Privacy Impact Assessment
for the

Data Analysis System
(DAS)

DHS/ICE DAS/PIA-048

September 29, 2017

Contact Point
Patrick F. Gannon
National Criminal Analysis and Targeting Center
Office of Enforcement and Removal Operations
U.S. Immigration and Customs Enforcement
(802) 657-4606

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Data Analysis System (DAS) is an analytical database owned, operated, and maintained by the U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO). The National Criminal Analysis and Targeting Center (NCATC), located within ERO's Targeting Operations Division, uses DAS to assist ERO field offices in locating aliens convicted of criminal offenses and other aliens who are amenable to removal. DAS was first deployed in 2006 and a discussion of the system was included in the Privacy Impact Assessment (PIA) for the Fugitive Case Management System (FMCS), which has been dispositioned.[1] ICE is publishing this PIA to describe the personally identifiable information (PII) within DAS and the way in which the NCATC uses the database. ICE will retire the FCMS PIA with the publication of this PIA.

Overview

ICE enforces the nation's civil immigration laws by apprehending and removing aliens who are amenable to removal. Individuals who are amenable to removal are those who are unlawfully present in the United States or those once lawfully present who have been convicted of crimes that render them removable. In support of the Agency's immigration enforcement mission, ICE's NCATC uses DAS, along with other technical and knowledge-based capabilities, to generate comprehensive, actionable, and timely leads, called "Information Referrals." ERO and others with immigration enforcement authorities pursuant to Section 287 of the Immigration and Nationality Act (INA)[2] (*e.g.*, certain state and local law enforcement officers) use these Information Referrals to assist in identifying and locating aliens who are amendable to removal.

DAS Data

DAS resides on an encrypted server behind ICE's firewall and compiles and stores dataset extracts from various DHS and non-DHS sources, thereby allowing for the efficient and effective analysis of data. These data sources include: ICE's Enforcement Integrated Database (EID), the U.S. Citizenship and Immigration Services (USCIS) Computer Linked Application Information Management System 3 (CLAIMS 3), the USCIS Central Index System (CIS), the Federal Bureau of Prisons (BOP) SENTRY System, the Federal Bureau of Investigation (FBI) Interstate Identification Index (III), and the California Department of Corrections and Rehabilitation (CDCR) Strategic Offender Management System (SOM), and publicly available data from two commercial sources.[3] ICE has entered into information access agreements and arrangements to

[1] *See* DHS/ICE/PIA-009 Fugitive Case Management System (FCMS), *available at* www.dhs.gov/privacy.
[2] Section 287 of the INA (8 U.S.C. § 1357) describes the authorization of immigration officers and employees.
[3] For reference, the Privacy Impact Assessments for these systems may be found at the locations below:

- *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, *available at* receive data from the non-DHS sources listed below in Question 2.2. The datasets contain a variety of categories of information including: biographical information, criminal history, immigration history, custody data (immigration and criminal), case history (immigration and criminal), immigration benefit information, naturalization information, and vehicle and insurance information. They are routinely obtained from each source via scheduled batch jobs, manual extracts, or responses to requests for information (in the case of open source data from a commercial vendor with which the NCATC has a contract), and each dataset uploaded into DAS. The previous dataset from each source is fully replaced with every update to ensure DAS contains the most current information available. Each dataset remains separate and distinct within DAS, and data elements are pulled together to populate Information Referrals in response to searches entered by DAS users.

The data within DAS is primarily about aliens; however, information about U.S. citizens may be included in some datasets. The presence of U.S. citizen information in DAS occurs when the source of the dataset does not maintain or is otherwise unable to provide NCATC with the citizenship status of the individuals within the dataset. For example, DAS contains a dataset from the BOP that contains biographic and criminal custody information about inmates in federal prisons who are foreign-born, but may or may not be United States citizens. This dataset does not include the inmate's citizenship status and, in some cases, foreign-born inmates may be U.S. citizens. NCATC employees attempt to verify the citizenship status of all individuals during their analysis by searching against data from other U.S. Department of Homeland Security (DHS) databases (*e.g.*, CIS) to which they have access. If individuals are confirmed to be U.S. citizens or their status cannot be confirmed, ERO does not pursue enforcement action against them.

DAS also contains the names and geographical areas of responsibility (AOR) of certain ERO officers who are the NCATC points of contact (POC) within the AORs. NCATC Management and Program Analysts (Analysts) who have full read and edit access to DAS input the names and AORs into a separate table in DAS. DAS pulls information from this table to ensure leads for specific AORs are provided to the correct points of contact.

www.dhs.gov/privacy.

