Exhibit H

Privacy Impact Assessment

for the

Global Enrollment System

April 20, 2006

Contact Point
Sandra Faye Scott
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-2548

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Introduction

The Global Enrollment System (GES) is an information technology (IT) system that consolidates the enrollment and vetting processes for individuals who voluntarily exchange personally identifiable information in return for expedited transit at U.S. border entry points.

U.S. Customs and Border Protection (CBP), a bureau within the Department of Homeland Security (DHS), currently operates different "trusted traveler" programs[1] at designated border ports of entry to expedite the processing of pre-approved, international, low-risk travelers effectively and efficiently through the border. (*see*, Appendix 1 for a list of existing trusted traveler programs). Several of the identified "trusted traveler" programs predate the creation of DHS and CBP and were designed and implemented by predecessor agencies such as the Immigration and Naturalization Service (INS) and the U.S. Customs Service. As a result, the biographical and biometric data currently collected from applicants and participants in the programs are stored through the use of localized application/enrollment processes and several stand-alone, port of entry level databases.[2] As these programs all essentially conduct application, enrollment, and background checks in similar fashions, CBP has developed a single, consolidated, and more efficient national approach to support each of these programs, which adopts the Global Enrollment System (GES) name, nationally.

CBP is in the process both of re-designing the IT system architecture for the existing trusted traveler programs, and designing additional programs. This PIA covers both the re-design of the architecture of the existing trusted traveler programs in order to consolidate the programs into the national GES system, and the addition of two new trusted traveler programs:

- Enrollment system for low-risk, international air passengers traveling through John F. Kennedy Int'l (JFK) Airport in Jamaica, New York, Houston Intercontinental Airport, Houston, Texas, and Washington Dulles International Airport, Dulles, Virginia, and
- Small Boat Reporting – for low-risk owners and operators of private or pleasure craft.

This Privacy Impact Assessment (PIA) will be updated as new programs are added to GES.

CBP will combine all of the port of entry GES databases into one fully integrated GES system. The integrated version of GES will contain the same data as the local information structure that currently support the existing trusted traveler programs; the only difference is that the data will reside in one place and access to the information will be controlled through headquarters. The single, integrated GES will be the backbone IT system to support all CBP trusted traveler programs and will be scalable to incorporate any future DHS-wide approach. This consolidated GES system will provide CBP with the ability to centralize many of the application and enrollment functions of

[1] Use of the term "trusted traveler" program(s) in this document is meant to also encompass and include all programs designated by DHS and/or CBP as either "registered traveler" or "trusted traveler" programs. "Trusted traveler" and "registered traveler" programs typically require the same or similar types of personnel information to be submitted by an individual; the difference between the types of programs is the greater level of vetting and screening performed upon participants in "trusted traveler" programs.

[2] The System of Records Notice for this precursor system was published by the former INS at 62 FR 11919. This system was also referred to as the Global Enrollment System. Under CBP/DHS, the local GES system of records is being updated to reflect the expansion and enhancement of the now national GES.

both existing and future "trusted traveler" programs and standardize the risk assessment processes for the programs, to offer a more efficient approach in the administration of these programs.

Current members of the trusted traveler programs will not see a change in the functioning of the program because of the consolidation of the registration information and process within the integrated GES system. GES will allow CBP/DHS to offer expanded membership opportunities into other programs without having to collect redundant data and re-vet applicants. For instance: a NEXUS Highway member will be able to apply for NEXUS Air generally without having to resubmit his or her application data and be re-vetted, as is currently the case due to the "stand alone" features of the current programs. A member of one program will simply indicate his/her desire to be considered as an applicant for another program, permitting use of the same personal information for consideration under another program's criteria.

An authorized user of the integrated GES system will have access to the information submitted by all enrolled travelers from all trusted traveler programs, regardless of where in the country the traveler is enrolled in the program. This national access within CBP will permit CBP Officers to clear trusted travelers at ports other than the port where the traveler first enrolled. As GES expands, this national access, internal to CBP, will permit more expeditious clearance for an enrolled traveler, even at ports where the particular trusted traveler program is not operational, because access to the information can still assist CBP in clearing the traveler.

The current GES systems support about 200,000 enrollees, with a projected 3 million enrolled by the end of the 10-year operational lifecycle for all programs. The integrated GES provides a scalable enrollment processing infrastructure supporting:

- enrollment application data capture;
- storage and retrieval;
- applicant biographic and biometric data capture;
- applicant vetting via interfaces to law enforcement data systems;
- issuance of enrollee identification cards and devices;
- validation of traveler enrollment and law enforcement status for border crossings and airplane boarding; and
- capture, storage and retrieval of border crossing event records.

