Privacy Impact Assessment
for the

Technical Reconciliation Analysis Classification System (TRACS)

June 6, 2008

Contact Point
Paul Hasson, Acting Privacy Officer
US-VISIT Program Office
(202) 298-5021

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program will operate the Technical Reconciliation Analysis Classification System (TRACS). TRACS will serve as an information management tool used for management and analysis of US-VISIT records to enhance the integrity of the United States immigration system by detecting, deterring, and pursuing immigration fraud, and by identifying persons who pose a threat to national security and/or public safety. US-VISIT is conducting this privacy impact assessment (PIA) because TRACS will use personally identifiable information.

Overview

The Department of Homeland Security (DHS) and the United States – Visitor and Immigrant Status Indicator Technology (US-VISIT) program is publishing this PIA, along with a Privacy Act system of records notice (SORN) and a notice of proposed rulemaking (NPRM), for the Technical Reconciliation Analysis Classification System (TRACS), an information management tool used for management and analysis of US-VISIT records. TRACS will help enhance the integrity of the United States immigration system by detecting, deterring, and pursuing immigration fraud, and by identifying persons who pose a threat to national security and/or public safety. TRACS will consist of paper files and electronic databases.

The Secretary of the Department of Homeland Security has delegated to US-VISIT the responsibility for enhancing the security of U.S. citizens and visitors; facilitating safe, efficient, and legitimate travel to the U.S.; promoting border security and the integrity of the immigration system; safeguarding the privacy of visitors to the U.S.; assisting in the prevention of immigration identity fraud or theft; and serving law enforcement, border officials, and others who make decisions on immigration matters, including decisions on immigration benefits and status, by –

- Identifying aliens seeking permission to enter, entering, visiting, residing in, changing status within, or exiting the U.S.; and
- Providing technical assistance and analytic services to other DHS functions and components; Federal agencies; State, local, tribal, and foreign governments, including international organizations, to better protect the Nation's physical and virtual borders.

Based on the above delegated mission, TRACS will be used to:

- Identify individuals who have remained in the United States beyond their authorized period of admission (overstays);
- Maintain information on why individuals are promoted to or demoted from the Automated Biometric Identification System (IDENT) list of subjects of interest;
- Provide the means for additional research in regards to individuals whose biometrics are collected by DHS and subsequently matched to the list of subjects of interest during a routine IDENT query. A query of this nature would take place following a background check or security screening related to the individual's hiring, retention, performance of a job function, or the issuance of a license or

credential, allowing them access to secured facilities to perform mission and non-mission related work. Examples of this include credentialing of Federal, non-federal, and contractor employees who work within the secured areas of our nation's airports;

- To further analyze information about individuals who may be identified as a subject of interest following a routine query against IDENT while applying for visas or other benefits on behalf of domestic partners, such as the U.S. Department of State or foreign partners, as is the case with the United Kingdom Border Agency's (UKBA) International Group Visa Services program, which support the DHS mission; and
- Provide information in response to queries from law enforcement and intelligence agencies charged with national security, law enforcement, immigration or other DHS mission-related functions.

Specifically, TRACS will be used for the analysis of overstays, for changes to the IDENT subject of interest lists, law enforcement and intelligence research, and to assist in developing and fostering foreign partnerships that enhance the goals and mission of US-VISIT, such as the work being done in association with the UKBA's International Group Visa Services project.

Overstays

US-VISIT reviews and analyzes information in the Arrival and Departure Information System (ADIS)[1], a US-VISIT system used for the storage and use of biographic, biometric indicator and encounter data on aliens who have applied for entry, entered, or departed the United States. ADIS consolidates information from various systems in order to provide a repository of data held by DHS for pre-entry, entry, status management, and exit tracking of immigrants and non-immigrants. Its primary use is to facilitate the investigation of subjects of interest who may have violated their authorized stay. To assist in the resolution of overstays, information related to them is copied to TRACS for review and further analysis against other US-VISIT programs and systems to better determine their status.

