Privacy Impact Assessment
for the

Arrival and Departure Information System (ADIS)

August 1, 2007

Contact Point
Claire Miller, Acting Privacy Officer
US-VISIT Program Office
(202) 298-5200

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

Abstract

This privacy impact assessment (PIA) for the Arrival and Departure Information System (ADIS) describes changes to ADIS corresponding to the publication of a new ADIS system of records notice (SORN). As now proposed, ADIS will be a Department of Homeland Security (DHS)-wide system to serve certain programs, including those of the intelligence community, that require information, in support of the DHS mission, on individuals who seek to enter or who have arrived in or departed from the United States. US-VISIT has conducted this PIA update based on these proposed changes.

Introduction

DHS is publishing this PIA, along with an update to the Privacy Act SORN for ADIS in order to expand its authority and capability to serve programs that require information on individuals who seek to enter or who have arrived in or departed from the United States. Changes to ADIS include: the addition of a routine use to allow for sharing of information with the intelligence community in support of the DHS mission to protect the United States from potential terrorist activities; the addition of a routine use for cases of identity theft; clarification on the sources of data in ADIS, which potentially includes foreign governments; and a reduction of the retention period for ADIS data. Previous PIAs covering ADIS's operations are published at www.dhs.gov/privacy.[1]

ADIS is a system 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.[2] 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 immigration status by remaining in the United States beyond their authorized stay. Other uses include assisting in determining visa or immigration benefits eligibility and providing information in support of law enforcement, intelligence, and national security investigations.

ADIS data is collected and used in connection with DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions. Additionally, ADIS data may be used to provide associated testing, training, management reporting, planning and analysis, or other administrative uses. The information is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally

[1] US-VISIT Increment 1 (December 18, 2003), Increment 2 (September 14, 2004), Update (July 1, 2005).
[2] An "alien" is defined by the Immigration and Nationality Act as anyone who is not a citizen or national of the United States. 8 U.S.C. § 1101 (a)(3).

identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies.

Consistent with DHS's information sharing limitations, information stored in ADIS may be shared with other DHS components, as well as appropriate federal, state, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in the Privacy Act SORN for ADIS.

ADIS is owned by the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. However, the data in the system is owned by the organization that had the original authority to collect the data, such as U.S. Customs and Border Protection (CBP), which collects the data of individuals who cross the border. This PIA update will focus specifically on the changes outlines above (specifically in paragraph one of this Introduction) as well as provide an overview of ADIS information collection and use.

Section 1.0
Information collected and maintained

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

1.1 What information is to be collected?

ADIS collects biographic, biometric indicator, and encounter data. Biographical data may include, but is not limited to, name, date of birth, nationality, and other personal descriptive data. Biometric indicator data may include, but is not limited to, fingerprint identification numbers. Encounter data provides the context of the interaction between the immigrant or non-immigrant and the border management authority. This data may include, but is not limited to, encounter location, document types, document numbers, document issuance information, and address while in the United States. The most common data types and the primary systems from which they come are presented in the table in section 1.2.

ADIS stores the biometric Fingerprint Identification Number (FIN) which is related to the biometric data stored in the Automated Biometric Identification System (IDENT), another US-VISIT system[3]. Thus, retrieving data from one system may point to additional information in the other.

[3] See US-VISIT IDENT PIA published July 31, 2006 and updated on May 25, 2007 at

1.2 From whom is information collected?

Data is collected by various government programs and transmitted to ADIS. Data may be transmitted on a real-time basis from DHS internal or external interconnected systems, or data may be transmitted on a single-time ad hoc basis. From within DHS, data may be collected from individuals by such agencies as CBP, Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), or any other DHS agency in support of a DHS mission. From outside DHS, data may be collected from such external organizations as the Department of State (DOS), foreign government border management agencies, or other organizations that collaborate with DHS in pursuing DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.

The data in ADIS comes primarily from the ICE Student and Exchange Visitor Information System (SEVIS), the USCIS Computer Linked Applications Information Management System (CLAIMS 3), the Passenger Processing Component of the CBP Treasury Enforcement Communications System (TECS), and US-VISIT IDENT. The data elements from each system are identified in the following table.

