DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[DHS–2005–0005]

Privacy Impact Assessment and Privacy Policy

AGENCY: Department of Homeland Security.

ACTION: Notice.

SUMMARY: Pursuant to the E–Government Act of 2002, the Department of Homeland Security, Bureau of Customs and Border Protection, is publishing a privacy impact assessment and privacy policy concerning the Advanced Passenger Information System.

DATES: Written comments must be received on or before May 9, 2005.

ADDRESSES: You may submit comments, identified by Docket Number DHS–2005–0005, by one of the following methods:

- EPA Federal Partner EDOCKET Web site: *http://www.epa.gov/feddocket*. Follow the instructions for submitting comments on the Web site.
- Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.
- Mail: Comments by mail are to be addressed to the Bureau of Customs and Border Protection, Office of Regulations and Rulings, 1300 Pennsylvania Avenue, NW. (Mint Annex), Washington, DC 20229. Comments submitted by mail may be inspected at the Bureau of Customs and Border Protection at 799 9th Street, Washington, DC. To inspect comments, please call (202) 572–8768 to arrange for an appointment.

Instructions: All submissions received must include the agency name and docket number for this privacy impact assessment. All comments received, including any personal information, will be posted without change to *http://www.epa.gov/feddocket*.

Docket: For access to the docket to read background documents or comments received, go to *http://www.epa.gov/feddocket*. You may also access the Federal eRulemaking Portal at *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: Charles Perez, Program Manager, Office of Field Operations, Bureau of Customs and Border Protection at (202) 344–2605 or Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security at (202) 772–9848.

SUPPLEMENTARY INFORMATION: Elsewhere in the **Federal Register** today, the Department of Homeland Security, Bureau of Customs and Border Protection (CBP), is publishing a final rule concerning the Advanced Passenger Information System (APIS). The rule requires that all commercial inbound and outbound air and sea carriers submit certain data on all passengers and crew members prior to entry to or departure from the United States. The data that must be provided includes the following: the country that issued the passport or alien registration number; the passenger or crew member's full name, date of birth, passport or alien registration number, country of residence, and U.S. destination address (foreign nationals only); and the locator number for the passenger's airline reservation data. For crew members and non-crew members,[1] the address of permanent residence and the pilot certificate number are also required.

Pursuant to the CBP Final Rule, the APIS data must be submitted to CBP by the carrier: (i) For passenger flights into the United States, 15 minutes after departure from a foreign port or place; (ii) for passenger flights departing the United States, 15 minutes prior to departure from the United States; (iii) for crew members (on passenger and all-cargo flights) and non-crew members (limited to all-cargo flights), 60 minutes prior to the departure of any covered flight[2] from a foreign port, the U.S. port of departure, or the U.S. port of arrival en route to a second U.S. port, as applicable; (iv) for vessel arrivals, no later than 24 hours and up to 96 hours prior to the vessel's entry at a U.S. port, depending on the length of the voyage; and (v) for vessel departures, no later than 15 minutes prior to the vessel's departure from a U.S. port. The CBP Final Rule also requires the carrier industry to submit APIS data in an electronic interchange approved by CBP.

In connection with this final rule, and in accordance with Section 208 of the E-Government Act of 2002, which requires federal agencies to conduct a privacy impact assessment when they use information technology to collect new information or make significant changes in existing information technology collections, the Department of Homeland Security conducted a Privacy Impact Assessment of APIS, and developed a privacy policy for this program. The privacy impact assessment and privacy policy are attached as appendix 1 to this notice, in keeping with the statutory requirement that such documents be published.

Dated: March 21, 2005.

Nuala O'Connor Kelly,

Chief Privacy Officer, Department of Homeland Security.