- *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* www.dhs.gov/privacy.
- *See* DHS/USCIS/PIA-009(a) Central Index System (CIS), *available at* www.dhs.gov/privacy.
- *See* Bureau of Prisons SENTRY System PIA, *available at* http://www.bop.gov/foia/sentry.pdf.
- See Federal Bureau of Investigation Fingerprint Identification Records System (FIRS), Integrated Automated Fingerprint Identification System (IAFIS) which includes the Interstate Identification Index (III), *available at* https://www.fbi.gov/foia/privacy-impact-assessments/firs-iafis.

The California Department of Corrections and Rehabilitation is a state entity and is therefore not subject to Section 208 of the E–Government Act of 2002 (P.L. 107-347) which requires federal agencies to complete Privacy Impact Assessments. Records maintained by the California Department of Corrections and Rehabilitation are available for inspection pursuant to procedures located here: http://www.cdcr.ca.gov/News/CPRA.html. Additional information about the Strategic Offender Management System may be found here: http://www.cdcr.ca.gov/SOMS/index.html.

DAS Users

DAS access is limited to only certain ERO employees assigned to work for or oversee the NCATC. NCATC Analysts are the primary DAS users. Analysts query DAS using a single known identifier (*e.g.*, name, alien number) and using scripts they have written that enable them to retrieve and analyze information based on multiple factors. They are also able to manually input ERO officer and AOR data as described in the previous section, and edit DAS for formatting purposes. For example, if a dataset contains an alien number (A-Number) that does not have leading zeros, an Analyst will add the leading zeros to complete the A-Number so that it is a static 9-digit number.

NCATC Detention and Deportation Officers (DDO) have read-only access to DAS. DDOs serve as liaisons between the ERO field offices and the NCATC by providing ready assistance in response to field requests that do not require the more extensive analysis the Analysts provide, and by delivering the Information Referrals Analysts generate to the ERO field offices. DDOs are able to search DAS data by inputting a limited set of known identifiers about an alien, such as an A-Number, FBI Universal Control Number, or name. Using an existing Excel script, DDOs use these identifiers either independently or in combination, depending upon the data available to them, to query DAS for associated records. DAS returns a standard set of results based on the information in the query.

DAS Analysis & Information Referrals

NCATC Analysts access DAS through Single Sign-On (SSO) with Personal Identity Verification (PIV)-card authentication. Once Analysts use their PIV-cards to access the ICE network, they are able to access DAS. Once logged into DAS, Analysts develop customized queries (*i.e.*, scripts) to pull data from the various datasets within DAS for analysis. These scripts enable Analysts to support ERO field office requests for information when there are limited identifiers. For example, a field office may request information on all aliens within its AOR who are out of status and, therefore, amenable to removal. Analysts write a script to search DAS for all aliens who are out of status and whose last known address contains the zip code(s) within that AOR. Analysts use the results to populate Information Referrals in a spreadsheet or word processing template. The Information Referrals are not stored within DAS; they are saved on local, access-controlled ICE network file servers that are dedicated to the NCATC. Access to Information Referrals is controlled by ICE network permissions based on the individual's user account and job role within the NCATC. ICE intends to retain the Information Referrals for three (3) years. An Information Referral can be tailored to include or exclude data elements within DAS based on the query criteria the Analyst uses. At a minimum, these referrals contain biographic information, last known address, and the source and date of the last known address.

A typical transaction involving an Information Referral is as follows: An ERO field office point of contact (POC) will email the NCATC with a list of A-Numbers of recently paroled aliens in a certain state in an effort to identify which of them are amenable to removal. The Analyst will run a query in DAS using the A-Numbers provided and import the results into a spreadsheet. The Analyst then reviews the query results and runs additional queries in DAS for additional useful data – for example, identifying individuals who are already in ICE custody – that would eliminate the need for the field office to take further action. The Analyst notes these factors in the Information Referral and saves it to the NCATC server. The DDO for the requesting AOR reviews the Information Referral and delivers it via email to the requesting field office. The ERO field office uses the Information Referral as a starting point and conducts additional research to verify that the information provided is still current (*e.g.*, status, address, applicability of immigration benefits) based on other resources available to the field offices before determining whether to take any action.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

DHS has been authorized to collect information for this project pursuant to the following authorities: 8 U.S.C. § 1103; 8 U.S.C. § 1225; 8 U.S.C. § 1226; 8 U.S.C. § 1324; 8 U.S.C. § 1360(b); 8 U.S.C. §§ 1365a; 1365b; and the Illegal Immigration Reform and Immigrant Responsibility Act of 1996[4].