As designed, a managed service provider (MSP) (a company contracted by the Government to provide the described services) is employed on a transaction-level basis to capture application data and serve as a fiscal intermediary for processing program fees. The MSP serves as an initial clearinghouse for applications and does not have further access to system data once the application data has been inputted. Following routine spot checks by the MSP to ensure data accuracy, the application data is destroyed and the MSP retains no access to the application data. All vetting, the

process of clearing applicants through background checks, will continue to be performed by government personnel, but the application, enrollment and vetting processes will be standardized and centralized.

Currently, system requirements have been completed by CBP's Office of Information Technology (OIT) to support GES as an enterprise-wide capability and have been published in the "DHS Enrollment System (ES) Functional and Users Requirements Document" delivered December 2004.

Trusted Traveler programs have existed for many years with no real changes. They are covered by the Global Enrollment System of Records Notice of the former Immigration and Naturalization Service (INS) in 1997 (62 FR 11919, March 13, 1997). Since the system predated the E-Government Act of 2002 and no substantial changes were made to the system thereafter, no Privacy Impact Assessment regarding GES has yet been published. Given the departmental reorganization pursuant to the Homeland Security Act of 2002 and CBP's plan to integrate the local GES enrollment systems into a networked database for all CBP trusted traveler programs, DHS deemed it appropriate for a Privacy Impact Assessment to now be completed in accordance with the guidance issued by the Office of Management and Budget (OMB) on September 26, 2003.

A revised Privacy Act System of Records Notice for GES will also be published in conjunction with this PIA to reflect structural changes in the system resulting from the government reorganization under the Homeland Security Act. As part of that reorganization, certain biometric information that would have been maintained in GES will be collected and maintained in the DHS Automated Biometric Identification System (IDENT) to minimize the redundant collection of this information in conjunction with the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program. An update of the IDENT SORN **DHS/ICE-CBP-CIS-001,** is also being published in conjunction with this PIA. This Privacy Impact Assessment is published in an effort to address any privacy concerns associated with GES and will be updated to reflect any future changes to the system.

Section 1 – The Data and its Purposes

1.1 What information is to be collected (e.g., nature and source)?

Participation in the trusted traveler programs is completely voluntary, and the applicants agree to provide personal biographical and biometric data for the purposes of conducting law enforcement based background checks and criminal history checks by officers of CBP to determine their "low-risk" status. In return, the traveler is often provided expedited (and where logistically feasible, exclusive) processing through the border. The traveler information collected and used to support enrollment in a trusted traveler program is similar to the routine information travelers provide each time they enter the U.S. By collecting it in advance and fixing the passenger's identity (through biometrics) to that set of data, CBP can use the results of the advanced inspection through the application/enrollment process to expedite the passenger's admission to the United States each time they enter.

Information will be collected through each of the trusted traveler programs and be added into GES and IDENT. GES will maintain the majority of the enrollment data for the programs. This

information includes the application data (biographic data), biometric data collected from the applicants (exclusive of fingerprints), results of the background check performed, and border crossing information.

IDENT will maintain fingerprints, both two prints from each border crossing and ten prints from the initial vetting process, limited identity information (name and birth date), and border crossing information. This information will be designated as GES data in the IDENT database in order to be easily distinguishable from non-GES data stored in IDENT. This designation will allow CBP to limit access in accordance with mission responsibilities.

The application:

Each trusted traveler program collects data either by utilizing an OMB approved application form based upon the original Immigration and Naturalization Service (INS) Form I-823, or by receiving a data transfer from the Canadian Border Services Agency (CBSA), the Canadian government agency that collects the information directly from the applicants in accordance with Canadian law[3]. Although all versions of the I-823 collect a majority of the same data elements, separate versions have received approval by OMB (and been issued a distinct form number) to reflect both the identity of the particular program and the separate timeframe in which each program was created. Both the low-risk passenger enrollment system and the Small Boat Reporting Program have received OMB approval for their individual collections of information. (*see*, Appendix 2 for a list of programs and their respective forms). During the pilot phase of both low-risk enrollment system and the Small Boat Reporting Program, and for a period of time thereafter, the various versions of the I-823 will continue to be used for all of the programs.