Appendix 1—Privacy Impact Assessment and Privacy Policy; Advance Passenger Information System (APIS) Program

The Aviation and Transportation Security Act of 2001 and the Enhanced Border Security and Visa Reform Act of 2002 together mandated the collection of certain information on all passenger and crew members who arrive in or depart from the United States on a commercial air or sea carrier. The information required to be collected and submitted to the Advance Passenger Information System (APIS) can be found on routine entry documents that passenger and crew members must provide when processed into or out of the United States. The APIS information includes full name, date of birth, citizenship, passport/alien registration card number, passport/alien registration card country of issuance, passport expiration date country of residence and U.S. destination address (where applicable). The APIS information is collected in advance of a passenger's arrival or departure from the United States in order to perform law enforcement queries to identify security risks to the aircraft or vessel, to its occupants, or to the United States and in order to expedite CBP processing.

Advance Passenger Information System (APIS)—Privacy Impact Assessment

I. Introduction

The Advance Passenger Information System (APIS) was developed as a voluntary program by the former United States Customs Service (Customs Service) in 1989 in cooperation with the former United States Immigration and Naturalization Service (INS) and the airline industry. Air carriers and sea vessels collected passengers' biographical data and transmitted the data to the Customs Service while the flight or the vessel was en route. The Customs Service Data Center used APIS data to perform a check against the combined Federal law enforcement database known as the Interagency Border Inspection System (IBIS). Through the voluntary APIS program, these checks were performed in advance of arrival and quickly referenced once the passengers arrived. This resulted in a significant time savings for the passengers and carriers.

In the Aviation and Transportation Security Act of 2001 (ATSA) and the Enhanced Border Security and Visa Reform Act of 2002 (EBSA), Congress made mandatory the collection of certain information on all passenger and crew

[1] ''Non-crew member'' means air carrier employees and their family members and persons traveling onboard a commercial aircraft for the safety of the flight (such as an animal handler when animals are onboard). The definition of ''non-crew member'' is limited to all-cargo flights. (On a passenger or dual flight (passengers and cargo), air carrier employees, their family members, and persons onboard for the safety of the flight are considered passengers).

[2] A ''covered flight'' is one to, from, continuing within, or overflying the United States.

members who arrive in, depart from, or transit through the United States on a commercial air or sea carrier, and, in the case of foreign crew members, those who continue domestically on a foreign carrier. The purpose of this collection is to identify high risk passengers and crew members who may pose a risk or threat to vessel or aircraft safety or to national security, while simultaneously facilitating the travel of legitimate passengers and crew members. As mentioned above, this information collection also assists in immigration processing at ports of entry, resulting in a significant time savings.

To implement the mandatory collection of APIS information under ATSA and EBSA, the Customs Service issued an interim regulation (see 19 CFR 122.49a), 66 FR 67484 (December 31, 2001), as amended 67 FR 42712 (June 25, 2002) (Interim Regulation), mandating the transmission of APIS data for all inbound commercial air carriers. The INS issued a Notice of Proposed Rulemaking (NPRM) on January 3, 2003, expanding these requirements to outbound commercial air carriers and inbound and outbound commercial sea carriers. (*See* 68 FR 292.) With the creation of the Department of Homeland Security (DHS), the inspection and patrol functions of the former INS were incorporated in the U.S. Customs Service which was renamed United States Customs and Border Protection (CBP) under DHS. CBP is now responsible for border enforcement activities, including the collection of APIS information.

To carry out its statutory responsibilities, CBP is now issuing a final rule to require the submission of certain biographical data to CBP through APIS prior to a passenger's or crew member's entry into and exit from the United States. CBP's final rule also provides small air and sea carriers, which do not have the means to transmit data through APIS, a web site to collect this information in the required timeframe. In keeping with the requirements of Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act, the mandatory collection of information required by APIS is the subject of this Privacy Impact Assessment.

II. System Overview

What Information Is To Be Collected

The information to be collected from passengers and crew members by the air and sea carrier industry consists of: Complete name, date of birth, gender, country of citizenship, passport/alien registration number and country of issuance, passport expiration date, country of residence, travel document type, U.S. destination address for foreign nationals (other than those in transit), and the passenger name record locator number.[1] Most of the information collected is contained in the machine-readable zone (MRZ) of an official travel document such as a passport or alien registration card. When a traveler checks in for an international flight, the airline representative will swipe the traveler's travel document through a document reader designed to electronically capture specific information and populate the carrier's computer screen. The carrier will also collect and transmit to CBP the U.S. destination address (foreign nationals only, other than those in transit) and country of residence, which is not contained in the MRZ.

