS's own retention period for the dataset).

The Department identified several privacy risks that emerged as a result of a better understanding of ADIS's mission-driven capabilities and limitations and in light of information sharing under the 2010 MOU. Specifically, the Department determined that U.S. Person information might be retained by NCTC or the IC longer than allowed under the revised AG Guidelines because (1) ADIS may not accurately differentiate U.S. Person information from non-U.S. Person information, and (2) immigration status may change over time, but these changes may not be recorded in ADIS or transmitted to NCTC. Using the Framework, the Department concluded that a unified temporary retention period of less than five years would mitigate this risk. Accordingly, DHS approved a retention schedule for U.S. and non-U.S. Person information that increased from 180 days to two years for U.S. Person data and decreased to two years from 75 years for non-U.S. Persons.

After further consideration, the Department approved a bifurcated retention period of three years for U.S. Person information and 10 years for non-U.S. Person information, along with a number of safeguards, privacy protections, and oversight requirements. An updated Memorandum of Agreement (MOA) with NCTC was executed on November 25, 2013. The MOA incorporates the new retention periods described above and imposes the following safeguards, privacy protections, and oversight requirements:

[19] *See* NCTC's AG Guidelines at 9.
[20] *See* NCTC's AG Guidelines at 9.

- In order for DHS to fulfill its oversight role, NCTC will provide access to information concerning any and all uses of DHS data by NCTC;
- NCTC will develop and implement the technical capability to receive real-time status updates from ADIS, as soon as practicable but no later than two years from the effective date of the MOA;
- DHS will conduct a formal review of NCTC's data stewardship two years from the effective date of the MOA; and
- Any gross compromise of NCTC data stewardship will constitute grounds for rescission of the MOA.[21]
- DHS and NCTC will provide appropriate public notice about the existence and contents of the MOA, including jointly developing a PIA on the overarching bulk information sharing relationship between DHS and NCTC no later than one year from the effective date of MOA. DHS and NCTC will also cooperate to promote transparency through joint presentations to Congress and the DHS Data Privacy and Integrity Advisory Committee (DPIAC).
- NCTC will use its Information Sharing Environment (ISE) Privacy Guidelines Redress Process for individuals whose PII has been retained as Terrorism Information in ADIS. This process will direct any request for correction or redress of those records to DHS for resolution. Should DHS correct any records, it will notify NCTC. NCTC must, upon receipt of notification, correct those records in its possession.
- NCTC staff must complete training on privacy and ADIS information as a prerequisite to receiving and maintaining access to ADIS. Both DHS and NCTC will ensure that their employees, including contractors, have completed privacy training on the handling of PII. DHS will provide annual and periodic training requirements to NCTC on the proper interpretation of ADIS information and the treatment of information regarding Special Protected Classes, including, but not limited to, Refugees, Asylees, and individuals subject to the protections of 8 U.S.C. § 1367. NCTC staff must complete the training within six months of its implementation or they will lose access to ADIS information until such time as they have completed the training. NCTC staff with access to ADIS information will complete refresher training on ADIS, Special Protected Classes, and U.S. Person information on an annual basis to retain access to ADIS information.
- NCTC may not forward any ADIS data unless it has been determined to be Terrorism Information and the information is only being shared with other appropriate United States Government authorities for counterterrorism purposes.

These safeguards, privacy protections, and oversight requirements are conditions for

[21] "Memorandum of Agreement Between the Department of Homeland Security and the National Counterterrorism Center Regarding Arrival and Departure Information System Data," effective November 25, 2013.

NCTC's use of ADIS data. They are intended to ensure that the information is only used for the counterterrorism purposes explicitly permitted under the MOA and in a manner that is consistent with this PIA and the DHS/NPPD-001 ADIS System of Records Notice (SORN).[22]

In light of the foregoing changes, this PIA updates the DHS/NPPD/PIA-005(a) ADIS PIA last published on August 1, 2007 and with the transition to CBP the PIA will be renumbered to DHS/CBP/PIA-024.

Privacy Impact Analysis

Authorities and Other Requirements

The 2012 NCTC AG Guidelines that were issued under EO 12333 changed the temporary retention of U.S. Person information from 180 days to up to five years.