All applicants for trusted traveler programs will submit the applicable form for the program(s) for which they wish to apply (hereinafter described as the "applicable trusted traveler application form"), as well as the required travel documents (such as a U.S. passport or foreign passport and appropriate visa) to the requested trusted traveler program processing location. Depending on the particular application and requirements of the individual program, the applicable form collects of the following personal information: full name, place and date of birth, sex, address(es), telephone number(s), country of citizenship, alien registration number (if applicable), biometric data (such as fingerprints and photograph), driver's license number and issuing state or province, the make, model, color, year, license number and license issuing state or province of the applicant's vehicle, the flag and home port (where the vessel is foreign flagged), name, registration number and registration issuing state or province of the applicant's vessel, the name and address of the vehicle's or vessel's registered owner if different from the applicant, and the amount of fee paid, when applicable, based on requirements.

Biographic data and digital photographs already resident in the local databases for older trusted traveler programs will be placed into the national GES system and any biometric information will be placed in the IDENT system. Prior to placing data from local databases into the national systems, CBP will validate the information contained in the local databases by comparing and cross referencing data from the local databases with information contained in the national law

[3] Unlike the other trusted traveler programs, the NEXUS programs are jointly administered by CBP and the CBSA. Applicants submit application information directly to the CBSA initially and then the information is passed to CBP. In the future, as other bilateral agreements are reached for international participation in US PASS, a similar application sharing process may be instituted with other countries.

enforcement databases used to vet applicants. Once the data has been vetted, it will be placed in the national system. Upon completion of the transfer of data out of the local systems, those systems will be decommissioned and any remaining data will be destroyed.

The biometric data:
GES maintains full biographic information collected from trusted traveler applicants, and biometric information, consisting of a digital photograph. GES will not maintain fingerprints.

IDENT maintains ten fingerprints for initial vetting, two fingerprints from each border crossing, and limited biographic information, name and birth date, which will be used to identify those fingerprints. The ten fingerprints are sent to the FBI for vetting purposes to check against law enforcement databases, and are not maintained by the FBI. As the traveler crosses the border at the port of entry, he/she provides two index fingerprints, typically at an automated machine, to verify that they are the same individual who was initially approved as a trusted traveler and enrolled in the program. IDENT maintains a record of every encounter during which an individual's two index fingerprints are submitted and compared with the two enrollment fingerprints already stored in the system. The record includes limited biographic data, the fingerprints, and the date, time and location of where the fingerprints were collected. Presently, the SENTRI Pedestrian and NEXUS Air programs use two fingerprints to validate identity. The low-risk enrollment system and the Small Boat Reporting Program will also use fingerprints to validate identity once they are established. In lieu of using fingerprints to validate identity, certain programs such as FAST and NEXUS Highway are employing RFID (Radio Frequency Identification) cards that provide the CBP Officer with identity information, including a digital photograph for those enrolled prior to arrival at the POE, which expedites clearance.

Additional information:
GES additionally contains the results of, and pointers to, vetting information from the enrollment process, as well as border crossing information. In the vetting process, the biometric information collected at enrollment (ten fingerprints) is compared with the data held in law enforcement databases to access the applicant's background and determine if he/she is "low risk".

The main database checked during the vetting process, before individuals will be enrolled in any trusted traveler program, is the Treasury Enforcement Communication System/Integrated Border Inspection System (TECS/IBIS). TECS/IBIS contains historical and enforcement data on travelers, and provides a gateway to other sources of data. These other sources include the Terrorist Screening Database (TSDB), FBI criminal history and National Crime Information Center (NCIC) outstanding wants/warrants, vehicle and driver's license-related data contained in National Law Enforcement Telecommunication System (NLETS), and Department of State alien records, lookouts, and status indicators.

An applicant's ten fingerprints are submitted to the FBI to correlate identity checks with criminal histories located in the Integrated Automated Fingerprint Identification System (IAFIS). Fingerprints are not maintained by the FBI. An applicant's two index fingerprints[4] are also submitted to the DHS Automated Biometric Identification System (IDENT) for the purpose of

[4] In the future, IDENT will collect ten fingerprints from each person.

checking for any immigration related records on the person. The results of the background check, as well as any matching information and the final determination on membership (accepted or denied) is stored in GES, exclusively.

1.2 Why is the information being collected?

Information is being collected from voluntary applicants in order to assess whether the individuals are low risk travelers and, thus, eligible for enrollment in a GES-supported trusted traveler program. Persons eligible for the GES-supported trusted traveler programs include U.S. citizens, lawful permanent residents of the United States, and citizens of Mexico, Canada, and other nations who travel frequently to the United States. Non-U.S. citizens must have valid entry documents, be admissible to the United States, and demonstrate they are low risk travelers by providing certain documents called for by regulation (e.g., 8 CFR 235.7) in conjunction with a completed applicable trusted traveler application form for the desired program.