Pursuant to the Homeland Security Act of 2002 (Pub. L. No. 107-296, Nov. 25, 2002), the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include, but are not limited to, laws residing in Titles 8, 18, 19, 21, 22, 31, and 50 of the U.S. Code. The Secretary delegated this authority to ICE in DHS Delegation Number 7030.2, Delegation of Authority to the Assistant Secretary for the Bureau of Immigration and Customs Enforcement and the Reorganization Plan Modification for the Department of Homeland Security (January 30, 2003).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The information in DAS derived from EID, the ERO officer and AOR information, the publicly available information received from commercial sources, and the Information Referrals created using DAS are all covered by the Criminal Arrest Records and Immigration Enforcement Records (CARIER) system of records notice (SORN).[5]

[4] Pub. L. 104-208, 110 Stat 3009-546, Sep. 30, 1996.

[5] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (Oct. 19 2016).

The information that DAS receives from other federal systems is covered by the SORNs for those source systems, as follows:

USCIS CLAIMS 3 – Alien File, Index, and National File Tracking SORN[6]; Background Check Service SORN[7]; and Benefits Information System SORN[8]

USCIS CIS – Alien File, Index, and National File Tracking SORN

BOP SENTRY – Inmate Central Records System SORN[9]

FBI III – National Crime Information Center SORN[10]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. DAS has a system security plan in place. On July 25, 2013, DAS was granted an Authority to Operate by the ICE Office of the Chief Information Officer. DAS is in the ongoing authorization program and approved every year through the Tailored Risk Assessment Report.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. ICE is in the process of scheduling DAS records.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information stored in DAS is not covered by the Paperwork Reduction Act because DAS does not directly collect information from the individual.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

DAS contains the following categories of information about aliens, foreign-born inmates, and immigration benefit beneficiaries and petitioners:

[6] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013).
[7] DHS/USCIS-002 Background Check Service, 72 FR 31082 (Jun. 5, 2007).
[8] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).
[9] JUSTICE/005 Inmate Central Records System, 72 FR 3410 (Jan. 25, 2007).
[10] DOJ/FBI-001 National Crime Information Center (NCIC), 72 FR 3410 (Jan. 25, 2007).

Biographical Information: Name; date of birth; country of birth; country of citizenship; gender; weight; height; eye and hair color; race; marital status; last known address; phone number; known aliases; and identifying numbers, such as Social Security number (SSN), A-Number, and driver's license number.

Criminal Case History Information: Jurisdiction; court case name and number; adjudication and adjudication date; arrest date; degree level; fines; plea; deposition; case ID number; removal charge; removal case category; docket case office; attorney name; suspended time; party status disposition code; and disposition description.

Criminal Custody Data: Facility name, type, and location; admission assignment and destination assignment; arrival and projected release date; and identifying numbers, such as the Bureau of Prison ID number; and inmate number.

Criminal History: Summary of conviction and conviction date; offense; sentence description and date; incarceration date; arrest date; arrest level degree; National Crime Information Center group and number; severity code; crime code and description; escape information; and identifying numbers, such as the FBI Universal Control Number, State Identification Numbers, and sex offender registry ID number.

Immigration Benefit Application Data: Date of benefit application and decision; adjudicative status; beneficiary (*i.e.*, worker, dependent, fiancé(e)/spouse, or child) and petitioner (*i.e.*, employer or individual filing for their spouse or children) biographical information; number of beneficiaries; benefit start and end date; benefit appeal date; class preference; and consulate.

Immigration Case History: Hearing code and date; charge; final order date; case closed date; notice to appear issue; docket ID number; case ID number; and the name of the attorney assigned to the case.

Immigration Custody Data: Detainer date; detention date and location; and release date.

Immigration History: Apprehension date, method, and site; processing disposition and code; interview date; sentence; length; removal case ID number; departure date; case category; and refugees, asylum and parole designation.

Naturalization History: Naturalization status; naturalization date; and immigration status.

Vehicle and Insurance Information: Vehicle identification number; plate number; vehicle color, make, and model; vehicle registration and expiration date.

ERO Officer Information: Name and AOR (for officers who are the NCATC POCs for their AORs).

2.2 What are the sources of the information and how is the information collected for the project?

Datasets from certain government (federal and state) IT systems are manually uploaded to DAS on a periodic basis. DAS does not collect information directly from individuals. There are no system-to-system connections with DAS, nor does DAS supply information back to any of the source systems.

DHS Sources

Enforcement Integrated Database (EID)[11]**:** DAS contains datasets from EID. This database captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, U.S. Customs and Border Protection, and USCIS. NCATC receives this dataset on a weekly basis via a file uploaded to a secured NCATC shared drive on an NCATC server. Access to the shared drive is provided based on an individual's ICE network account. Analysts who are designated as system administrators upload the datasets into DAS.

This dataset contains data from EID's Enforcement Alien Removal Module (EARM) and the ICE Integrated Decision Support System (IIDS), which is a reporting sub-system of EID. EARM supports ICE's processing and removal of aliens from the United States and provides a comprehensive view of a detainee's detention and removal status, including criminal history information and information from the Department of Justice's Executive Office for Immigration Review. IIDS uses data from EID to provide reporting about aliens throughout the alien identification, encounter apprehension, and removal processes.