Changes to IDENT Subject of Interest List

To maintain the integrity of the immigration and customs programs, DHS maintains records within IDENT to identify individuals who may present a terrorist threat to the United States as well as those individuals who may not be allowed to enter the country because of past violations of immigration or customs law. An individual is either promoted to or demoted from the list of subjects of interest within IDENT. As IDENT is not a case management system; it merely records the change, not the justification for the change.[2] TRACS will have the ability to serve as a case management system and not only use the information regarding the changes to the list of subjects of interest that is recorded in IDENT but also to record an store the actual justification for any change. The user will also have the ability to enter data in pre-determined selectable categories or manually by either free text or by cutting and pasting information retrieved from other systems and placing it into a workspace in TRACS so that analysis can be performed.

[1] 72 FR 47057, Arrival and Departure Information System (ADIS), System of Records Notice, August 22, 2007.
[2] 72 FR 31080, Automated Biometric Identification System (IDENT), System of Records Notice, June 5, 2007.

Assist in Background Check and Security Clearance

During the background investigation for employment at DHS or receipt of a DHS license or credential, applicants may have their information searched against ADIS or IDENT records. Clearance, employment eligibility, or other license or credential applications that have a match against ADIS or IDENT may require additional research regarding the applicant. Such information would be maintained and tracked in TRACS.

Applications for Visas or Other Benefits

On behalf of domestic or foreign partners, US-VISIT will assist its partners in analyzing information held by US-VISIT where such analysis supports the DHS mission. For example, for the UKBA International Group Visa Services project, US-VISIT will receive biometric information from the United Kingdom (UK) for UK visa applicants and query their biometric information against the IDENT list of subjects of interest. US-VISIT will then provide the results from the query back to the UK for purposes of visa adjudication.

Law Enforcement and Intelligence Research

US-VISIT may also receive requests from other law enforcement agencies, such as Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), and the Federal Bureau of Investigation (FBI), as well as from other intelligence agencies, to provide further information regarding the immigration status for individuals of interest to those organizations. US-VISIT tracks these requests and the responses in TRACS.

Information in TRACS comes primarily from ADIS and IDENT. TRACS may also contain information from other DHS component programs or systems, or publicly available source systems that are manually queried while researching a particular case. Data researched or identified through publicly available source systems, such as the internet, will be identified and referenced in the individual's record in TRACS. If it becomes routine for a specific public source system(s) to be used on a regular basis, the PIA will be updated to reflect this system(s) as a common source of information and data. For research conducted, based on an external request, information may also be provided from the requesting entity, as described below for the DHS/United Kingdom Border Agency's (UKBA) International Group Visa Services program.

Additional law enforcement and intelligence research systems include but are not limited to:

1. CBP Treasury Enforcement Communications System (TECS);
2. Department of State (DOS) Consolidated Consular Database (CCD);
3. ICE Student and Exchange Visitor Information System (SEVIS);
4. United States Citizenship and Immigration Services (USCIS) Central Index System (CIS);
5. USCIS Computer-Linked Application Information Management System (CLAIMS 3 and 4);
6. USCIS Refugees, Asylum, and Parole System (RAPS);
7. ICE Deportable Alien Control System (DACS);
8. ICE Enforcement Case Tracking System (ENFORCE)[3]; and

[3] 66 FR 53029, Treasury Enforcement Communication System (TECS), System of Records Notice, October 18, 2001;

9. Public information from Web searches for addresses and telephone numbers.

UKBA's International Group Visa Services Project

Recently the United Kingdom enacted legislation requiring the submission of biometric data by almost all individuals filing visa applications for entry into the United Kingdom. Officials from the UK and DHS have agreed that individuals who are physically located in the United States may provide the requisite biometrics and limited biographical information at USCIS Application Support Centers (ASCs) for forward transfer to the UK in support of the adjudication of applications for visas. USCIS, working in conjunction with US-VISIT will utilize components of TRACS, ADIS and IDENT for the UKBA International Group Visa Services project[4].

For the UKBA visa services project, US-VISIT will receive biometric information from the UK for UK visa applicants and query their biometric information against the IDENT list of subjects of interest. US-VISIT will then provide the results from the query back to the UK for purposes of visa adjudication. US-VISIT will also provide to IDENT stakeholders only those positive results from the query that matched for law enforcement, and or national security purposes. If a biometric match against the IDENT list of subjects of interest is verified, then the applicants' biographic information is retained by US-VISIT in TRACS.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as the reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is to be collected, used, disseminated, or maintained in the system?

TRACS contains biometric, biographic, biometric indicator, immigration or criminal encounter, and information management data, along with publicly or commercially available data.