Much of the data collected in the application process is data that CBP Officers often already routinely encounter and utilize for official law enforcement and compliance purposes as provided for by their unique border security and search authority. By collecting and processing this passenger data in advance of travel, CBP seeks to offer expedited service for those travelers who elect to volunteer and are otherwise eligible to participate.

1.3 Is the information relevant and necessary to the purpose for which the system is being designed?

Yes. The biographical data and documentary travel data are required to ensure all applicants meet customs and immigration requirements and to assess whether an individual is appropriate for a given GES program. The biometric data is collected at enrollment and stored in both GES (digital photographs) and IDENT (two and ten fingerprints) for two primary reasons: to forward the information to the FBI for comparison with data contained in IAFIS and other law enforcement databases, and to establish the verification process of the identity of the trusted traveler, which will occur when the individual uses the designated program's alternative expedited processing lane at the time of travel (most times at an automated machine).

1.4 What is the intended use of the information?

The biographic and biometric information collected from each applicant is used and stored in GES and IDENT to help determine whether the applicant qualifies for enrollment as a low risk traveler in one or more of the trusted traveler programs. This information is checked against various Federal and State law enforcement databases before applicants are enrolled. Since border inspections are facilitated and streamlined for members of the programs, enrollment includes a detailed vetting process. In addition to using the information collected at enrollment to vet the applicant, the enrollment information may be accessed to verify identity, by CBP, as part of the operation of a particular trusted traveler program.

Trusted traveler program participants are told that they are also subject to random checks when using the GES specific travel lanes. Even though the low risk traveler is enrolled in a program, a

CBP Officer can conduct a random check at the time of entry. The random check can be either background or physical or both, indicating that it will proceed based on the progression of the secondary inspection. Such checks help to safeguard the lane's integrity. A participant found to be inadmissible when using the lanes will be processed in the same way as any other malefactor and their membership in the applicable trusted traveler program may be suspended or revoked.

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

The sources for the information housed in GES and IDENT are the following: the applicant-prepared applicable trusted traveler application form and supporting travel or other submitted documents, fingerprints collected from the applicant, digital photographs, the law enforcement databases used for vetting (TECS/IBIS, NCIC, NLETS, IAFIS, IDENT) and border crossing data collected from the traveler at time of travel.

1.6 Where and how are you acquiring the information?

The information is acquired as follows:

- Biographic information is obtained voluntarily from the applicant filling out and submitting the applicable trusted traveler application form, with supporting travel documents. This information in conjunction with any form of payment is forwarded to the MSP for entry into GES to create the traveler's account.
- Fingerprints are collected by a CBP Officer at the local enrollment center during the applicant's interview, which is conducted as part of the enrollment process. The full set of ten fingerprints is stored in IDENT with limited biographic information, name and date of birth and sent to, but not maintained by, the FBI for comparison with IAFIS. The two index fingerprints are collected during each border crossing and maintained in IDENT with limited identifying information.
- A digital photograph is taken by a CBP Officer during the same interview process at the local enrollment center.
- Queries to the law enforcement databases identified above are performed by CBP Officers at official CBP locations accessing the databases through the CBP secure data network.
- Border crossing records are created at the port of entry (POE) and stored in GES and if biometric information is taken, it is stored in IDENT every time the member uses the expedited processing lane at time of travel. Similarly, information collected by Canadian authorities as part of the NEXUS program is transmitted to and stored in GES as it is collected.

1.7 How will the information be checked for accuracy?

The initial application data is submitted by the applicant and is checked during the vetting process by CBP Officers who check multiple law enforcement databases (see Question 1 above). The data is verified again during the enrollment phase when the CBP Officer interviews the applicant to verify the applicant's information and travel documents. CBP also uses the interview to address

any discrepancies identified between the application data submitted by the applicant and the data entered into the system by the MSP.

Acceptance of an applicant for enrollment in a trusted traveler program will be based (partially) upon the results of searches of the various law enforcement databases identified above. If there are doubts as to whether an individual applying for the trusted traveler program is the same individual of record in a law enforcement database, or if that law enforcement database record's accuracy is questionable, CBP will utilize the personal interview, the complete application data, and/or offer the applicant an opportunity to reapply and clarify the potential inaccuracy to determine the validity and relevancy of the data. This is very similar to how CBP Officers process travelers each day to determine admissibility when encountering potential matches during routine searches of law enforcement databases.