In addition to collecting information directly from the traveler, the carrier also must transmit to CBP the following supplementary information: Foreign airport/port where the passengers and crew members began their air transportation to the United States; for passengers and crew member destined for the U.S. the location where the passenger will be processed through customs and immigration formalities; and for passengers and crew members that are transiting through the U.S. and not clearing customs and immigration formalities, the foreign airport of ultimate destination, and status on board (whether an individual is crew or non-crew). Finally, information also is collected about the particular flight or voyage, such as date of arrival/departure, carrier name, flight number, departure location, arrival location, country of registry.

Why the Information Is Being Collected and Intended Use of the Information

The information is being collected pursuant to the ATSA and the EBSA. The purpose of the collection is to screen passengers arriving from foreign travel points and departing the United States to identify those passengers who (1) may pose a risk to the transportation industry, to other travelers and to the United States, (2) are identified as or suspected of being a terrorist or having affiliations to terrorist organizations, (3) have active wants and warrants for criminal activity, (4) are currently inadmissible, or have been previously deported from the United States, or (5) are subject to other intelligence that may identify them as a security risk.

At the same time, the system allows CBP to facilitate effectively and efficiently the entry of legitimate travelers into the United States. As travelers arrive into the United States, through APIS, CBP officers can quickly reference the results of the advanced research that has been conducted through CBP's law enforcement databases, confirm the accuracy of that information by comparison of it with information obtained from the traveler and from the carriers, and make immediate determinations as to a traveler's security risk and admissibility.

How Will Information Be Checked for Accuracy?

Upon a traveler's arrival into the United States, a CBP officer verifies that the data transmitted by the carrier is the same as that on the traveler's travel documents. If discrepancies are found, a CBP officer can correct the data at the point of entry and update the information. Additionally, CBP audits and tracks the sufficiency and error rates of individual carrier transmissions to APIS and may assess penalties against carriers that fail to transmit APIS data within system parameters on a recurring basis or incur large error rates in the review of their transmissions. CBP also performs periodic audits and routine maintenance on its Information Technology Systems to ensure that system protocols and programming remain intact and operational.

Will the System Derive New Data or Create Previously Unavailable Data About an Individual Through Aggregation From the Information Collected?

Certain APIS data is maintained and examined in order to view an individual's travel history. In addition to maintaining an individual's travel record, this data is aggregated with information from law enforcement databases to assist CBP employees in making determinations as to a traveler's security risk and admissibility into the United States.

What Notice Is Given and What Opportunities Does an Individual Have To Consent?

CBP has provided notice through publication of its Interim Regulation (*see* 66 FR 67484; as amended 67 FR 42712), the NPRM (*see* 68 FR 292), as well as this privacy impact assessment and its privacy policy, which is being published simultaneously.

Clearance for the arrival or departure of a commercial vessel or aircraft may be contingent upon the submission of passenger and crew manifest information to CBP through APIS.

A foreign traveler who declines to provide APIS information to a carrier is inadmissible to the United States. Such an individual may withdraw his or her application for admission, or be subject to removal proceedings.

United States citizens who refuse to provide the information to the air or sea carrier may be subject to action by that particular carrier. A carrier may prohibit the person from traveling. However, if the carrier allows the passenger to board without providing the required information, the person will be subject to security checks upon arrival.

III. APIS System Architecture

APIS is a system that resides within the Treasury Enforcement Communications System (TECS), a law enforcement database. (The most recent System of Records Notice for TECS can be found at 66 FR 52984 (October 18, 2001).) APIS comprises a subset of the data collected and maintained within TECS. The data particular to APIS is accessed through functionality that is separate from data within TECS. Certain APIS data (complete name, date of birth, date of arrival, date of departure, time arrived, means of arrival (air/sea), immigration lane, ID inspector, travel document, departure location, airline code and flight number, and result of the CBP processing) is moved to the general TECS database once an individual traveler has cleared immigration.