- Biometric data may include, but is not limited to, photographs and fingerprints. Biographic data may include, but is not limited to, names, aliases, date of birth, nationality, and other personal descriptive data.
- Biometric indicator data may include, but is not limited to, fingerprint identification numbers.

---

70 FR 14477, Student and Exchange Visitor Information System (SEVIS), System of Records Notice, March 22, 2005; 72 FR 1755, Central Index System (CIS), System of Records Notice, January 16, 2007; 67 FR 64132, Computer Linked Application Information Management System (CLAIMS 3 and 4), System of Records Notice, October 17, 2002; and 67 FR 64136, Deportable Alien Control System (DACS), System of Records Notice, October 17, 2002.

[4] The signed Memorandum of Understanding(January 2008) is between the Department of Homeland Security of the United States of America and the [UKBA International Group Visa Services program formerly known as] UKVISAS as the Authority Appointed by the Secretary of State for the Home Department and the Secretary of State for Foreign and Commonwealth Affairs of the United Kingdom of Great Britain and Northern Ireland, regarding Information Vetting and Sharing

- The encounter data provides the context of the interaction (e.g., border entry screening encounter, immigration enforcement encounter, and visa application encounter) with an individual. This data may include, but is not limited to, encounter location, document types, document numbers, document issuance information, conveyance information, and addresses while in the U.S.
- Information management data is used to manage ongoing analyses or investigations and may include, but is not limited to, case resolution, status, comments and notes from interviewers or by the analysts assigned to the case(s).
- TRACS may include commercial or publicly available data such as name, address, and phone number as found in open source searches of internet phone directories. Such searches serve to resolve discrepancies or gaps in existing information; the information is not used as the sole basis for investigation and is not determinative of any resolution of a case or investigation. Currently, TRACS does not obtain commercial data, however the plans to include such available data in the future. This PIA will be updated once such expanded use occurs.

TRACS contains data primarily collected on non-U.S. citizens, although it will also contain data on: (1) U.S. citizens who have a connection to the DHS mission (e.g., individuals who have submitted a visa application to the UK through the UKBA International Group Visa Services program, or have made requests for clearance to work in Federal government-secured areas (credentialing), and who are believed to be subjects of interest); (2) U.S. citizens who have an incidental connection to the DHS mission (e.g., individuals living at the same address as non-U.S. citizens who have remained in this country beyond their authorized stays); and (3) individuals who have, over time, changed their status and become U.S. citizens.

1.2 What are the sources of the information in the system?

The data contained in TRACS is primarily from the US-VISIT systems—Arrival and Departure Information System (ADIS) and the Automated Biometric Identification System (IDENT)—and the Treasury Enforcement Communications System (TECS), a Customs and Border Protection (CBP) system. Additionally, TRACS receives data from the Consolidated Consular Database (CCD), a Department of State (DOS) system, as well as from other systems, including the Student and Exchange Visitor Information System (SEVIS); the Central Index System (CIS); the Computer-Linked Application Information Management System (CLAIMS 3 and 4); the Refugees, Asylum, and Parole System (RAPS); the Deportable Alien Control System (DACS); and the Enforcement Case Tracking System (ENFORCE).

These systems contain information on individuals who are potentially the subjects of interest for further analysis by DHS. TRACS analysts review information collected from various Government programs and publicly available sources, and then is manually extracted (i.e. cut and pasted, hand typing) from the systems listed above, on a case-by-case basis, for use in each particular case or investigation, and included in TRACS. Currently, TRACS does not obtain commercial data, however US-VISIT plans to include such data in the future. This PIA will be updated once such expanded collection occurs.

1.3 Why is the information being collected, used, disseminated, or maintained?

TRACS collects data from the above mentioned source systems when necessary to support the analysis, investigation, and management of illegal immigration, fraud, redress inquiries, or encounters at ports of entry, and investigative referrals from other agencies such as Department of State and Department of Justice.