1.8 Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

GES will create previously unavailable data concerning an individual through the process of determining whether or not the individual is found to be 'low risk' and accepted into a trusted traveler program or is denied admission. The review of biographic application data in GES and biometric information in IDENT, and the comparison of this information with other law enforcement databases, permit a CBP Officer to determine the relative risk level of the applicant and record whether or not the applicant is admitted into the trusted traveler program. While the biometric information and corresponding identifying biographic information in IDENT will not contain this newly derived or created information, there will be cross-references to the biographic and derived or created information in GES. As new trusted traveler programs are developed and new travelers are added to GES through various enrollment processes, the information and determinations will be input directly into the GES system.

In the cases where applicants are found to be "high risk" and denied entry into or removed from a trusted traveler program, GES will keep a record of the application data and the status of the application's approval or denial. IDENT will also maintain the biometrics and limited biographic information, but there will be no designation indicating status (low risk or high risk) within a trusted traveler program. With the exception of border crossing information for active accounts, GES will contain pointers to the vast majority of information that it cross-references against data that is already documented in the law enforcement databases. For instance, a person could be denied participation in NEXUS due to a previous smuggling related incident that was documented in TECS. Upon application to NEXUS, GES would identify that information in TECS forms the basis for the reason for the applicant's denial from the NEXUS program. The actual derogatory information will remain in TECS with a pointer in GES to provide the location of the necessary background information which supports the negative determination on program admissibility contained in GES.

GES will also collect border-crossing information on each trusted traveler every time he/she transits the border. IDENT will save and store the fingerprints as well as record the date, time and

location every time a member's two index fingerprints are presented at the POE in the expedited processing lane.

1.9 Will the newly derived data be placed on the individual's record?

Newly derived data concerning whether or not an individual is a trusted traveler and that person's instances of transiting the border will be accessible directly when that individual's records are accessed. Separately in instances where information about an enrollee is discovered during vetting, the fact of the newly derived information about the enrollee's background, discovered during vetting, is returned from TECS. If a "hit" is made (where there is a match between the person queried and the record found in TECS), then the person's GES record will indicate that a "hit" was made and the location of the information appearing in TECS. The "hit" pointer will be stored in GES as part of the person's record. The actual hit information will remain in TECS. Access to both the indication of a "hit" in GES and to the actual information in TECS will be restricted to a select set of authorized users who are CBP Officers or Supervisors. Border transit records will be kept separately in GES as part of the member's record and may be made available to authorized GES users. Border crossing information is also stored in TECS.

1.10 Can CBP make new determinations, as a result of information supplied under the system, about an individual that otherwise would not be possible?

Yes. The new data can provide information demonstrating patterns of behavior in crossing the borders. Additionally, the TECS checks can provide information about the current criminal status of an individual. This is an essential feature of GES that will allow CBP to identify a traveler as "low-risk" to participate in a voluntary, trusted traveler program.

1.11 How will the newly derived data be verified for relevance and accuracy?

Mechanisms to check the accuracy of GES data are described in the answer to question 5 above. Enrollee information is provided to TECS for comparison at the time of vetting and if a CBP Officer finds a need to perform an enforcement check at the time of travel. However, GES does not have any mechanism to validate the accuracy of TECS data. The CBP Officer who receives the results of the comparison, determines the relevancy of the information provided and the appropriate course of action, based upon agency regulations and guidelines.

1.12 Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, the data elements are described in detail in the "DHS ES User Requirements and High-level Design Document V1.0 (Draft) December 2004."

Section 2 – Redress

2.1 What opportunities do individuals have to decline to provide information?

The trusted traveler programs are all voluntary. In order to participate in a trusted traveler program, specific information is required. The programs will accommodate persons who volunteer to participate, who go through the several steps of the enrollment process, and who are found to meet the program's qualifications as low risk travelers. Individuals may decline to provide information requested by a particular program application or enrollment process, and thus, decline to participate in said program. However, in order to be a member of any of the trusted traveler programs, each individual must provide the required information for enrollment.

2.2 What opportunities do individuals have to consent to particular uses of the information?

Application for the programs will constitute consent. GES and IDENT data distribution and usage are subject to Privacy Act considerations.

2.3 How do individuals grant consent concerning how their information will be used or shared?

Application for the trusted traveler programs will constitute consent for use and sharing of the information as outlined in the System of Records Notice. GES and IDENT data distribution and usage are subject to Privacy Act considerations. In addition, the application form contains a Privacy Act Statement regarding the authority of CBP to collect the requested information and identifying the uses to which the information will be put.