Computer Linked Application Information Management System 3 (CLAIMS 3) [12]**:** DAS contains a subset of data from USCIS's CLAIMS 3. This system is used to track and process applications for naturalization. On a monthly basis, USCIS provides a subset of information collected on the application for immigration benefits to NCATC. This dataset is transmitted via secure electronic transmission to an NCATC server on the DHS network and manually uploaded into DAS by NCATC Analysts.

Central Index System (CIS)[13]**:** DAS contains a limited subset of data from USCIS's Central Index System. CIS serves as a DHS-wide index, maintaining immigrant benefit and naturalization information. On a quarterly basis, USCIS provides biographic information and a

[11] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, *available at* www.dhs.gov/privacy.

[12] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* www.dhs.gov/privacy.

[13] *See* DHS/USCIS/PIA-009 Central Index System, *available at*, www.dhs.gov/privacy.

subset of information from the Central Index System to NCATC. This dataset is transmitted via secure transmission to an NCATC Server on the DHS network and manually uploaded into DAS by NCATC Analysts.

<u>*Non-DHS Sources*</u>

SENTRY Inmate Management System**:** The BOP maintains the SENTRY system, which contains information related to the processing of federal inmates and prison property management. On a weekly basis, the BOP shares with the NCATC an extract of a subset of SENTRY data containing biographic, criminal custody, and criminal history information of foreign-born inmates. The NCATC does not receive information pertaining to inmates born within the United States. This information is provided in an electronic format to a secure ICE Network Server and manually uploaded into DAS. Both the SENTRY dataset on the ICE server and the dataset in DAS are both overwritten with each weekly file. The old file/dataset is no longer available once the new one is received.

Interstate Identification Index (III) System**:** The FBI's Criminal Justice Information Services Division maintains the III system. NCATC biannually provides a limited set of A-Numbers belonging to certain removable aliens in an encrypted, password-protected file on removable media to the FBI via secure mail courier. Using the Interstate Identification Index system, the FBI queries the Universal Control Number and the state identification number associated with the provided A-Number. The FBI provides results to the NCATC in an encrypted, password-protected file on removable media via secure mail courier. NCATC Analysts then manually uploads the dataset into DAS.

Strategic Offender Management System (SOM): The CDCR operates all state adult prisons and juvenile facilities, as well as a variety of community correctional facilities in the state of California. CDCR uses SOM for case management. SOM allows for identification of an offender throughout his/her time in the CDCR. On a monthly basis, the CDCR creates a file from SOM with biographic information and criminal custody data of foreign-born incarcerated individuals who are either on parole or in a California state correctional facility and places it on a secure CDCR file transfer protocol (FTP) encrypted server accessible to law enforcement partners and agencies. NCATC Analysts access this server through accounts requiring unique user names and passwords. Once retrieved by an NCATC Analyst, the dataset is manually uploaded into DAS.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. DAS uses publicly available information from two commercial sources:

United States Post Office: The NCATC has a subscription to receive a publicly available dataset from the United States Post Office. This dataset contains comprehensive information about zip codes and their corresponding city and county names. The NCATC receives this information once a month and Analysts load it into DAS. The dataset is used to ensure that address data tables in DAS are routinely updated to accurately report city place names by zip code. This dataset does not include PII.

Commercial Vendor: The NCATC also contracts with a commercial data vendor to obtain relevant open source (*i.e.*, publicly available) information about removable aliens, as needed. This open source data augments the data already in DAS and increases the probability of a location an alien for apprehension and removal. On a weekly basis, the NCATC provides alien names and dates of birth to the commercial data vendor in an electronic format via secure encrypted email transmission. The vendor queries the open source data on a weekly basis in order to identify and provide updated information pertaining to the requested aliens. Vendor results include biographical information, criminal history, criminal case history, and vehicle information (including vehicle registration information). An NCATC Analyst reviews the results and uploads the dataset into DAS. NCATC Analysts use the vendor-provided data to inform the Information Referrals that will assist ERO field offices in locating the aliens for removal. This commercial vendor dataset, as with all datasets in DAS, is labeled and kept separate to ensure the Analyst can distinguish the source of the information.

2.4 Discuss how accuracy of the data is ensured.

The information maintained in DAS is primarily received from other government agency systems (described in section 2.2). These source systems generally contain information that was collected directly from the alien at the time of encounter, benefit application, arrest, and/or placement into custody, as well as from the law enforcement officers who recorded and entered them into the databases. Collecting information about an individual directly from that individual generally ensures a high degree of accuracy. However, individuals do sometimes provide false identities or other information in an effort to avoid enforcement action or to hide previous law enforcement encounters or removals. Therefore, information is scanned for errors and verified at both the NCATC and the ERO field offices.