Characterization of the Information Collected and Retained in ADIS

ADIS is a "mixed system" because it consists of data collected and aggregated from Non-U.S. and U.S. Persons. The information is collected during DHS's routine interactions with the public, including the screening of international travelers at the border, and issuance of immigration benefits or other credentials.

Privacy Risk.

- *NCTC Might Retain Data on U.S. Citizens Longer than Permissible under EO 12333 Because ADIS May Inadvertently Retain and Store Data about U.S. Citizens.*

There is a risk that ADIS might inadvertently retain data about U.S. Citizens. To mitigate this risk, CBP has several filters in place to prevent known U.S. Citizen ("Known U.S. Citizen") information from being ingested into ADIS. Known U.S. Citizens are identified by a U.S. passport, naturalization certificate, or indicia of a class of admission associated with U.S. citizenship in their travel records. In addition to these first line filters, the ADIS Program uses supplemental filters to ensure that information about U.S. Citizens that may have inadvertently entered into the ADIS production database is removed. The ADIS program further monitors ADIS transmissions for U.S. Citizens and removes them when the ADIS program is aware of their status, e.g., if another travel event occurs during which the individual presents a document associated with being a Known U.S. Citizen.

There may be instances, however, when a U.S. Citizen may not be correctly identified as a U.S. Citizen when his or her information is sent to and stored in ADIS. This can occur, for example, if a U.S. Citizen presents an approved travel document other than – or in addition to – a U.S. Passport or naturalization certificate when entering the country (e.g., a pilot's license, a trusted traveler credential, military identification, or merchant mariner identification).

[22] May 28, 2013, 78 FR 31955

Alternatively, ADIS may receive a document number without a document type and/or country of issuance, which thereby prevents ADIS from being able to accurately differentiate between U.S. and non-U.S. Citizens.

In these instances, there is a risk that U.S. Citizen information will be recorded in ADIS as non-U.S. Person data, and these individuals may not be afforded the privacy protections contemplated by EO 12333, the 2012 NCTC AG Guidelines, and DHS policy, including a shortened temporary retention by NCTC. As a result, there is a risk that the data could become stale, misused, misinterpreted, or unintentionally disclosed, creating a greater chance that the individual will be incorrectly linked to terrorism.

This risk is mitigated when DHS personnel examine each ADIS data delivery for new evidence of Known U.S. Citizens. For example, if an individual has a new travel event that shows he or she is a Known U.S. Citizen, then his or her information will be removed from both the historical ADIS data transmitted to NCTC and from ADIS. If the documents do not indicate an individual's U.S. Citizen status, then NCTC will retain the records for 10 years.

Privacy Risk.

- *NCTC Might Retain Data on a U.S. Person or Special Protected Class Alien Longer than Permissible Because ADIS Does Not Reflect an Individual's Changed or Adjusted Status.*

There is a risk that ADIS might retain data longer than is permissible due to ADIS's inability to reflect an individual's updated status as a Refugee, Asylee or U.S. Citizen. ADIS was created to identify individuals who may have overstayed their lawful period of admission to the United States. It collects and stores arrival and departure information on foreign nationals traveling to the U.S. and generates overstay status updates for each traveler. ADIS consolidates data from several DHS immigration systems and uses that data to match events to a unique person. By matching data from the source systems, ADIS creates a comprehensive record of immigration-related events during a visit and closes out each trip into and out of the United States.

ADIS is not notified when an individual becomes a Refugee, Asylee, or U.S. Citizen. Consequently, that person's status as a U.S. Person or Special Protected Class alien (e.g., a Refugee or Asylee) -- particularly as it changes over time -- may not be accurately reflected in ADIS. As a result, there is a risk that records pertaining to these individuals, which may include sensitive information about the subjects of the records, will be exposed to prolonged retention and continual assessment by the IC. For example, if the LPR has an "Open Arrival" ADIS will retain the notification in the database, which will close the travel event and indicate that the LPR is not a potential overstay. If the LPR does not have an "Open Arrival," ADIS will not retain the notification because the LPR would not be treated as potentially having overstayed his or her visit. Under the circumstances, ADIS may inadvertently share this U.S. Person information with

NCTC without identifying the U.S. Person status of the record, thereby allowing NCTC to retain and continually assess the record for 10 years.