TRACS is used to:

- Identify individuals who have remained in the U.S. beyond their authorized period of admission (overstays);
- Maintain information on why individuals are promoted to, or demoted from, the Automated Biometric Identification System (IDENT) list of subjects of interest;
- Provide the means for additional research in regards to individuals whose biometrics are collected by DHS and subsequently matched to the list of subjects of interest during a routine IDENT query. A query of this nature would take place following a background check or security screening relating to the individual's hiring, retention, performance of a job function, or the issuance of a license or credential, allowing them access to secured facilities to perform mission and non-mission related work. Examples of this include credentialing of Federal, non-Federal, and contractor employees who work within the secured areas of our nation's airports;
- To further analyze information about individuals who may be identified as a subject of interest following a routine query against IDENT while applying for visas or other benefits on behalf of domestic partners such as the U.S. Department of State or foreign partners, as is the case with the UKBA's International Group Visa Services program, which support the DHS mission; and
- Provide information in response to queries from law enforcement and intelligence agencies charged with national security, law enforcement, immigration or other DHS mission-related functions.

1.4 How is the information collected?

As a case or investigation is opened, information from the various systems is manually retrieved and placed in TRACS. This minimizes the collected information to only that which is required for a particular case. There is no direct connection between TRACS and any other system, either within or outside of DHS.

1.5 How will the information be checked for accuracy?

One of the primary functions of TRACS is to compare various data to ensure that any action taken is based on the most accurate, complete, and up-to-date data. DHS constantly works to identify not only the best data in any particular case under investigation, but also seeks out additional data sets that will improve the data's accuracy, completeness, and timeliness. Nevertheless, because of the diverse environments in which this data is collected, accuracy, completeness, and timeliness may vary considerably. In most cases, the

organization from which TRACS receives data is the original collector and that organization attempts to verify the data with the individual, or entity, from whom the data was collected.

In addition to comparing data from multiple DHS and Department of State systems, USVISIT may review commercial data or readily available public data in order to compare the information for accuracy. Data available and obtained from public sources present concerns because this type of data is prone to a lack currency and correctness. However, these data elements are not in and of themselves used for making decisions about individuals. Data of this type may be used, for example, to confirm previously collected information, to assist in identifying the location of an individual, and to verify the identity and status of a potential subject of interest for further analysis. Publicly available records are not relied on as the sole source to determine outcomes for any analysis or inquiry.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The data is collected and maintained in TRACS under the authority provided by:

- The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106–215;
- The Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106–396;
- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (U.S.A. PATRIOT Act), Public Law 107–56;
- The Enhanced Border Security and Visa Entry Reform Act (Border Security Act), Public Law 107–173; and
- The Immigration and Naturalization Act (INA), Title 8, United States Code, as delegated by the Secretary, Department of Homeland Security.
- Homeland Security Presidential Directive/HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors.
- The signed Memorandum of Understanding (January 2008) is between the Department of Homeland Security of the United States of America and the [UKBA International Group Visa Services program formerly known as] UKVISAS as the Authority Appointed by the Secretary of State for the Home Department and the Secretary of State for Foreign and Commonwealth Affairs of the United Kingdom of Great Britain and Northern Ireland, regarding Information Vetting and Sharing.

1.7 Privacy Impact Analysis: Given the amount and type of data being collected, discuss the privacy risks identified and how they were mitigated.

TRACS does not collect any data directly from individuals; it relies on the collection of data from various external and DHS internal organizations. Consequently, TRACS must rely on the other organizations to ensure that the data is collected appropriately and within the bounds of their individual legal authority. There is no direct connection between TRACS and any other system. The TRACS user will have the ability to

enter data in pre-determined selectable categories or manually by either free text or by cutting and pasting. The information is then placed into a workspace in TRACS so that analysis can be performed, ensuring that only the minimal amount of data necessary for a particular case or investigation will be maintained in TRACS. TRACS uses a minimal amount of data provided by public records to verify or establish identity, status, or location, or to perform basic research on subjects of interest, in order to enhance the integrity of the United States immigration system. To ensure accuracy, US-VISIT has established and employs quality assurance and human-verification procedures on all leads, encounters.