DAS runs automated scripts to evaluate the datasets for errors (*i.e.*, formatting, duplicate records, and incorrect data/codes) before the datasets are uploaded. Records containing errors are not accepted by DAS. An NCATC Analyst then reviews, reconciles, and/or validates the records in error prior to uploading the records to DAS. Identifiers for each dataset and system of origin remain with the information within and outside of DAS so that Analysts can identify the source of data within DAS. Additionally, the DAS dataset source is provided in the Information Referral disseminated to the ERO field offices so ERO officers can conduct system checks to validate and update the accuracy of information they receive from the NCATC.

NCATC Analysts also work with NCATC Criminal Targeting Specialists who have access to other systems and conduct citizenship checks to ensure that the Analysts provide accurate information related to an individual's citizenship status before providing information to ERO field offices. If the alien's citizenship status has changed since the DAS dataset was last received, it is noted in the Information Referral provided to the ERO field office. This indication is done to alert the ERO field office that certain individuals are no longer considered amenable to removal (*e.g.*, in the case of naturalization) or, in the case of a lawful permanent resident, more research should be performed before attempting to locate the alien to determine if there is a sufficient level of criminality to be considered for removal (*e.g.*, certain sex offenses; sentence length; victims under a certain age).

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: DAS may present a risk of over-collection of PII.

Mitigation: ICE collects information needed to locate, apprehend, and remove aliens. To mitigate over-collection of PII, only select data fields are provided to NCATC to be stored in DAS. The datasets maintained in DAS are extracts containing subsets of data that is necessary to verify the identity and potential removability of aliens and to identify their locations. Further, ICE does not take enforcement action against any individual without confirming that the individual is removable from the United States. Therefore, if DAS users or ERO officers who receive Information Referrals determine that the information from DAS relates to a U.S. citizen or an alien who is not amenable to removable, ERO will not take action against that individual.

Privacy Risk: Use of commercial data could present a risk of data inaccuracy.

Mitigation: ICE uses data from commercial vendors only to augment existing data in the DAS system, not as a primary source of information or data. Further, ICE does not rely solely on address information obtained from commercial data sources, but verifies address accuracy through non-commercial sources.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

ICE maintains information in DAS to assist in the location, detention, and removal of aliens. Specifically, this information is collected to support the following ICE activities: confirming the correct identity of an alien; determining the citizenship status of individuals thought to be aliens; determining the likelihood of or confirming an alien's continued presence within the United States; and providing ERO with information to further investigate and locate aliens who are amenable to removal. ERO also uses DAS information to more efficiently allocate agency resources toward effective, targeted enforcement actions.

Biographical information is used to verify an alien's identity. An alien's FBI number is necessary for determining criminal history information, and the A-Number is needed for determining immigration status. Additionally, any SSN associated with an alien is used to help confirm that alien's identity.

Immigration information (including case and custody information) is used to determine if there is an outstanding order of removal, whether or not the alien is already in ICE custody, or if the alien has been removed from the United States. This information would be used by the field office to prioritize the allocation of time and resources related to locating that alien.

Benefit data is useful in determining the allocation of time and resources related to locating an alien. For example, if an alien is in the process of receiving an immigration benefit (*e.g.*, lawful permanent resident status) after receiving a final order of removal, the field office may decide to allocate resources to other aliens who have not applied for or are not in the process of receiving an immigration benefit. The immigration benefit applications also provide possible current addresses for aliens who may be amenable to removal.

The NCATC uses naturalization information to verify an individual's citizenship status, which is essential in determining if an individual is amenable to removal. For example, if an ERO field office submits an Information Referral request on an alien, data from the Central Index System would be used to determine if the individual is now a U.S. citizen, in which case he or she would not be removable, and ERO would not attempt to locate or remove him or her from the United States.

Criminal history and criminal case information is used to prioritize the allocation of time and resources of the ERO office to those aliens with a criminal history and to assess risk. Criminal custody data is used to identify aliens who are currently incarcerated. This information may be provided to an ERO field office in response to an Information Referral request and used in the prioritization and allocation of time and resources. This information is also used to determine if any aliens with outstanding removal orders are already incarcerated.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. DAS does not use technology that conducts electronic searches, queries, or analyses to identify a predictive pattern or anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. Other DHS components do not have access to DAS. Only NCATC Analysts and DDOs have access to the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that data may become outdated or incorrect without real-time refresh from all source systems.