	TECS	SEVIS	CLAIMS	IDENT
Complete Name	X	X	X	X
Date of Birth	X	X	X	X
Citizenship	X			X
Sex	X	X	X	X
Travel Document Information	X			X
Fingerprint ID Number	X			X
Watchlist Match	X			X
Nationality	X	X	X	
Carrier Code	X			
Vessel Port	X			
Vessel Name	X			
PNR Number	X			
Arrival Information	X			
Departure Information	X			
U.S. Destination Address	X		X	
Passenger Status	X			
Class of Admission	X			
Admit until Date	X			

	TECS	SEVIS	CLAIMS	IDENT
Country of Residence	X			
Visa Information	X	X		
Passport Information	X	X	X	
SEVIS ID		X	X	
SEVIS Status		X		
Country of Birth			X	
A-Number			X	
I-94 Number			X	
SSN			X	

Although some of the personal information received by ADIS is duplicative, this is an intentional mechanism designed to ensure the accuracy of the information.

1.3 Why is the information being collected?

There is no change to the purpose for which the data is being collected. Biographic, biometric indicator, and encounter data associated with aliens who have applied for entry, entered, or departed from the United States are being collected and stored in ADIS to support DHS mission activities. It is the primary repository of data held by DHS for pre-entry, entry, status management, and exit tracking of immigrants and non-immigrants. This data may be used in connection with national security, law enforcement, immigration, intelligence, and other DHS mission-related purposes. Similar data may be collected from multiple sources to verify or supplement existing data and to ensure a high degree of data accuracy.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

The authorities to collect and record the data contained in ADIS are 6 U.S.C. 202; 8 U.S.C. 1103, 1158, 1201, 1225, 1324, 1357, 1360, 1365a, 1365b, 1372, 1379, and 1732.

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

As the primary DHS system for the storage and use of biographic, biometric indicator, and encounter data bearing on the entry status of immigrants and non-immigrants throughout the pre-entry, entry, status management, and exit processes, ADIS relies on the collection of data from various external and DHS internal organizations. Consequently, ADIS must rely on the other organizations to ensure that the data is collected appropriately and within the bounds of their

individual legal authority. While in some cases ADIS data may be derived from records related to entry or exit data of foreign countries collected by foreign governments in support of their respective entry and exit processes, records collected from foreign governments must relate to individuals who have entered or exited the United States at any time, i.e., the individual must have an existing record in ADIS. The same ADIS data type may come from more than one source so that ADIS can compare and update data to ensure it is of the greatest accuracy possible.

US-VISIT, as the owner of ADIS and the steward of the data within ADIS, has developed a formalized data stewardship program that reviews proposed new data to ensure that the data types and sources are appropriate for ADIS and that the storage and/or processing requested from ADIS is/are being made to support a DHS mission. Privacy risks associated with specific data collections are described in the appropriate associated program PIA.

Section 2.0
Uses of the system and the information

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

2.1 Describe all the uses of information.

ADIS data is used for near real-time entry and exit status tracking throughout the immigrant and non-immigrant pre-entry, entry, status management, and exit processes, based on data collected by DHS or other federal or foreign government agencies and used in connection with DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions It is also used to provide associated testing, training, management reporting, planning and analysis, or other administrative uses.

Specifically, the ADIS data may be used to identify lawfully admitted non-immigrants who remain in the United States beyond the period of authorized stay, which may have a bearing on an individual's right or authority to remain in the country or receive governmental benefits; to assist DHS in supporting immigration inspection at ports of entry (POEs) by providing quick retrieval of biographic and biometric indicator data on individuals who may be inadmissible to the United States; and to facilitate the investigation process of individuals who may have violated their immigration status or may be subjects of interest for law enforcement or intelligence purposes. The current expansion will specifically allow for the collection of additional sources of data, such as information from foreign governments, on individuals associated with United States entries and exit. This additional data collection is done to validate or improve the accuracy of information currently held by ADIS. Furthermore, the use of ADIS data by intelligence agencies will support the DHS mission of protecting the United States from potential terrorist activities.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

ADIS does not conduct data mining. However, the ADIS data may be used as a source in data mining done to support DHS national security, law enforcement, immigration, intelligence, or other DHS mission-related functions. Any use of the data in this manner must be approved by the data owner and supported by the required documentation, e.g. SORNs, PIAs, and Memoranda of Understanding (MOUs) between the parties.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Much of the functionality of ADIS relies on its ability to match encounters either one to one (i.e., is this the same person we previously encountered with this identity?) or one to many (i.e., have we ever encountered this person before?). This means that great value is placed on the accuracy, currency, and completeness of the information collected and transmitted to ADIS. However, because of the diverse environments in which the information is collected, accuracy, completeness, and currency may vary considerably. In most cases, the organization from which ADIS receives data is the original collector and that organization attempts to verify the data with the individual from whom the data was collected. In addition, in the case of data received from foreign governments' border management organizations, the same ADIS data type may come from more than one source so that ADIS can compare and update data to ensure it is of the greatest accuracy possible.

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.