The APIS data is cross-referenced or compared against other law enforcement data maintained in TECS. These cross-references and comparisons occur through IBIS. IBIS resides in TECS and provides access to the National Crime Information Center (NCIC), which allows users to interface with all 50 states via the National Law Enforcement Telecommunications System (NLETS). IBIS

[1] The Passenger Name Record locator number allows CBP to access PNR if necessary, consistent with its regulatory authority under 19 CFR 122.49b.

also contains the names of individuals on terrorist watch lists.

IV. Maintenance and Administrative Controls on Access to the Data

With Whom the Information Will Be Shared

The personal information collected and maintained by APIS will be accessed by employees of DHS components. Strict security and access controls are in place to ensure that only those personnel with a need for the information in the performance of their official duties will be able to access information in the system.

Additionally, the information may be shared with other federal, state, local or foreign agencies responsible for investigating or prosecuting violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where DHS becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation. The system of records notice for TECS, where APIS data reside, provides notice as to the conditions of disclosure and routine uses for the information collected by APIS, and provides that any dissemination of information maintained within APIS be compatible with the purpose for which the information originally was collected.

As discussed previously, certain APIS data are transferred to the general TECS database after a traveler has cleared immigration. The information transferred to and stored in the general TECS database includes: Complete name, date of birth, date of arrival, date of departure, time arrived, means of arrival (air/sea), immigration lane, ID inspector, travel document, departure location, airline code and flight number, and result of the CBP processing. APIS is the source data for this travel information stored in the general TECS database.

For individuals subject to US–VISIT requirements, certain APIS data also is transferred to the Arrival and Departure Information System (ADIS) for effective and efficient tracking of foreign nationals. This information includes: Complete name, date of birth, gender, nationality, U.S. destination address, passport number, country of issuance,[2] alien registration number, port of entry, entry date, port of departure, and departure date.

Retention and Destruction

APIS information, which is used at the port of entry for verification purposes, is retained temporarily in the APIS component of the TECS system for no more than 12 months from the date of collection at which time the data is erased from the APIS component of the TECS system. Information that is transferred to the general TECS database (as described above) will be maintained for as long as operationally necessary, subject to retention reviews that occur both periodically and each time information is accessed, but in no case will information be retained longer than fifty years past the date of collection. Information that is transferred to ADIS (as described above) is maintained for 100 years in accordance with the retention period of the ADIS system of records notice.

[2] For non-immigrants authorized to work.

How the Information Will Be Secured

APIS, as a component of TECS, is approved through the TECS Certification and Accreditation (C&A) under the National Institute of Standards and Technology. The last certification was on February 23, 2003. Although APIS is currently under the TECS C&A, it will have its own certification and accreditation in calendar year 2005, to provide specific assurances regarding the safety and security of APIS data.

APIS information is secured in full compliance with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules, which will be applied to component systems, communications between component systems, and at interfaces between component systems and external systems.

One aspect of the DHS comprehensive program to provide information security involves the establishment of rules of behavior for each major application, including APIS. These rules of behavior require users to be adequately trained regarding the security of their systems. These rules also require a periodic assessment of technical, administrative and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. System users must also complete annual privacy awareness training to maintain current access.

APIS transactions are tracked and can be monitored. This allows for oversight and audit capabilities to ensure that the data are being handled consistent with all applicable federal laws and regulations regarding privacy and data integrity.

Data exchange, which will take place over an encrypted network between the carrier industry and CBP and between CBP and other DHS components that have access to the APIS data, is limited and confined only to those entities that have a need for the data in the performance of official duties. These encrypted networks comply with standards set forth in the Interconnection Security Agreements required to be executed prior to external access to a CBP computer system.