2.4 What are the procedures for individuals to gain access to their own information?

To gain access to government-held information, an enrollee may request information about their records contained in GES and IDENT through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a (d).

2.5 What are the procedures for correcting erroneous information?

Any participant who has reason to believe his/her GES information is incorrect should contact in writing CBP's Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W. (Room 5.5C), Washington, DC 20229, Fax: 202-344-2791. The letter to CBP's Customer Satisfaction Unit should explain which information is erroneous and set forth the correct information.

Section 3 – Access to the Data

3.1 Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others) and is it documented?

CBP Supervisors, CBP Officers involved in the program management, system administrators, employees and supervisors of the MSP (only with respect to the information submitted as part of the application process), and Canadian Officers involved in the operation and administration of the NEXUS program (only with respect to the information pertaining to the NEXUS program) will have access to the GES data on an official need-to-know basis (as with any information CBP utilizes).

Similarly, DHS employees authorized to have access to IDENT will also have access to the corresponding cross-referenced or pointed to data identified as residing in GES. In both the instance of access to data in IDENT and data in GES, access by employees of DHS will be on an official need-to-know basis.

3.2 How will access to the data by a user be determined?

Access to the information within CBP is determined by the role prescribed for a given individual. For all programs administered solely by CBP, including the low-risk enrollment system and the Small Boat Reporting Program, the CBP Supervisory level will identify individuals and their respective roles with regards to the information. For the NEXUS programs, which are jointly administered by CBP and the CBSA, the CBSA supervisory level will identify individuals and their respective roles within that agency. Access to the data outside of CBP will be restricted to 'need to know' in accordance with the routine uses of the GES SORN and IDENT SORN. The defined roles and their capabilities include:

Risk Assessor (CBP employee)

- Performs risk assessment
- Changes status
- Unable to override the Canadian risk assessment decision
- Generate reports

Risk Assessor Supervisor (CBP employee)

- Performs same functions as Risk Assessor
- Reviews denied applications
- Able to override Risk Assessor decisions
- Generates letters
- Unable to override the Canadian risk assessment decision
- Performs system administration

CBP Officer

- Interviews traveler at enrollment center
- Prints summary of application data
- Able to perform risk assessment

- Captures traveler's biometrics
- Scans traveler's documents
- Performs IDENT Search and Enroll (S&E)
- Changes status
- Unable to override the Canadian risk assessment decision
- Issues RFID
- Generates reports

Local System Control Officer (LSCO) (CBP employee)

- Performs same functions as Officer
- Reviews denied applications
- Reviews revoked participants
- Able to override Officer decisions
- Performs system administration

IDENT User (DHS employee)

- Generates reports on GES information within IDENT
- Performs IDENT S&E on forwarded GES information
- Performs risk assessment on forwarded GES information

Canadian Officer

- Interviews Nexus traveler at enrollment center
- Prints summary of application data from forms provided by traveler
- Captures traveler's biometrics
- Scans traveler's documents
- Changes status
- Issues RFID

Managed Service Provider (non-government)

- Transfers application information from submitted application to System data pertaining to individual
- Collects and records payment information

3.3 What controls are in place to prevent the misuse (e.g. browsing, expired privileges, etc.) of data by those having access?

Access to GES data is controlled through administrative passwords and restrictive rules regarding access to the CBP Intranet as well as the database itself. In addition, the users are limited to the roles defined for their use of the system.

Access to IDENT, and thus, GES data stored there, is controlled through administrative passwords and restrictive rules regarding access to the database. In addition, users are limited to the roles defined for their use of the system.

3.4 Do other systems share data or have access to data in this system? If yes, explain. Include a discussion of who will be responsible for protecting the privacy rights of individuals affected by the interface?

The ten fingerprints collected during the enrollment process are shared with the FBI for initial vetting. CBSA shares biographic and biometric data with CBP related to the NEXUS programs. CBSA receives the application data from all applicants and initially processes the information for enrollment consideration. Once approval is granted, CBSA forwards the data to CBP for enrollment consideration if found to be low-risk (CBP can still deny an applicant based upon U.S. information) and stored in GES. The data is provided to CBP, but not by means of a direct link between GES and any Canadian IT system. Otherwise, the information with GES and IDENT are not shared outside of the border crossing environment controlled by CBP.