Mitigation: DAS relies upon the source systems listed in Section 2.2 to ensure that data used by the system is accurate, complete, and up-to-date at the time it is received. DAS receives updates from the source systems at various intervals regarding any changes to those source system datasets. Discrepancies may be identified in the context of an Analyst's review of the data in DAS from these various sources. If a discrepancy is identified, an Analyst notes this in any Information Referrals containing the potentially discrepant information. The Information Referrals indicate the sources of the data, and DDOs send a message to the field offices within the emails stating (paraphrasing) that the leads have not been reviewed with regard to the exercising of prosecutorial discretion; that field offices must review and make decisions about enforcement efforts; and that case officers must continue to verify alienage, removability, criminality, and location of all subjects. ERO officers do system checks in EID, CLAIMS 3, CIS, and other systems to which they have access, to validate and update the data in Information Referrals before taking any action. Although this risk cannot be fully mitigated without real-time data refreshes to DAS, there are sufficient checks in place both at the NCATC and the field offices to ensure field offices are relying on the most current information when making decisions about enforcement activities.

Privacy Risk: There is a risk of unauthorized access to or disclosure of information contained in DAS.

Mitigation: To mitigate this risk, NCATC has limited the DAS user group to two specific user groups, both of which have a need to know. The access roles are pre-designated by the individuals' position, which ensures users are only granted access to information necessary to perform their official duties. For example, only NCATC Analysts have read/write access to DAS. DDOs have read-only access and can only query DAS to obtain limited information. Additionally, all users receive training regarding the proper use of ICE systems and rules of behavior prior to being granted access to the system. All DAS users complete annual mandatory privacy and security training, which stresses the importance of appropriate and authorized use of personal data in government systems. Finally, DAS has implemented IT security processes that include audit logs and Single Sign-On capability.

Privacy Risk: There is a risk of unauthorized disclosure arising from DAS users' practice of emailing Information Referrals to ERO field offices.

Mitigation: Information Referrals are emailed to ERO field offices using the ICE internal network; the PII remains secure because the emails do not traverse the open internet. ERO field office personnel ensure that Information Referrals containing PII are secured in accordance with agency policy. Further, all ICE employees are reminded in the annual privacy and security training of their responsibility to protect all sensitive PII by only sending it to those who have a business-related need to know, and of the privacy incident reporting requirements.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Notice provided by ICE to the individual prior to collection of information is limited. This PIA provides notice of the existence of the system. In addition, the Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN,[14] provides notice that information about fugitive aliens is being collected. ICE and other DHS components provide notice, when necessary, through the publication of PIAs, SORNs, and other notifications deemed appropriate by the DHS component or the DHS Privacy Office. Individuals providing information that is ultimately transmitted to DAS are provided notice at the time of the initial collection using Privacy Notices that inform the individuals of the authority for and purpose of the collection, the uses for which the information will be shared, and whether providing the information is mandatory or voluntary. The DHS/ICE-011 SORN provides general notice that information about aliens and members of the public is collected. Certain national security, intelligence, and law enforcement collections may not provide advance notice, or may not provide notice through a PIA, because to do so would jeopardize the ability to collect information.

As discussed in Section 2.3, the NCATC subscribes to two commercial data vendor services to obtain information to assist in the location of aliens. The data in these datasets is collected by commercial entities from their own sources for the purpose of selling it to other parties, and is not collected on behalf of or at the request of ICE. These data services are responsible for providing the appropriate notice to individuals whose information they collect under applicable laws; however, when information is gathered by these vendors from open (*i.e.*, publicly available) sources, individuals may have no notice or only constructive notice, if they understand their information is widely accessible when they select to put it into public fora.

[14] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (Oct. 19 2016).

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Because the data included in DAS is mostly collected in other systems and provided to the NCATC for law enforcement purposes, opportunities for individuals to decline to this sharing of the information pertaining to them are nonexistent. However, aliens who are arrested have rights afforded to them under the U.S. Constitution to decline to provide information to law enforcement. Individuals may also have the opportunity to opt out of providing information that is collected in the other source systems that feed information to DAS, as well.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware their information is contained within DAS, or that DAS collects open source data collected and provided by a commercial vendor.

Mitigation: ICE and other Federal Government agencies mitigate this risk by the public notice provided through this PIA and the associated SORNs. Additionally, certain individuals receive notice of collection of information when seeking immigration benefits (*e.g.*, visa or immigration benefit applications) or upon being detained. Open source data repositories may provide some notice; however, individuals whose information is gathered from publicly available sources may not have notice or may have constructive notice if they understand that information they elect to put into public fora is broadly accessible. In order to lessen the risk of interference with the performance of official duties, law enforcement agencies collecting data about individuals may not provide notice to the subjects of investigation.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

Datasets from other federal systems that are loaded in DAS are copies of federal records and, therefore, the DAS copies are not subject to records retention requirements. The original federal records persist in the systems from which the extracts are derived. Since ICE is not subject to the original records retention schedules, ICE keeps records for a shorter period of time than the original records. The maximum time any copied dataset is being retained by DAS is 3 months. ICE is overwriting the copied datasets with every new upload. ICE is in the process of scheduling the original and non-federal DAS datasets (*i.e.*, the manually input EOR officer name and AOR information, the CDCR SOM dataset, and the two commercial datasets) and the Information Referrals that are created using data from DAS. ICE intends to request to retain unique DAS records for three (3) years from the end of the fiscal year in which the NCATC received the data. ICE intends to request to retain Information Referrals for three (3) years from the end of the fiscal year in which any associated immigration case was closed. Until ICE has a NARA-approved retention schedule in place, ICE will keep the records indefinitely.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Some of the data DAS receives will not pertain to aliens who are amenable to removal, which creates a risk that DAS may retain more information than is necessary to serve the purposes for which it exists.