The eAPIS Web based system, which permits submission of manifest information over the Internet by carriers who do not have the capability to transmit electronic PNR data, is subject to the same security precautions, standards, laws, and regulations with respect to the collection, retention, and safeguarding of APIS data. Exchanges of data submitted via eAPIS will be no different than exchanges of APIS data collected by other means. eAPIS submissions will be made over an encrypted Internet portal accessed via an approved username and password.

V. Redress

CBP has created a Customer Satisfaction Unit in its Office of Field Operations to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems (including TECS, IBIS, and APIS). If the traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries should be directed to the Customer Satisfaction Unit at the following address: Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5C, 1300 Pennsylvania Avenue, NW., Washington, D.C. 20229, fax (202) 344–2791. Individuals making inquiries should provide as much identifying information as possible regarding themselves, to identify the record at issue. Individuals may provide additional information to CBP to ensure that the information maintained by CBP is accurate and complete. The Customer Satisfaction Unit will respond in writing to each inquiry.

The DHS Chief Privacy Officer will exercise comprehensive oversight of all phases of the program to ensure that privacy concerns are respected throughout the process. The DHS Chief Privacy Officer will also serve as the final review authority for all individual complaints and concerns about the program.

VI. System of Records

APIS data is a subset of the system data within the Treasury Enforcement Communications System (TECS) and is covered by the System of Records Notice for TECS. The most recent TECS publication can be found at 66 FR 52984 (October 18, 2001). APIS data is also contained in the system data for the Arrival and Departure Information System (ADIS) and is also covered by the System of Records Notice for ADIS. The most recent ADIS publication can be found at 68 FR 69412 (December 12, 2003).

Privacy Controls

APIS collects personal information necessary for its purposes. While APIS does not constitute a new system of records, the final rule requiring submission of data expands the types of data collected, the number of travelers from which the data is collected, and makes the system mandatory rather than voluntary. These changes create a potential privacy risk. This risk is mitigated, however, by establishment of the privacy policy supported and enforced by the comprehensive privacy program. This program includes mandatory privacy training for system operators and appropriate safeguards for data handling.

The APIS system collects data to be compared against an existing law enforcement database—TECS—to promote the safety and security of sea and air carriers, their passengers and the United States. Some data collected via APIS manifests is transferred to TECS and may become available for later research of the entry and exit of travelers. This presents a potential privacy risk. This risk is mitigated in several ways. First, APIS data is controlled by separate functionality within the TECS system from other data maintained in that system. While the APIS data may be compared against other data maintained in TECS, this action requires an affirmative act by the user that is subject to regular agency review and audit. Second, the TECS system,

and APIS within TECS, has its own published System of Records Notice (SORN), which explains the uses to which the data that is collected will be put. This SORN includes the purposes underlying APIS as part of its terms. This SORN assists in putting the travelling public on notice of the uses of APIS data. Third, Memoranda of Understanding and of Agreement with other agencies carefully regulate the uses for TECS data. This PIA and APIS Privacy Policy make this use of APIS data transparent.

APIS intends to ensure that the program is as transparent as possible. To that end, in addition to publishing this privacy impact assessment and the final rule, CBP has developed a comprehensive privacy policy, a copy of which is appended to this report and which is posted on the DHS Web site.

VII. Summary and Conclusions

The APIS program is based on Congressional concerns with improving the safety and security not only of sea and air carriers and their passengers, but also the national security of the United States. Requirements for the program, including the implementation of an integrated and interoperable passenger manifest screening system, are established by various provisions of the Aviation and Transportation Security Act of 2001 and the Enhanced Border Security and Visa Reform Act of 2002. These requirements include, in particular, the integration of arrival, departure, and transit data on all passengers and crew members traveling and listed on commercial sea or air carrier manifests; and integration of this information with other law enforcement and security systems.

CBP structured the APIS program, as promulgated in the final rule, to foster the goals of these statutes, mindful of the need to protect the privacy of the individuals whose data is being collected. This PIA examines the potential privacy risks and describes those actions CBP has taken to mitigate these risks.