The risk associated with adjusted status for LPRs and Special Protected Class aliens is mitigated by supplemental filters ADIS uses for sharing bulk information with the IC. The filters search for LPR or Special Protected Class alien information by using indicia of status – such as a Permanent Resident Card (a/k/a Green Card) or other document type, class of admission, or membership on a USCIS-provided list of individuals who are protected by statute.[23] The filters implement a "whole person" concept, under which ADIS searches for any record that would suggest an individual is a U.S. Person or Special Protected Class alien, regardless of when a travel event occurred, and updates the individual's status. These supplemental filters also remove Known U.S. Citizen information from ADIS data transmitted in bulk to the IC if that information was not already removed from the ADIS production database.

Risk is further mitigated by NCTC's data updates, which are based on the results of ADIS's supplemental filters. As noted, with each data delivery to NCTC, ADIS updates an individual's status based on all of the information available in the ADIS production database. If there is new information in the ADIS production database to indicate that an individual has become a U.S. Person or Special Protected Class alien, then DHS will notify NCTC to change the individual's status in its holdings as well. NCTC is then required to adjust each ADIS record that has not been deemed Terrorism Information associated with the individual to three years from the date that each of the records was provided to NCTC.

The Department will re-evaluate the extent to which the filters and other technology at DHS and NCTC fully mitigate this risk.

Changes to DHS's Uses of the Information

ADIS data is being used for counterterrorism purposes under both the 2010 MOU and 2013 MOA. The 2012 NCTC AG Guidelines explicitly allow NCTC to "continually assess" the data for the full temporary retention period. Accordingly, non-U.S. Person data might be continually assessed for 10 years.

Privacy Risk.

- *Prolonged Retention of ADIS Data by NCTC Increases the Risk that Information About U.S. Persons and Special Protected Class Aliens Will Be Continually Assessed Beyond the Period that is Authorized Under the 2012 NCTC AG Guidelines and DHS Policy.*

The MOA permits NCTC to retain U.S. Person data for three years and non-U.S. Person data for 10 years. Due to the characteristics of the ADIS system, as discussed above, there is a

[23] 8 U.S.C. § 1367.

risk that the 10 year temporary retention period for non-U.S. Person information will result in the continual assessment of some U.S. Citizens for 10 years. Likewise, if an LPR is not identified as a U.S. Person, his or her information may be continually assessed for 10 years. The authority to retain and continually assess ADIS data beyond the time NCTC initially compared ADIS data to its derogatory counterterrorism holdings could subject individuals to long-term monitoring for terrorism links.

To mitigate this risk, when NCTC replicates ADIS information, the records will be marked with a "time-to-live" date, which will specify when the ADIS information will be deleted if it is not identified as Terrorism Information. NCTC will purge all ADIS records for U.S. Persons, Refugees, and Asylees that are not determined to constitute Terrorism Information no later than three years from the day after the receipt of the records from DHS. NCTC will purge all other ADIS records not determined to constitute Terrorism Information no later than 10 years after the receipt of the records from DHS. All ADIS records collected under the previous information sharing agreements with NCTC will be brought in line with these new retention periods.

Furthermore, DHS conditioned its provision of the ADIS dataset to NCTC on several privacy-enhancing conditions. NCTC must accept a DHS-assigned on-site oversight representative to monitor NCTC's data handling and stewardship and adherence to privacy, civil rights, and civil liberties protections. This representative will coordinate his or her activities with the Office of the Director of National Intelligence's Civil Liberties and Privacy Office and Office of the General Counsel, as appropriate. NCTC will provide this oversight representative with access to information concerning any and all uses of DHS data by NCTC in order to allow the oversight representative to fulfill this oversight role. Two years from the date the MOA is effective, the DHS representative will commence a formal review of NCTC stewardship of DHS datasets and complete a written report documenting the findings and results of that review.

Notice

This PIA provides notice of the changes in DHS's sharing relationship with NCTC and NCTC's retention of ADIS data. As required by the MOA, DHS and NCTC will also develop a joint PIA on the overarching bulk sharing relationship between DHS and NCTC within a year of the MOA's effective date.

Privacy Risk.