Mitigation: This risk is partially mitigated. DAS predominantly receives datasets that are tailored to provide information on aliens who are amenable to removal and, in fact, the majority of the data contained in DAS pertains to those individuals. In limited cases, however, these datasets will include information on U.S. citizens (*e.g.*, the BOP dataset that includes data on foreign-born inmates) or aliens who are not, in fact, amenable to removal. Federal datasets are entirely overwritten when each new dataset is received, as they are copies and, therefore, not required to be managed by ICE in accordance with their applicable federal records schedules. Overwriting the datasets mitigates the risk of retaining data not pertaining to aliens who are amenable to removal. ICE is in the process of scheduling the non-federal datasets and is mitigating the identified risk by proposing a three-year retention period. Given the relatively limited retention period, the due diligence regarding citizenship that the NCATC conducts before including information about individuals in Information Referrals (as described elsewhere in this PIA), and the controlled access to the DAS, the privacy risks are sufficiently mitigated.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

DAS information may be shared with other DHS components, as well as certain federal or international government agencies for the purpose of safeguarding national security pursuant to applicable laws and policies, and within the bounds of official Memorandums of Understanding (MOU) and Memorandums of Agreement (MOA).

ICE also discloses limited identifying information to a single contracted commercial data vendor on a routine basis so that the vendor may conduct batch and ad hoc searches of its proprietary systems, and return the results of those queries to NCATC. NCATC personnel email a limited set of biographical information to the commercial data vendor via an encrypted, password-protected file. The vendor then queries a wide range of public sources, and sends the results to an NCATC Analyst via a secure encrypted email attachment. The vendor's use of the data is limited by the terms of the contract and subject to ICE security standards for the use and handling of sensitive PII.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The external sharing described above is compatible with the original purpose for collection, as permitted by the Privacy Act of 1974 (5 U.S.C. § 552a) and pursuant to routine uses published in the Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN.[15] This information is shared primarily to generate Information Referrals for ERO field offices to assist with the enforcement of United States immigration laws and the removal of aliens. Identification of individuals unlawfully present in the U.S. is one of the purposes described in the CARIER SORN. All external sharing falls within the scope of applicable law, including the published routine uses in the applicable SORNs.

6.3 Does the project place limitations on re-dissemination?

Federal agencies that receive DAS information are subject to the Privacy Act and may not re-disclose information without clear authority to do so when the information disclosed by ICE is subject to the Privacy Act's protections. The vendor with which ICE shares DAS information is prohibited under terms of its contract from re-disseminating information from DAS or the results it sends to ICE.[16] It is also required to maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information, and notify NCATC when it becomes aware of any breach of security of interconnected systems or potential or confirmed unauthorized use or disclosure of personal information.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures made outside of ICE are typically made as a result of an ongoing investigation or other law enforcement activity; the record of the disclosure is placed in the relevant file by the ICE employee making the disclosure.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a potential risk that external disclosures could result in the unsecure transmission of information.

[15] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (Oct. 19 2016).

[16] More specifically, the contract prohibits the vendor from publishing, permitting to be published, or distributing for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of the contract, without the prior written consent of the Contracting Officer. Additionally, electronic or printed copy of any material proposed to be published or distributed shall be submitted to the ICE Contracting Officer.

Mitigation: Appropriate security measures have been established for the transmission of DAS data so that the risk of compromise is minimal, including encryption and use of secure DHS Intranet connections. Other means of transmission are handled securely in accordance with DHS policy.

Privacy Risk: There is a risk that information may be shared with outside Government and non-government entities without a need to know.