Contact Point and Reviewing Official

Contact Point: Charles Perez, Program Manager, Office of Field Operations, U.S. Customs and Border Protection, (202) 344–2605.

Reviewing Official: Nuala O'Connor Kelly, Chief Privacy Officer, DHS, (202) 772–9848.

Advance Passenger Information System (APIS)—Privacy Policy

What Is the Purpose of the APIS Program?

The Aviation and Transportation Security Act of 2001 and the Enhanced Border Security and Visa Reform Act of 2002 together mandated the collection of certain information on all passenger and crew members who arrive into or depart from the United States on a commercial air or sea carrier. The Advance Passenger Information System (APIS) information is collected in advance of a passenger's arrival into the United States in order to perform law enforcement queries to identify security risks to the aircraft/vessel, its occupants, and the United States. The information is also used to verify departure when the traveler leaves the United States at the conclusion of a visit.

Who Is Affected by the Program?

All travelers and crew members who arrive and depart the United States, all crew members on aircraft who fly over the United States, and crew members on foreign aircraft who arrive from an international departure location and continue domestically within the United States are covered by the APIS Program.

What Information Is Collected?

The information to be collected from passengers and crew members by the air and sea carrier industry consists of: complete name, date of birth, gender, country of citizenship, passport/alien registration number and country of issuance, passport expiration date, country of residence, travel document type, U.S. destination address for foreign nationals (other than those in transit), and the passenger name record locator number.[3] Most of the information collected is contained in the machine-readable zone (MRZ) of an official travel document such as a passport or alien registration card. When a traveler checks in for an international flight, the airline representative will swipe the traveler's travel document through a document reader designed to electronically capture specific information and populate the carrier's computer screen. The carrier will also collect and transmit to CBP the U.S. destination address (foreign nationals only, other than those in transit) and country of residence, which is not contained in the MRZ.

In addition to collecting information directly from the traveler, the carrier also must transmit to CBP the following supplementary information: Foreign airport/port where the passengers and crew members began their air transportation to the United States; for passengers and crew member destined for the U.S. the location where the passenger will be processed through customs and immigration formalities; and for passengers and crew members that are transiting through the U.S. and not clearing customs and immigration formalities, the foreign airport of ultimate destination, and status on board (whether an individual is crew or non-crew). Finally, information also is collected about the particular flight or voyage, such as date of arrival/departure, carrier name, flight number, departure location, arrival location, country of registry.

How Is the Information Used?

The purpose of the information collection is to screen passengers arriving from foreign travel points and departing the United States to identify those passengers who (1) may pose a risk to the transportation industry, to other travelers and to the United States, (2) are identified as or suspected of being a terrorist or having affiliations to terrorist organizations, (3) have active warrants for criminal activity, (4) are currently inadmissible, or have been previously deported from the United States, or (5) are subject to other intelligence that may identify them as a security risk.

[3] The Passenger Name Record locator number allows CBP to access PNR if necessary, consistent with its regulatory authority under 19 CFR 122.49b.

At the same time, the system allows CBP to facilitate effectively and efficiently the entry of legitimate travelers into and through the United States. As travelers arrive into the United States, CBP officers can quickly reference the results of the advanced research conducted through the law enforcement databases and make immediate determinations as to a traveler's security risk and admissibility.

Is the Collection of APIS Data Duplicative of Data Collected by the US–VISIT?

No. US–VISIT does not, in itself, collect traveler manifest data. US–VISIT coordinates the exchange of data collected by existing systems that are utilized by the Department of Homeland Security (DHS), such as the APIS system operated by CBP.

Will the Collection of APIS Data Be Duplicative of the Data Required by the Secure Flight Program as Proposed by the Transportation and Security Administration?

No. The Secure Flight Program is proposed only for domestic carriers transporting travelers within the United States. APIS is restricted to passengers entering and exiting the United States and crew members entering, exiting, overflying, and continuing domestically on a foreign carrier.

Who Will Have Access to the Information?

The personal information collected and maintained by APIS will be accessed by employees of DHS components. Strict security and access controls are in place to ensure that only those personnel with a need for the information in the performance of their official duties will be able to access information in the system.