In order to reduce the risk of misuse or inappropriate use of information, US-VISIT has implemented information technology (IT) security processes, including audit logs and password protections. Additionally, DHS employees and contractors are trained on the appropriate use of the personally identifiable information.

As part of the standard process for accepting data, data is checked for a minimum level of quality and completeness. ADIS has extensive system and manual processes to help ensure the highest possible degree of data accuracy, completeness, and currency. This allows DHS to know, with the greatest degree of certainty possible, whether an individual has actually left the United States. All new uses of ADIS data are analyzed as part of the PIA process or in the development of

data sharing agreements, as applicable, to ensure that they support one or more DHS missions. The PIA and/or data sharing agreements define the controls that will be in place to ensure that data is used in accordance with the allowed uses. Data sharing agreements stipulate proscribed and permitted activities and uses, auditing requirements, and integrity controls.

Risks associated with information accuracy are substantially mitigated by the storing of duplicative information from ADIS's various sources. Any duplicative information is confirmed by other sources. For example, data could be received from foreign governments' border management organizations to verify or update existing ADIS data. Any inconsistent information is resolved as part of the investigation for which the information was retrieved or other related activities conducted by the ADIS user.

Section 3.0 Retention

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

3.1 What is the retention period for the data in the system?

The ADIS SORN published in 2003 (68 FR 69412) indicated a retention period of 100 years. In order to align more closely with IDENT, which holds most of the biometric data to which the ADIS biometric associated data relates, the SORN revision to be published simultaneously with this PIA proposes retaining the data in ADIS until the statute of limitations has expired for all criminal violations or until the data is older than 75 years, whichever is longer.

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

The modification to the retention schedule as described above is currently in development with NARA.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

ADIS was originally developed for the Immigration and Naturalization Service (a predecessor to DHS). Its retention period of 100 years was established when the system was used primarily for holding the biographic and encounter data on subjects of interest in immigration

and border management or law enforcement activities. However, as a DHS-wide repository of biographic, biometric indicator, and encounter data for DHS missions, ADIS holds data that may not need to be held this long. In addition, as ADIS works closely with IDENT, and as much of the biometric-associated data references biometrics in IDENT, it is appropriate to align the retention policies. ADIS holds this information for immigration benefits and immigration enforcement, which can span the lifetime of an individual.

Section 4.0
Internal sharing and disclosure

The following questions are intended to define the scope of sharing within DHS.

4.1 With which internal organizations is the information shared?

As a primary DHS-wide repository of biographic, biometric indicator, and encounter data, ADIS data is collected from and shared with components throughout DHS. The primary organizations with whom ADIS shares data are ICE, USCIS, and CBP. However, ADIS may occasionally share with other DHS organizations on an ad hoc basis, such as the United States Coast Guard (USCG), Office of Intelligence and Analysis (I&A), or other departmental components who have a need to know the information.

4.2 For each organization, what information is shared and for what purpose?

ADIS data is shared, with the consent of the data owner, for DHS national security, law enforcement, immigration, intelligence, and other mission-related functions. Data may be shared to provide associated testing, training, management reporting, planning and analysis, or other administrative uses that require the use of biographic, biometric indicator, and encounter data.

4.3 How is the information transmitted or disclosed?

There is no change in the information transmission methods when ADIS data is shared. In most cases of sharing with ICE, USCIS, and CBP, the data is transmitted between ADIS and other systems on the DHS core network, an unclassified, secure wide-area network. Other types of transmission or disclosure may be required in some circumstances. The mode of transmission or disclosure will be described for each program in the PIA or MOU or other data-sharing agreement, as appropriate, associated with that particular program.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

In order to reduce the risk of misuse or inappropriate use of information, US-VISIT has implemented IT security processes, including audit logs and password protections. Additionally, DHS employees and contractors are trained on the appropriate use of the personally identifiable information. In many cases DHS internal data sharing is required to comply with statutory requirements for national security and law enforcement. In all cases, however, this data must be kept secure, accurate, and appropriately controlled. Data owners ensure that privacy risks are mitigated through relevant data sharing agreements that require physical, technical, and administrative controls.

Section 5.0
External sharing and disclosure

The following questions are intended to define the content, scope, and authority for information sharing with organizations or entities external to DHS, including federal, state, and local governments and the private sector.

5.1 With which external organizations is the information shared?

ADIS shares data with federal, state, local, tribal, foreign, or international government agencies engaged in national security, law enforcement, immigration, intelligence, and other DHS mission-related functions, as determined by DHS. The primary external organization with whom ADIS data is shared is DOS. With the publication of this PIA and SORN update, ADIS will be allowed to share data with external intelligence organizations that have an established need to know and for which the sharing is compatible with the purpose of the original collection. The data in ADIS is valuable to intelligence agencies in order to identify and minimize potential terrorist threats to the United States. The use of ADIS data in this way supports the DHS mission to protect the homeland.