Section 2.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

TRACS is used when US-VISIT identifies a subject of interest as requiring additional research because of possible violation of immigration law. It is also used as the case management system to track requests for information from organizations outside of DHS. In particular TRACS is used to:

- Identify individuals who have remained in the U.S. beyond their authorized period of admission (overstays);
- Maintain information on why individuals are promoted to or demoted from the IDENT list of subjects of interest;
- Provide the means for additional research in regards to individuals whose biometrics are collected by DHS and subsequently matched to the list of subjects of interest during a routine IDENT query. A query of this nature would take place following a background check or security screening relating to the individual's hiring, retention, performance of a job function, or the issuance of a license or credential allowing them access to secured facilities to perform mission and non-mission related work. Examples of this include credentialing of Federal, non-Federal, and contractor employees who work within the secured areas of our nation's airports;
- To further analyze information about individuals who may be identified as a subject of interest following a routine query against IDENT while applying for visas or other benefits on behalf of domestic partners, such as the U.S. Department of State or foreign partners, as is the case with the UKBA's International Group Visa Services program, which support the DHS mission; and
- Provide information in response to queries from law enforcement and intelligence agencies charged with national security, law enforcement, immigration or other DHS mission-related functions.

The primary TRACS transactions are: (1) maintaining a record of the justification and background for a promotion to or demotion from a DHS list of subjects of interest; and (2) Analyzing an individual who has an entry record but no matching exit record in ADIS. Once such a discrepancy is identified in ADIS, the known data on the individual is loaded into TRACS and an analyst will conduct basic searches in other relevant data sets to determine if it can be established that the individual did in fact exit the country. If such information is found, the individual would be identified as having left the country to prevent any problems

if the individual decides to return. If no verification of an exit can be found, this information may be passed on to Immigration and Customs Enforcement (ICE) for further analysis.

In addition, once the data is in TRACS, further basic analysis on individuals who are the potential subjects of interest may be conducted to:

- Analyze data quality, integrity, and utility; and
- Analyze/establish possible trends and patterns in the data for future investigative analysis or enforcement actions.

Trend and pattern analysis would only be conducted on specific information already in the system. For example, if a particular address is associated with several discrete cases of individuals who remained in the U.S. beyond their authorized stays, it could help future investigations.

2.2 What types of tools are used to analyze data and what type of data may be produced?

TRACS does not rely on automated predictive processes, although patterns of data are analyzed by human analysts and in some cases acted on to identify individuals and to prevent immigration and law enforcement violations. However, because data is manually placed in TRACS on particular cases, the amount of data is minimal and it is only useful for basic types of analysis, such as the matching and verification of data elements. For example, visa recipients who have previously been tentatively identified as needing additional scrutiny before entry to the U.S. can have their situation analyzed using data from various systems combined to determine if there is enough information to clear the visitor and allow them to be granted a waiver for an offense where they have overcome their grounds for inadmissibility. US-VISIT staff, using the information in TRACS can then demote them from the list of subjects of interest prior to their arrival at a port of entry, thus not being stopped by a Customs and Border Patrol (CBP) officer for additional screening when entering the U.S.

Users will be able to identify patterns for fraud indicators associated with traveler records. Trend and pattern analysis would only be conducted on the specific information in the system. For example, if a particular address is associated with several discrete cases of individuals who remained in the U.S. beyond their authorized stays, it could help future analysis.

2.3 If the system uses commercial or publicly available data, please explain why and how it is used.

USVISIT employees may use publicly available data to confirm previously collected information and to assist in identifying the address or telephone number of an individual. The information is used as a secondary check on the information provided initially. Public records are not relied upon as the sole determining factor in any analysis or inquiry.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above-described uses.

USVISIT uses TRACS to manage cases where there is a possible violation of immigration law that needs additional analysis or where pursuant to an approved Routine Use an entity outside of DHS requests the information.

Because there is only a limited amount of information in TRACS, used only for unique or specific cases, there is little ability to do complex automated analysis. The primary types of analysis involve comparing and matching information from various sources to establish or verify an identity or other attributes about a particular individual.

Data available from publicly available records presents particular issues because this type of data is prone to a lack of currency and correctness. However, these data elements are not in and of themselves used for making decisions about individuals.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The TRACS SORN published concurrently with this PIA proposes that data will be disposed of when the information regarding the potential subject of interest has either been adjudicated or when the 75 year retention schedule has been met. Seventy-five years is the retention period of IDENT and ADIS, the primary source systems of TRACS. Because TRACS is frequently used to establish and track decisions that affect the lists of subjects of interest and overstay status in IDENT and ADIS, it is necessary that the retention period correspond to these systems.

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention schedule is currently in development with the National Archives and Records Administration (NARA).