Additionally, the information may be shared with other federal, state, local, or tribal or foreign agencies responsible for investigating or prosecuting violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where DHS becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

How Will the Information Be Protected?

Personal information will be kept secure and confidential and will not be discussed with, nor disclosed to, any person within or outside the APIS program other than as authorized by law and as required for the performance of official duties. Careful safeguards, including appropriate security controls, will ensure that the data is not used or accessed improperly. The APIS functionality is a part of the Treasury Enforcement Communications System (TECS), a law enforcement database. Its accreditation is in accordance with the CBP Information Systems Security Policy and Procedures Handbook (CIS HB 1400–05A, dated June 22, 2001) and with National Information Standards and Technology (NIST) guidance. The TECS system was certified and accredited on February 23, 2003. APIS also will have individual certification utilizing the NIST guidance in calendar year 2005.

Roles and responsibilities of DHS employees, system owners and managers,

and third parties who manage or access information in the APIS program include:

1. DHS Employees and Contractors

As users of APIS systems and records, DHS employees shall:

- Access records containing personal information only when the information is needed to carry out their official duties.
- Disclose personal information only for legitimate government purposes and in accordance with applicable laws, regulations, and applicable policies and procedures.

2. Owners/Managers of the DHS Systems Storing APIS Data

System Owners/Managers shall:

- Follow applicable laws, regulations, APIS program guidance and DHS policies and procedures in the development, implementation, and operation of information systems under their control.
- Conduct a risk assessment to identify privacy risks and determine whether it is necessary and appropriate to implement additional security controls to protect against the risk.
- Ensure that only personal information that is necessary and relevant for legally mandated or authorized purposes is collected.
- Ensure that all business processes that contain personal information have an approved Privacy Impact Assessment, which meets appropriate DHS and OMB guidance and which is updated as the system progresses through its development stages.
- Ensure that all personal information is protected and disposed of in accordance with applicable laws, regulations, APIS program guidance and DHS policies and procedures.
- Use personal information collected only for the purposes for which it was collected, unless other purposes are explicitly mandated or authorized by law.
- Establish and maintain appropriate administrative, technical, and physical security safeguards to protect personal information.

How Long Is Information Retained?

APIS data is subject to temporary and permanent retention requirements. The information initially collected by APIS is used for entry screening purposes and is retained for twelve months. Certain data obtained through the APIS transmission (complete name, date of birth, date of arrival, date of departure, time arrived, means of arrival (air/sea), primary inspection, ID inspector, travel document, departure location, airline code and flight number, and result of the CBP processing), however, is moved to the general TECS database once an individual traveler has cleared primary inspection. Other information is transferred to the Arrival and Departure Information System (ADIS) for US–VISIT purposes. The transferred data is retained in accordance with the retention schedules approved for TECS and ADIS, as applicable. In general, information stored in the TECS database will be retained for as long as operationally necessary, subject to retention reviews that occur both periodically and each time information is accessed, but in no case will information be retained longer than fifty years past the date of collection. Information stored in ADIS will be retained consistent with the retention schedule for that records system (100 years).

Is a Form of Redress Available?

CBP has created a Customer Satisfaction Unit in its Office of Field Operations to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems. Inquiries should be addressed to: Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5C, 1300 Pennsylvania Avenue, NW., Washington, DC 20229, fax (202) 344–2791. Individuals making inquiries should provide as much identifying information as possible, to identify the record at issue.

The DHS Chief Privacy Officer will exercise comprehensive oversight of all phases of the program to ensure that privacy concerns are respected throughout the process and will also serve as the final review authority for all individual complaints and concerns about the program.

For Further Information Contact:

Charles Perez, Program Manager, APIS, Office of Field Operations, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW., Washington, DC 20229, Tel: (202) 344–2605.

Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, Tel: (202) 772–9848.

[FR Doc. 05–6522 Filed 4–6–05; 8:45 am]

BILLING CODE 4410–10–P