3.5 Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

With the exception of the CBSA identified under User Roles in response to question 2 of section 3 above, and sharing of the ten fingerprints with the FBI for initial vetting, no other international, Federal, state, or local systems have access to GES. There may be instances where reports from GES are requested by one or more of these systems. Data sharing would be done on a case-by-case basis and would have to be supported by an MOU between CBP and the requesting Federal, state or local organization. In the case of an international request, DHS/CBP may participate in international negotiations or formalize an agreement giving access to GES under the information sharing process. The same would be true with respect to information in IDENT obtain from GES.

3.6 How will the data be used by these other agencies?

With regard to the possible sharing of the data on a case-by-case basis, the use of the data will be restricted by both the approved uses and the restrictions regarding confidentiality of information contained in either the letter authorizing exchange of the information or the respective MOU. GES and IDENT may also share information with other federal, state, local, tribal, and foreign law enforcement partners to accomplish common goals through data sharing agreements that address privacy and security concerns, as well as operational requirements.

3.7 Who is responsible for assuring proper use of the data by other agencies?

If and when a data sharing opportunity arises, all data usage will be controlled by an MOU with the requesting agency.

3.8 How will the system ensure that other agencies only get the information they are entitled to?

CBP personnel who have the appropriate role-based access to the data will compile the requested information. The compiled data will be screened by a CBP Supervisor to ensure that it contains only the data that the MOU stipulates may be shared with the requesting agency.

Section 4 – Maintenance of Administrative Controls

4.1 Are the data secured consistent with agency requirements under the Federal Information Security Management Act? Specifically:

The GES was subject to Certification and Accreditation by the Department of Justice, consistent with the development of GES under the former Immigration and Naturalization Service. At the time that GES was transferred to CBP this C&A covered the system. Presently, CBP is preparing GES for review under its own separate C&A to ensure its compliance with FISMA. Until this review is completed, GES relies upon its former Department of Justice C&A. The GES security plan is under development and a C&A will be scheduled after its completion.

4.1.a. Affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured;

Currently not applicable.

4.1.b. Acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls;

Currently not applicable.

4.1.c. Describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information, and

Currently not applicable.

4.1.d. Provide a point of contact for any additional questions from users.

Additional information is available from Sandra Scott, GES Program Manager, Office of Field Operations, Border Security and Facilitation, 1300 Pennsylvania Ave., NW, Room 5.3-14, Washington, DC 20229, (202) 344-2548.

4.2 If the system is operated in more that one site, how will consistent use of the system and data be maintained in all sites?

The system is only operated at the National Data Center (NDC). All access is directly linked to the database at the NDC.

4.3 What are the retention periods of data in the system?

CBP is working with the U.S. National Archives and Records Administration (NARA) to develop a retention schedule for these records that will be more closely aligned with program requirements. A similar review is also being undertaken by the U.S. VISIT program office in conjunction with NARA to determine the appropriate retention period for biometric information maintained in IDENT. The previous retention period for data contained in GES when that system resided in the former Immigration and Naturalization Service stated that: (a) all records would be destroyed three years after the dedicated commuter lane permit expires or three years after the denial of an application or removal of an individual from the program; and (b) litigation records will be destroyed three years after resolution or court decision.

4.4 What are the procedures for expunging the data at the end of the retention period and are these procedures documented?

Data is expunged in one of two ways: hard copy or physical data, such as application information and physical copies of submitted versions of the I-823, are destroyed by shredding within a reasonable time following verification of the MSP's entry efforts and the applicant interview (the reasonable time is subject to further clarification following completion of the record retention review by both CBP and NARA); electronic data is expunged through erasure of magnetic media in conformance with FIMSA standards—again, the timeframe for this destruction is dependent upon the aforementioned retention review.

4.5 Will the system provide the capability to monitor individuals or groups of individuals? If yes, explain.

Through the border crossing records collected on enrollees, the system will maintain information on the border crossing habits of an individual or group of individuals.

4.6 What controls are in place to prevent unauthorized monitoring of individuals or groups of individuals?

The controls consist of applying password and role-based access capabilities to pre-cleared personnel. In addition, CBP personnel are subject to periodic refresher training on system access rights and responsibilities. Lastly, CBP performs routine audits of access by CBP personnel to ensure compliance with internal CBP access procedures. CBP employees found to have engaged in unauthorized access to CBP systems are subject to disciplinary action that could result in criminal penalties and/or loss of job.