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

TRACS may support decisions to change the list of subjects of interest status in IDENT; overstay status in ADIS, and visa eligibility from the DOS CCD. As such, TRACS needs to retain the information that justifies those decisions for the period of time that the information is retained in IDENT, ADIS, and CCD. Coordinated retention times will allow DHS or DOS to confirm that a previous decision was administered correctly and that it is still appropriately applied. Otherwise, it might not be possible to determine why a particular status change was made, should differing retention schedules be used.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared, and for what purpose?

The data in TRACS, including any conclusions derived from that data, may be shared throughout the operational and analytical components of DHS, including, but not limited to, ICE, CBP,USCIS, DHS's Intelligence & Analysis Office (I&A), the Transportation and Security Administration (TSA), and Office of Security. This data includes data derived from the various associated systems for which it is necessary to:

- Identify individuals who have remained in the U.S. beyond their authorized period of admission (overstays);
- Maintain information on why individuals are promoted to or demoted from the IDENT list of subjects of interest;
- Provide the means for additional research in regards to individuals whose biometrics are collected by DHS and subsequently matched to the list of subjects of interest during a routine IDENT query. A query of this nature would take place following a background check or security screening relating to the individual's hiring, retention, performance of a job function, or the issuance of a license or credential allowing them access to secured facilities to perform mission and non-mission related work. Examples of this include credentialing of Federal, non-Federal, and contractor employees who work within the secured areas of our nation's airports;
- To further analyze information about individuals who may be identified as a subject of interest following a routine query against IDENT while applying for visas or other benefits on behalf of domestic partners, such as the U.S. Department of State or foreign partners, as is the case with the UKBA's International Group Visa Services program, which support the DHS mission; and
- Provide information in response to queries from law enforcement and intelligence agencies charged with national security, law enforcement, immigration or other DHS mission-related functions.

Only the minimal data necessary, is provided to each operational component of DHS to appropriately carry out its responsibilities. For example, CBP would be notified when an individual is no longer on a list of subjects of interest, thus allowing that individual to enter or leave the U.S. without additional scrutiny. Another example is that USCIS would be notified when an individual may be in an overstay status and consequently may be ineligible for certain benefits.

4.2 How is the information transmitted or disclosed?

In some cases, information is indirectly transmitted from TRACS to other systems in the various components of DHS. For example, the TRACS analysis may result in a change to ADIS or IDENT and various components will then receive ADIS or IDENT data as updates in accordance with the normal process for accessing these systems. In other cases, the TRACS analysis may result in information that needs to be transmitted by e-mail or other means to a DHS component for action. E-mail would be sent on the DHS core network, an unclassified but secured wide area network. Other types of transmission or disclosure may be required in some circumstances.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

There is very little data that is actually shared directly from TRACS to other DHS components. In most cases the TRACS analysis will result in a change to the data in IDENT or ADIS, and only the changed data in IDENT or ADIS would be shared; and that sharing would take place in the normal course of data sharing from these systems. When data is directly shared from TRACS, it is shared only as necessary to comply with a statutory requirement for immigration or law enforcement, national security, intelligence, or preparedness and critical infrastructure protection purposes. The data is transmitted in a way that will ensure that it is kept secure.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS, which includes Federal, State and local governments, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The data in TRACS, including any conclusions derived from that data, may be shared with appropriate Federal, State, local, tribal, foreign, or international government agencies charged with national security, law enforcement, immigration, intelligence, or other DHS mission-related functions, provided that the data will be used consistently with the purpose for which it was collected in the first place. This data includes data derived from the various associated systems for which it is necessary to:

- Identify individuals who have remained in the U.S. beyond their authorized period of admission (overstays);
- Maintain information on why individuals are promoted to or demoted from the IDENT list of subjects of interest;
- Provide the means for additional research in regards to individuals whose biometrics are collected by DHS and subsequently matched to the list of subjects of interest during a routine IDENT query. A query of this nature would take place following a background check or security screening relating to the individual's hiring, retention, performance of a job function, or the issuance of a license or credential allowing them access to secured facilities to perform mission and non-mission related work. Examples of this include credentialing of Federal, non-Federal, and contractor employees who work within the secured areas of our nation's airports;
- To further analyze information about individuals who may be identified as a subject of interest following a routine query against IDENT while applying for visas or other benefits on behalf of domestic partners, such as the U.S. Department of State or foreign partners, as is the case with the UKBA's International Group Visa Services program, which support the DHS mission; and
- Provide information in response to queries from law enforcement and intelligence agencies charged with national security, law enforcement, immigration or other DHS mission-related functions.

