Privacy Impact Assessment
for the

Changes to Requirements Affecting H-2A Nonimmigrants and Changes to Requirements Affecting H-2B Nonimmigrants and Employers Final Rules

December 18, 2008

Contact Point
Donald Hawkins, Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security
(202) 272-8000

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

Abstract

United States Citizenship and Immigration Services (USCIS) is publishing this Privacy Impact Assessment (PIA) in conjunction with two Final Rules titled *Changes to Requirements Affecting H-2A Nonimmigrants* and *Changes to Requirements Affecting H-2B Nonimmigrants and Employers*. The Final Rules announce employers' requirements to notify USCIS when an H-2A or H-2B worker absconds, fails to report for work, or is terminated early and/or when any prohibited fees are collected from aliens as a condition of H-2A or H-2B employment. USCIS has conducted this PIA because the nonimmigrant visa programs associated with these Final Rules involve the collection of personally identifiable information (PII).

Overview

USCIS receives and adjudicates petitions and applications for various immigration benefits, including petitions filed by or on behalf of employers seeking to employ nonimmigrant workers on a temporary basis in the United States. The Final Rules titled *Changes to Requirements Affecting H-2A Nonimmigrants* and *Changes to Requirements Affecting H-2B Nonimmigrants and Employers* announce petitioners' requirements to notify USCIS when an H-2A or H-2B worker absconds, fails to report for work, or is terminated early and/or when any prohibited fees are collected from aliens as a condition of H-2A or H-2B employment. The DHS Privacy Office is publishing this PIA under the authority of Subsection 4 of Section 222 of the Homeland Security Act of 2002, as amended, which calls for the DHS Chief Privacy Officer to conduct a "privacy impact assessment of proposed rules of the Department."

The implementation of these new rules will not substantially change the privacy impacts of the H-2A and H-2B process of USCIS customers, as the changes are highly technical adjustments to the existing benefits process. USCIS conducted this PIA to cover the entire H2-A and H2-B nonimmigrant worker benefit process, including those changes brought about by the new Final Rules.

When U.S. employers face a shortage of available U.S. workers to fill temporary jobs in certain industries, they may petition USCIS for permission to employ foreign workers to perform that work in the United States. Such a petition must be accompanied by an approved temporary labor certification from the U.S. Department of Labor or the Governor of Guam for H-2B employment on Guam indicating that there are no U.S. workers able, willing, qualified, and available to perform the work. If such a petition is approved, eligible workers who are outside of the United States may then apply for a temporary work visa at an embassy or consulate abroad, which will facilitate their travel and admission to the United States.

The H-2A and H-2B Nonimmigrant Classifications

The H-2A program allows U.S. employers to bring foreign nationals to the United States to fill temporary agricultural jobs for which U.S. workers are not available. The H-2A nonimmigrant classification applies to aliens seeking to perform agricultural labor or services of a temporary or seasonal nature in the United States on a temporary basis. Employment of a seasonal nature is employment that is tied to a certain time of year by an event or pattern, such as a growing season, and requires labor levels far above those necessary for ongoing operations. Under the regulations being modified by the rule, employment is of a temporary nature if the employer's need for the worker will, except in extraordinary circumstances, last no longer than a year.

The H-2B nonagricultural temporary worker classification is available to aliens who are coming

temporarily to the United States to perform temporary services or labor in positions for which there is a shortage of available U.S. workers. Temporary services or labor under the H-2B classification refers to any job in which *the petitioner's need* for the duties to be performed by the worker is temporary, whether or not the underlying job can be described as permanent or temporary. The petitioner must show that its need is based one of the following: (1) one-time occurrence; (2) seasonal need; (3) peakload need, or (4) intermittent or occasional need. Persons granted H-2B status generally may not remain in the United States for longer than 3 consecutive years.

Process for obtaining H-2A or H-2B Status

Prospective employers of H-2A or H2-B workers must first obtain certification from the U.S. Department of Labor (DOL) or the Governor of Guam for H-2B employment on Guam that (1) there are not sufficient U.S. workers who are able, willing, qualified, and available to do the work; and (2) the employment of H-2A and/or H-2B aliens will not adversely affect the wages and working conditions of similarly employed U.S. workers.