4.7 Under which Systems of Record Notice (SORN) does the system operate? Provide Number and Name.

GES was published as a System of Records by the former Immigration and Naturalization Service, U.S. Department of Justice (System Number: Justice/INS – 017, 62 FR 11919, March 13, 1997). As the successor to the immigration functions of the former INS, CBP now manages the GES SORN, which also covers the current SENTRI program. CBP is presently amending the GES SORN to reflect the transition of GES into the Department of Homeland Security and the enhanced capability described in this document. IDENT (Enforcement Operational Immigration Records [ENFORCE/IDENT]) was re-published as a System of Records by the Department of Homeland Security (System Number: DHS/ICE-CBP-CIS-03, 68 FR 69414, December 12, 2003) to address the collection of information supporting the U.S. VISIT program. Separately, the IDENT SORN is also being amended and republished to reflect changes described in this document.

Section 5 – Decision Analysis

5.1 Did you evaluate competing technologies on their privacy handling capabilities? If yes, explain.

Yes, CBP evaluated the relative merits of maintaining GES as a series of standalone systems resident at the respective ports of entry where the enrollees submitted their applications as compared to placing the system in a national database accessible from all ports of entry. From a system architecture perspective CBP found that privacy and security were enhanced by moving to a national database maintained at a secure facility as opposed to a local system maintained at a port and subject to varying security precautions. From a user access perspective CBP found that data in the national database was exposed to greater access by CBP authorized users, although CBP does not believe that this degrades privacy protection because of the training, auditing, and uniformity of procedures, including role-based access, employed to ensure limited, "need to know" access of information in national databases by CBP users. Separately, CBP determined that the benefit in utility derived for the enrollee from a national database would far outweigh the potential degradation in privacy resulting from greater possible user access.

5.2 Were any choice changes made to system architectures, hardware, software, or implementation plans as a result of doing a PIA? If yes, explain.

Yes, as part of the decision to migrate GES data from local standalone databases to a national system, CBP determined that it would be necessary to validate the local data before placing it in the national system. CBP performs a screening of the data similar to the checks performed on new enrollee data prior to loading the data obtained from local databases into the national database. This validation of the data permits all the data collected in the national system to be similarly reliable and subject to the same or related sources for verification.

In summation, the primary risks to privacy posed by the migration of GES to a national database are the accuracy of the data and the expanded CBP user access to any one individual's information.

These risks are principally mitigated through uniform enrollment procedures created under the national system and through the regular training and auditing to which all users of CBP national systems are subject. The uniform procedures for collecting the data ensure that the same type of information is collected from all individuals and that the manner of collection is consistent. With regard to training and auditing, CBP is able to control, centrally, access to its national systems, which allows for the implementation of uniform procedures in data handling.

For questions or comments, please contact:

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Office of Regulations and Rulings, CBP, (202) 572-8712.

Appendix 1

List of Existing Trusted Traveler Programs that will be incorporated into the new design for CBP's Global Enrollment System.

Currently, CBP has approximately 200,000 travelers registered and approved in the following voluntary programs:

- Free And Secure Trade (FAST) for low-risk, commercial cargo shipments at the Northern and Southwest land borders;
- Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) – for low-risk, international air passengers traveling through Los Angeles, Miami, Newark, New York, San Francisco, and Washington-Dulles airports, as well as the U.S. preclearance sites at the Vancouver and Toronto, Canada airports.
- NEXUS Highway – for low-risk drivers and passengers on the Northern border;
- NEXUS Air – for low-risk, U.S. and Canadian air passengers traveling between the two countries through Vancouver Int'l Airport;
- NEXUS Marine – for low-risk, international pleasure boaters in Detroit/Windsor area;
- Secure Electronic Network for Travelers Rapid Inspection (SENTRI) Highway – for low-risk drivers and passengers at the Southwest land border;
- SENTRI Pedestrian – for low-risk pedestrians at the San Ysidro land border crossing;
- Remote Port Entry Program (RPEP) – for low-risk, remote border crossers along the U.S.-Canada border; and
- Pre-enrolled Access Lane (PAL)- for low-risk drivers and passengers at Border Patrol checkpoints on the Southern border.

Appendix 2

- NEXUS Highway – Form I-823N/E 643E. E 643E is the Canadian form number for the application. Canadian forms are used when the program's application process requires the applicant to submit his or her application information directly to the Canadian Border Services Agency (CBSA), the Canadian agency that administers the particular trusted traveler program jointly with CBP.
- NEXUS Air – Canadian Form E 694E
- NEXUS Marine – Canadian Form E 695E
- SENTRI Highway – Form I-823S
- SENTRI Pedestrian – Form I-823S
- PAL – Form I-866
- RPEP – Form I-823S
- Low-risk enrollment system – Form CBP 823A has been approved by OMB for use when the pilot begins.