Only the minimal data necessary is provided to each operational DHS component to appropriately carry out its responsibilities. For example, DOS would be notified when an individual is no longer on a list of subjects of interest, allowing that individual to be granted a visa required to enter the U.S. This is similar to the current process of DOS notifying DHS when a visa has been denied.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing of data from TRACS will be compatible with the original collection purpose and authorized by a routine use in the SORN. USVISIT generally shares information with other Federal, State, local, tribal and foreign governments when a possible subject of interest is identified.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

In some cases, information is indirectly transmitted from TRACS to other systems in various components of DHS. For example, the TRACS analysis may result in a change to ADIS or IDENT and the various

components will then receive the ADIS or IDENT data as updates in accordance with the normal process for accessing these systems. In other cases, the TRACS analysis may result in information that needs to be transmitted by other means, such as secure e-mail or portable media. E-mail or portable media would be encrypted and transmitted in such a way that a chain of custody can be established.

DHS has entered into memorandums of understanding (MOUs) and other agreements with non-DHS organizations with which TRACS shares information, either indirectly through IDENT and ADIS or directly from TRACS. These agreements provide the conditions of sharing or disclosure, including governance of the protection and use of the information.

All information users must participate in a security and privacy training program. In some cases this training may be provided by DHS. In other cases, it is the standard security and privacy training given by the receiving organizations.

5.7 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The minimum necessary data will be shared directly from TRACS to external agencies. In most cases the TRACS analysis will result in a change to the data in IDENT or ADIS. Any sharing that occurs through IDENT and ADIS is controlled by an MOU or other agreement that ensures that data is kept secure and is used appropriately. For example, analysis may be conducted that establishes that an individual has not exceeded his or her authorized stay and so is not an overstay. The information in ADIS would be updated so that when DOS checks while processing a subsequent visa application, that agency would not be misinformed that this person may have overstayed his or her valid admissibility. When data is directly shared from TRACS, it is shared as necessary to comply with a statutory requirement for immigration or law enforcement, national security, intelligence, or other DHS-mission related purposes.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Notice regarding the information management and analysis work performed by TRACS is provided by this PIA and the concurrently published TRACS SORN.

Because the data in TRACS is not directly collected from individuals, but rather from other systems that collect the data for various purposes, the extent of the notice will vary depending on the particular collection. In some cases, notice is provided through a PIA published by the specific program or

organization conducting the collection. Certain national security 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 the information in the first place. USVISIT has reviewed the systems from which it will be collecting information to ensure that their use is compatible with the published privacy compliance documentation.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

In some cases, individuals will have had an opportunity or right to decline to provide their information when it is originally collected. In other cases, individuals do not have an opportunity or right to decline to provide information. However, once the information has been collected in the various systems, individuals have no opportunity and/or right to decline to provide their data for use in TRACS.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Whether individuals have a right to consent to a particular use of their data depends on the purpose of the collection, which—if such a right exists—will be described in the PIA specific to the program collecting the data. In the case of publicly available data, individuals may or may not have the ability to consent to a particular use of the data. However, in most cases, because of the national security, law enforcement, immigration, intelligence, or DHS mission-related purposes for which the information is collected, no such right exists. If individuals had such a right and exercised it, their information would not be used for those purposes.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice of the inclusion of this data in TRACS is provided by this PIA and by the concurrently published TRACS SORN. Once the data has been collected by the original system, there is no opportunity or right to decline to provide this information to TRACS. The extent of notice and the opportunity or right to decline consent to particular uses will vary based on the particular purpose associated with the original collection of the information. In many law enforcement or national security contexts, notice of awareness, or the opportunity to consent, would compromise the ability of the agencies to perform their missions. In these cases, notice and consent may not be available. Publicly available data presents a particular challenge because, almost invariably, individuals will not know that their data is being used for the purposes described here.

Section 7.0 Access, Redress and Correction

The following questions are directed at the ability of individuals to ensure the accuracy of the information collected about them.