5.2 What information is shared and for what purpose?

The primary purpose of this update is to allow for sharing with the intelligence community. Intelligence agencies potentially need access to the data in ADIS to fulfill their duties in identifying, investigating, and minimizing terrorist activities. Intelligence agencies will have access to the full range of ADIS data once they have established that they will use the information for a purpose which is compatible with the purpose of the original collection. ADIS data is shared, with the consent of the data owner, for DHS national security, law enforcement, immigration, intelligence, and other mission-related functions. Information may also be shared to provide

associated testing, training, management reporting, planning and analysis, or other administrative uses that require the use of biographic, biometric indicator, and encounter data.

5.3 How is the information transmitted or disclosed?

Information may be shared electronically via secure internal or external network connection or through a secure and encrypted portable media where no secure direct electronic connection is available.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

DHS has entered into MOUs or other agreements with non-DHS organizations with which ADIS shares information. These agreements provide the conditions of sharing or disclosure, including governing the protection and use of the information.

5.5 How is the shared information secured by the recipient?

There is no change to the requirements for securing shared ADIS data. External connections must be secured and documented in an interagency security agreement that outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. Organizations with which ADIS shares information must agree to maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information. Furthermore, recipient organizations must notify ADIS after they become aware of any breach of security of interconnected systems or potential or confirmed unauthorized use or disclosure of personal information.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

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

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

The expansion of sharing ADIS data with intelligence agencies supports the DHS mission of protecting the homeland from terrorism. Intelligence agencies potentially need access to the data in ADIS to fulfill their duties in identifying, investigating, and minimizing terrorist activities. Any sharing with intelligence agencies will be evaluated to ensure that the requesting agencies will use the information for a purpose which is compatible with the purpose of the original collection. Data shared with external organizations must be kept secure, accurate, and appropriately controlled. Data owners ensure that any privacy risks are mitigated through data sharing agreements that require physical, technical, and administrative controls.

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? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Notice surrounding the changes to ADIS necessitating this PIA is provided by this PIA and also by the update to the ADIS SORN and the accompanying notice of proposed rulemaking (NPRM). 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 the information.

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

There is no change to an individual's right or opportunity to decline to provide information to ADIS collections from that which was published in previous PIAs. In most cases, because of the DHS national security, law enforcement, immigration, intelligence, or other DHS mission-related purposes for which the information is collected, such opportunities to decline

may be limited or may not exist. The specific opportunities to decline are described in the PIA or other relevant documents published by the program through which the information is collected.

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

There is no change to an individual's right to consent to particular uses of information to ADIS collections from that which was published in previous PIAs. In most cases, because of the DHS national security, law enforcement, immigration, or DHS mission-related purposes for which the information is collected, no such right exists.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

In order to mitigate the risk of individuals not being aware of the collection and uses of information in ADIS, DHS has provided the ADIS SORN, a PIA, and, through the main DHS web site, US-VISIT's website and CBP's website. Notice with regard to the changes to ADIS necessitating this PIA is provided by this PIA and by the concurrently published ADIS SORN update. The extent of notice and the opportunity to provide informed consent will vary based on the particular purpose associated with the collection of the information. In many law enforcement or national security contexts, notice or the opportunity to consent would compromise the ability of an agency to perform its mission. In these cases, notice and consent may not be available. However, many uses of ADIS data may require notice and consent. Each program will describe whether notice and consent are available and, if so, how they are accomplished.

Section 7.0
Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

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

Certain information may be exempt from individual access because access to the data in ADIS could inform the subject about an investigation of an actual or potential criminal, civil, or regulatory violation, or to the existence of such an investigation, and 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, tamper with witnesses or evidence, and avoid detection or apprehension. However, in other cases, individuals may request access to their data by contacting the US-VISIT Freedom of Information Act (FOIA) Officer at FOIA Officer, US-VISIT Program, U.S. Department of Homeland Security, Washington, DC 20528. Requests for information will be evaluated by DHS on a case-by-case basis to ensure that exemptions are only taken where the request meets the specific standards set forth in 5 U.S.C. § 552a(j)(2) and (k)(2).

7.2 What are the procedures for correcting erroneous information?

Individuals may have an opportunity to correct their data when it is being collected; otherwise, they may submit a redress request as described by each program collecting the data or to the Traveler Redress Inquiry Program (TRIP), which is located on the DHS web site at www.dhs.gov/trip.