Once the employer has obtained an approved temporary labor certification, the employer files a Form I-129, "Petition for a Nonimmigrant Worker," with USCIS to classify the individual as an H-2A or H-2B worker. If the petition is approved, the worker may apply for an H-2A/B visa at a U.S. embassy or consulate abroad. If the worker is already in the United States and in a valid nonimmigrant status, the petitioner may also request a change of nonimmigrant status to H-2A/H-2B or an extension of the worker's current H-2B nonimmigrant stay.

All persons arriving from abroad who are seeking H-2A/B nonimmigrant status must present themselves for inspection at a port-of-entry to DHS Customs and Border Protection, and if found admissible, will be admitted in H-2A/H-2B nonimmigrant status.

Relevant Information Technology

All H-2A and H-2B information is processed by USCIS's main case management database, Computer Linked Application Information System (CLAIMS 3) and associated systems.[1] The information in CLAIMS 3 is used for the adjudication and/or granting or denial of immigration benefits. Should an employer report a violation to USCIS as required in accordance with the H-2A and H-2B final rules, USCIS will post that violation in TECS[2] provided the identity of the alien is known (i.e., the alien is not an unnamed worker). Within TECS, CBP will run a name check which consists of a search of a database containing information from 26 different federal agencies. This check is performed on all aliens seeking admission at a port of entry. The information in TECS includes records of known and suspected terrorists, sex offenders, people who are public safety risks and other individuals who may be of interest (e.g., individuals who have wants and warrants issued against them, people involved in illegal gang activity etc.) to the law enforcement community.

[1] More information available in the PIA, USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) and the Benefits Information System system of records notice (SORN), DHS-USCIS-007, September 29, 2008 73 FR 56596, available at www.dhs.gov/privacy.

[2] More information available in the U.S. CBP System of Records Notice, DHS/CBP-011 TECS available at www.dhs.gov/privacy.

ICE also uses H-2 information within TECS for its investigations regarding immigration and customs violations.

Criteria for Exit Pilot Program with U.S. Customs and Border Protection

The rules also establishes criteria for a pilot program under which aliens admitted on certain temporary worker visas must present information upon departure from the country. This PIA does not cover that pilot program, which will require its own separate notice in the Federal Register and will require a dedicated PIA.

Authorities and Background

The authority to operate this program is found in the Immigration and Nationality Act (INA) sec. 101(a)(15)(H)(ii)(a), 8 U.S.C. 1101(a)(15)(H)(ii)(a); see 8 CFR 214.1(a)(2) (H-2A classification designation) and sec. 101(a)(15)(H)(ii)(b), 8 U.S.C. 1101(a)(15)(H)(ii)(b); see 8 CFR 214.1(a)(2) (H-2B classification designation).

For the purpose of this PIA, the following section discusses only H-2A and H-2B information located in CLAIMS 3. For a full discussion of information located in CLAIMS 3, please see the PIA for the USCIS *Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum* and the Benefits Information System SORN, DHS-USCIS-007, September 29, 2008 73 FR 56596.

Section 1.0 Characterization of the Information

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

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

The I-129 Form, "Petition for Non-Immigrant Worker", collects the following data elements:

Names: USCIS collects names (First, Last and Middle) for workers, aliases, H-2A and H-2B employer, and the name of the H-2A or H-2B facilitator, recruiter, or placement service to which alien beneficiaries paid or agreed to pay the prohibited fees[3] to identify the worker and verify the accuracy of