Mitigation: All ICE employees are trained on the appropriate sharing of PII, and told to contact the ICE Office of Information Governance and Privacy if they are not certain whether information sharing is appropriate. Data owners ensure that privacy risks are mitigated through data sharing agreements that place restrictions on re-disclosure and require physical, technical, and administrative controls. The commercial data vendor is also restricted from re-disclosing DAS information pursuant to the terms of their contracts and agreements with ICE.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking notification of and access to any record contained in this system of records may submit a request in writing to the ICE Freedom of Information Act (FOIA) officer by mail:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

All or some of the requested information may be exempt from access pursuant to the Privacy Act or the Freedom of Information of Act (for those individuals who are not U.S. citizens or lawful permanent residents and whose records are not covered by the Judicial Redress Act) in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in DAS could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals seeking to correct records contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE Office of Information Governance and Privacy by mail:

U.S. Immigration and Customs Enforcement
Privacy and Records Office
Attn: Privacy Branch
500 12th Street SW, Stop 5004
Washington, D.C. 20536-5004
(202) 732-3300
http://www.ice.gov/management-administration/privacy

All or some of the requested information may be exempt from correction in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in DAS could inform the subject of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension.

7.3 How does the project notify individuals about the procedures for correcting their information?

The procedure for submitting a request to correct information is outlined in this PIA and the associated SORNs. As stated above, individuals may submit requests for information and correction as permitted by the Privacy Act and agency policy, which will be reviewed and corrected on a case-by-case basis.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There are risks of a lack of access to information and inability to seek redress and correction.

Mitigation: Redress is available through requests as described above, however, providing individual access or correction of the records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in DAS could inform the public of ICE’s activities and leads. Access to these records could also impede ICE’s investigation and/or assist aliens in avoiding detection or apprehension. Further, amendment of the records could interfere with ongoing investigations and law enforcement activities, and may impose an impossible administrative burden on investigative agencies. The existing redress procedures are adequate to address the individual’s right to access and correct their records.

Privacy Risk: There is a risk that individuals will be unable to meaningfully control the use of their data as maintained in this system, or determine whether the system maintains records about them.

Mitigation: Because the records in DAS are aggregated from various other databases within DHS components and offices as well as other federal, state, and commercial databases, individuals' rights to be notified of the existence of data about them in the DAS system, and to direct how that data may be used by ICE, are limited. Individuals may also have the option to seek access to and correction of their data directly from the agencies that originally collected it. Information that is corrected in the original data source would be updated in DAS when the information is again accessed in the source database or based upon a request of an individual, or when ICE becomes aware of inaccuracies of the information.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

DAS operates within the DHS network and is protected by DHS network firewalls. DAS has a number of specific auditing measures and technical safeguards in place. User authentication at the network and database levels and network encryption prevent unauthorized access to DAS data. Workstations are configured to automatically lock a session after 15 minutes of inactivity and to terminate the session after sixty (60) minutes of inactivity. Inactive accounts are disabled after 45 days and deleted after 135 days of being disabled. Upon notification of an NCATC employee's termination, if that employee has access to DAS, system administrators immediately revoke user access by disabling the individual's credentials. Audit records indicate who deleted the user's account, as well as the date/time that the account was deleted.

Audit records and user authentication (logons and logoffs) are captured by the operating system. DAS retains the query/task name, the date and time of the query, and number of matches in the dataset. However, the actual results of the query are not saved in DAS. All failed logon attempts are recorded in an audit log and reviewed once a month by an NCATC Analyst. The Office of the Chief Information Officer (OCIO) at ICE also reviews activity logs when requested by the Information System Security Officers (ISSO). DAS user audit trails provide adequately detailed information to facilitate reconstruction of events if compromise or malfunctions occur. The audit trail is protected from actions, such as unauthorized access, modification, and destruction that would negate its forensic value. Individuals who are found to access or use DAS data in an unauthorized manner will be disciplined in accordance with ICE policy.

Finally, this PIA is subject to periodic revision in the case that (a) DAS beings to receive data from additional sources; (b) analytical data tools that identify predictive patterns or anomalies are introduced; or (c) changes to the mission DAS supports leads to changes in the way data is collected, analyzed, or disseminated to law enforcement partners. Any proposed change to the scope of DAS that would go beyond the bounds of what is described in this PIA would result in an updated PIA.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All personnel who have access to the ICE network are required to take annual privacy and security training, which emphasizes the DHS Rules of Behavior and other legal and policy restrictions on user behavior. Additionally, DAS users receive training on appropriate uses of DAS as part of NCATC's Operations Training.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only ICE personnel who require access to the data in DAS as a part of the performance of their official duties are granted access. NCATC management oversees and approves the assignment of user accounts to ICE personnel, and at present only individuals occupying two NCATC positions are authorized to access the system.

Only ICE network-authenticated users are granted access to DAS. Authorized users access DAS over the ICE network from ICE standard workstations. NCATC establishes user accounts and updates user identification, role, and access profiles as changes are needed. Access roles are assigned by a supervisor based on the user's job responsibilities. Access roles are reviewed regularly to ensure that users have the appropriate access. Individuals who no longer require access are removed from the access list.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All sharing agreements and MOU are reviewed by the program manager, component Privacy Officer, and counsel, and then sent to DHS for formal review.

Responsible Officials

Amber Smith

Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security