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

Redress procedures may be established and operated by the program through which the data was collected. In the case of redress requests for DHS organizations, TRIP procedures are on the DHS web site at www.dhs.gov/trip; 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.

7.4 If no redress is provided, what alternatives are available?

Redress procedures are provided.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, what procedural rights are provided, and if access, correction, and redress rights are not provided, please explain why not.

The redress requests that might arise with respect to the various data collections stored in ADIS shall be addressed by the program through which the data was collected (e.g., CBP, DOS, SEVIS, or US-VISIT). Individuals may submit their redress requests to TRIP, which will coordinate the redress requests.

Section 8.0
Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

DHS personnel and contractors will have access to the system. The primary user groups include system managers, developers, and analysts. Access will be limited to the extent required for the particular user group to complete its responsibilities. Other user groups will be discussed in the PIAs published by each program collecting the data.

8.2 Will contractors to DHS have access to the system?

Contractors will have access to the ADIS data.

8.3 Does the system use "roles" to assign privileges to users of the system?

Access to ADIS is assigned based on the specific roles of the users. Roles are created for each level of access required for individuals to perform their job functions. Examples of roles include basic user, system administrator, system auditor, and system manager.

8.4 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 ADIS. The minimum requirements for access to ADIS information are documented in security documentation and include a DHS security clearance, security and privacy training, and need based on job responsibility.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The assignment of access roles varies based on the use or disclosure of ADIS data as described in the various PIAs. However, in most cases access roles are assigned by a supervisor and are reviewed regularly to ensure that users have the appropriate access. Individuals who no

longer require access are removed from the access list. Access is audited and the audit logs are reviewed.

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

ADIS secures its data by complying with the requirements of DHS IT security policy, particularly the DHS Information Technology 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. ADIS is periodically evaluated to ensure that it complies with these security requirements.

Because ADIS contains data from a variety of sources, collected for a variety of uses, it is necessary to instantiate controls so that only those individuals making the appropriate use of the data are able to access that data. External connections must be documented and approved with both parties' signatures in an Information Sharing Agreement (ISA), which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

8.7 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 federal government users of ADIS data be trained on security and privacy issues. Some uses and sharing of ADIS data require system- or program-specific privacy training. Any specific privacy training would be defined in a specific system PIA or data sharing agreement.

8.8 Is the data secured in accordance with the requirements of the Federal Information Security Management Act of 2002 (FISMA)? If yes, when was Certification and Accreditation last completed?

The data is secured in accordance with DHS and national-level security requirements, including the FISMA requirements. ADIS was granted an authority to operate in October of 2006; this authority to operate will expire in October of 2009. Reaccreditation will be completed prior to October 2009.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

DHS has a robust security program that employs physical, technical, and administrative controls to mitigate the privacy risks noted above regarding the collection and use of personally identifiable information. These controls are validated through a Certification and Accreditation process on a regular basis. Users have limited access that is established based on their roles. Users are trained in the handling of personal information. The specific access controls for each use of information is described in the PIA relating to that use of information.

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, radio frequency identification (RFID), biometrics, and other technology.

9.1 Was the system built from the ground up or purchased and installed?

ADIS is comprised of standard commercial hardware and software which has been modified to meet the needs of DHS.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

ADIS uses a privacy risk management process based on information life-cycle analysis and fair information principles. Technical and programmatic design choices are informed by this approach, which analyzes proposed changes in terms of their life-cycle processes—collection, use and disclosure, processing, and retention and destruction—and the potential they may create for noncompliance with relevant statutes or regulations (the Privacy Act in particular) or for violations of fair information principles. When analysis determines that privacy risks may exist, either alternative design choices or appropriate technical, physical, and/or procedural mitigations are developed.

9.3 What design choices were made to enhance privacy?

Changes that would enhance or diminish privacy risks for purposes of this PIA are not being made to ADIS. Any changes that are made, or have been made in the past, are assessed using a privacy risk management process.

9.4 Privacy Impact Analysis: Given the above choices regarding technology, what privacy impacts were considered and how were they resolved?

The primary technical changes to ADIS have been the result of the expansion of the technical capability to match biographic, biometric indicator, and encounter data for investigative purposes. Any new technology proposed for adoption by ADIS is assessed using a privacy risk management process. If any privacy risks are identified as part of this risk management approach, a determination is made whether an alternative technology or other appropriate technical, physical, or administrative control can be used to mitigate the risk.

Responsible Officials

Claire Miller, Acting US-VISIT Privacy Officer
Department of Homeland Security

Approval Signature Page

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