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

Certain information may be exempt from individual access because access to the data in TRACS could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, or to the existence of the investigation, and could reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. A determination whether a record may be accessed will be made at the time a request is received. DHS will review and comply appropriately with information requests on a case-by-case basis. An individual desiring copies of records maintained in this system should direct his or her request to the Freedom of Information Act (FOIA) Officer, US-VISIT Program, U.S. Department of Homeland Security, Washington, D.C. 20528.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals may have an opportunity to correct their data when it is originally collected; otherwise, they may submit redress requests. Because most of the data in TRACS is copy of data provided by another system that originally collected the data, a redress request is most appropriately addressed to the originating system. If a correction is made to the information in the original system, this new information will be available to TRACS in the same manner that it was originally available. An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received. DHS will review and comply appropriately with information requests on a case-by-case basis. Requests for correction of records in this system may be made through the Traveler Redress Inquiry Program (TRIP) at www.dhs.gov/trip or via mail, facsimile, or e-mail in accordance with instructions available at www.dhs.gov/trip.

7.3 How are individuals notified of the procedures for correcting their information?

Notification is provided by the publication of this PIA and the concurrent SORN for TRACS. In the case of redress requests for DHS organizations, if an individual is not satisfied with the response, an individual can appeal his or her case to the DHS Chief Privacy Officer, who will conduct a review and adjudicate the matter. Redress procedures are also noticed by the program through which the data was originally collected, and notification will vary based on that system.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Not applicable as redress procedures are provided.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Because most of the data in TRACS is a copy of data from other systems of origin, the data must be corrected in the system of origin, which would then allow it to be corrected in TRACS. Redress requests that might arise with respect to the various data collections stored and used in TRACS would be handled by the program through which the data was collected (e.g., CBP, DOS, or US-VISIT). Alternatively, individuals may submit their redress requests to US-VISIT, which will forward the request to the appropriate collecting organization.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

DHS has documented standard operating procedures to determine which users may access TRACS. The minimum requirements for access to TRACS information are documented and include a DHS security clearance, security and privacy training, and the need-to-know, based on job responsibility.

Access to TRACS is assigned based on the specific roles of the users. Roles are created for each level of access required for individuals to perform their jobs. Roles include data analyst, data analyst with promotion capabilities, recommendations, final determinations, view only, and database administrator. Access roles are assigned by a supervisor and are reviewed regularly to ensure that users have the appropriate access. Accounts for individuals who no longer require access are deactivated. Access is audited, and the audit logs are reviewed.

8.2 Will Department contractors have access to the system?

Contractors will have access to the TRACS data.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

DHS requires that all users of TRACS be trained on general security and privacy issues.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Phase 1 of TRACS was recently evaluated to ensure that it will be in full compliance with requirements of the Federal Information Security Management Act of 2002 (FISMA). TRACS has been certified and accredited as part of the larger US-VISIT Local Area Network Accreditation for a minor application as of April 2008. Later phases will be certified and accredited as a stand-alone system.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

TRACS secures its data by complying with the requirements of DHS information technology security policy, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. TRACS will be periodically evaluated to ensure that it complies with these security requirements.

8.9 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

TRACS is located in a secure DHS location. TRACS and its location are protected by a robust security program that employs physical, technical, and administrative controls. Users have limited access based on their roles. Users are trained in the handling of personally identifiable information (PII). All of these controls are currently undergoing evaluation that will lead to an Authority-to-Operate through a Certification and Accreditation process.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics, and other technology.

9.1 What type of project is the program or system?

TRACS is an operational system that is comprised of standard commercial hardware and software that has been modified to meet the needs of DHS, as well as paper files, which are stored in access-controlled areas.

9.2 What stage of development is the system in and what project development lifecycle was used?

TRACS is in the development stage of the US-VISIT Enterprise Lifecycle Management Methodology (ELCM).

9.3 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

While TRACS may be used for analytic tasks, it is mainly an information management system. Even when used for analysis, because the amount of information is minimal, only information that is directly related to each individual case or investigation, does raise significant privacy concerns. The information used in the analysis has already been collected by other Government entities with the preexisting authority to do so. Each agency that contributes data to TRACS must comply with legislation as well as its own policies and procedures to protect privacy rights and civil liberties.

Responsible Officials

Paul Hasson,
Acting Privacy Officer
US-VISIT Program Office

Approval Signature

Original signed and on file with the DHS Privacy Office.
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security