- *Individuals are Unaware of the Sharing with the IC.*

This risk is mitigated through the publication of this PIA. Additionally, the existing system of records notice for ADIS has a routine use that supports this sharing. This risk is also mitigated by the requirements that the Department publish a joint PIA with NCTC over the next year, conduct joint briefings to Congress and DHS's DPIAC, and issue a report on sharing efforts at the conclusion of the initial two-year MOA.

Retention

The DHS retention period for ADIS data has not changed. However, the NCTC temporary retention periods for ADIS data have changed.

Under the 2010 MOU between NCTC and DHS, NCTC previously retained ADIS records for U.S. Persons, Refugees, and Asylees for 180 calendar days and other ADIS records for 75 years.

Under the 2013 MOA, NCTC is permitted to temporarily retain ADIS records for U.S. Persons, Refugees, and Asylees for three years. Although Refugees and Asylees are not included among the definition of U.S. Persons under EO 12333, the safeguarding and disclosure of this information is controlled by regulations and DHS policy. Therefore, NCTC's temporary retention of Refugee and Asylee information in ADIS is limited to three years. All other ADIS records are retained for 10 years to identify Terrorism Information in support of NCTC's and DHS's counterterrorism missions.[24]

The new retention periods commence the day after DHS delivers the ADIS information to NCTC.

Privacy Risk.

- *Bifurcated Retention Periods for U.S. Person and Non-U.S. Person Increase the Likelihood a Misidentified U.S. Person will be Retained Beyond the Period that is Authorized Under the 2012 NCTC AG Guidelines and DHS Policy.*

The reduction in retention from 75 years to 10 years for non- U.S. persons reduces this privacy risk. However, the bifurcated retention periods create a risk that information about U.S. Persons who were incorrectly identified as non-U.S. Persons will be held at NCTC and continually assessed for 10 years

To mitigate this risk, DHS uses the filters described above to reduce the number of misidentified individuals. DHS will continue to develop and improve upon these filters as feasible. DHS will also assess the impact of data quality on the sharing agreement at two years to determine whether improved technology can assist in identifying U.S. Person information so it is not retained for the full 10 years.

Information Sharing

DHS has entered into an information sharing MOA with NCTC under which DHS will share ADIS data to facilitate NCTC's counterterrorism efforts and to identify Terrorism

[24] Certain records subject to 8 U.S.C. § 1367 are subject to additional retention restrictions under DHS policy.

Information within ADIS. This information sharing is undertaken in support of DHS's mission to prevent and deter terrorist attacks pursuant to routine use H of the ADIS SORN.

Routine use H authorizes DHS to share ADIS information with "Federal, state, local, tribal, foreign or international government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure." The sharing will be evaluated as part of the MOA's auditing and reporting requirements to ensure that it provides real and ongoing value to both NCTC's and DHS's missions.

Within a year of its effective date, the MOA requires DHS and NCTC to produce a joint report regarding ways to enhance the value of this information sharing to the Department and the IC. DHS and NCTC will provide quarterly interim reports 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 contains strict safeguards and privacy protections. These protections include (1) DHS-provided training to NCTC users about the appropriate use of DHS PII; (2) DHS-provided annual and periodic training to appropriate NCTC personnel about the proper interpretation of the information contained in ADIS and the proper treatment of information from certain categories of information that require special handling, such as asylum and refugee data; and (3) the requirement that NCTC maintain an electronic copy and accounting of the ADIS information that is disseminated to other members of the IC, including to whom the information is disseminated and the purpose for the dissemination.

In addition, the MOA prohibits NCTC from disseminating information derived from ADIS information to third parties unless that information is identified as Terrorism Information.

Redress

There are no changes to DHS's redress procedures.

Auditing and Accountability

An on-site DHS Privacy Office representative will conduct oversight of NCTC's retention of DHS information and provide recommendations as appropriate in connection with the MOA's auditing and accountability requirements. Further, NCTC will invest in the capability to receive real-time status updates from ADIS within two years. A formal review of NCTC's stewardship of DHS data will take place at the end of two years. Any gross compromises of NCTC's stewardship are grounds for rescission of the agreement.

Responsible Official

Matt Schneider
Assistant Director,
DHS/CBP/OFO/PPAE Entry/Exit Transformation Office

Dr. Kenneth Clark
Director, Information Sharing and Intelligence Enterprise
Intelligence and Analysis
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security