[3] The H-2A and H-2B Final Rules provide DHS with the authority to deny or revoke (following notice and an opportunity to respond) an H-2A or H-2B petition if DHS determines that the worker has collected, or entered into an agreement to collect a fee or compensation as a condition of obtaining the H-2A or H-2B employment, or that the employer knows or reasonably should know that the beneficiary has paid or agreed to pay any facilitator, recruiter, or similar employment service as a condition of obtaining the H-2A or H-2B employment. See 8 CFR 214.2(h)(5)(xi)(A) and 8 CFR 214.2(h)(6)(i)(B). However, DHS will not deny or revoke the petition if the employer notifies DHS about the payments within 2 work days of finding out such payments. The types of fees that would be prohibited include recruitment fees, attorneys' fees, and fees for preparation of visa applications. Prohibited fees do not include the lower of the fair market value or actual transportation costs to the US, or payment of any

information provided in a petition or application. The name of the workers is not always required. H-2A and H-2B petitions may include unnamed beneficiaries (workers) for those aliens who are outside the United States, regardless of the number of beneficiaries on the petition or whether the temporary labor certification named beneficiaries. Beneficiaries of an H-2A or H-2B petition who are in the United States (and who are applying for a change of nonimmigrant status to H-2A or H-2B or an extension of their H-2A or H-2B stay) must be named in the petition.

Addresses: USCIS collects H-2A and H-2B employer addresses, the foreign address of H-2A and H-2B workers, H-2A and H-2B employers' email addresses, and the address of the H-2A or H-2B facilitator or recruiter. USCIS uses the addresses to send information (e.g., denial, grant and/or requests for additional information) to the employer or other persons relevant to the immigration process regarding the application.

Telephone Numbers: USCIS collects H-2A/H-2B employers' telephone numbers to contact the worker or the H-2A or H-2B employer if there are questions regarding information contained in the completed forms.

Birth Dates: USCIS collects birth dates of the H-2A and H-2B worker to verify the identity of the worker and to determine his/her eligibility for benefits.

Federal Employer Identification Number (EIN) / Social Security Numbers (SSN): USCIS collects EIN or SSN of the H-2A or H-2B to further identify the employer as a U.S. employer.

Citizenship/Nationality Information: USCIS collects citizenship information (country of citizenship, province of birth, country of birth) of the H-2A or H-2B worker to determine a worker's eligibility for benefits.

Information Regarding NonImmigrant Status: USCIS collects information regarding nonimmigrant status: date of arrival, I-94 Number (Arrival/Departure Document), current non-immigrant status, A-number if applicable, date nonimmigrant status expires, passport number, date passport issued, date passport expires, and DOL Labor Certification Application number(s) of H-2A and H-2B workers to determine eligibility for benefits.

Employment Related Information: An H-2A or H-2B employer must provide employment-related notifications (hiring, termination, absconders, etc) to USCIS within 2 work days of an event as specified in Section 4.1 of this PIA.

Tax, Financial, and Payment Information: USCIS collects H-2A and H-2B employer tax identification numbers to ensure compliance with statutory and regulatory requirements. Under this Final Rule, subsequent collections related to non-immigrant workers would expand but only upon notification of potential violation or fee circumstances.

In addition, the employer must include the following information in a required event notification:

---

government-specified fees required of persons seeking to travel to the US, such as fees required by a foreign government for issuance for passports and by the DOS for issuance of visas.

- The reason for the notification;
- The reason for untimely notification and evidence for good cause demonstrated by the H-2A employer, if applicable;
- The USCIS receipt number of the approved H-2A or H-2B petition;
- The petitioner's name, address, telephone number, and EIN;
- The employer's name, address, and telephone number, if it is different from that of the petitioner;
- The name, date and place of birth of the H-2A or H-2B worker in question; and
- The last known physical address and telephone number of the H-2A or H-2B worker in question.
- Name and address of the facilitator, recruiter, or placement service to which alien beneficiaries paid or agreed to pay the prohibited fees.

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

Information related to H-2A and H-2B petitions is collected directly from employers who may collect information from the non-immigrant workers.

Internal Sources (Within DHS)

In instances where ICE/CBP discovers a nonimmigrant violation of an H-2A or H-2B Visa, that violation may be entered into TECS. The USCIS Service Center staff performs queries of TECS with regard to incoming applications and petitions. Therefore, should any subsequent petition be filed on behalf of the beneficiary, the prior violation could factor into the adjudication process.

TECS Name Check

The TECS Name Check consists of a search of a database containing information from 26 different federal agencies. The information in TECS includes records of known and suspected terrorists, sex offenders, people who are public safety risks and other individuals that may be of interest (e.g., individuals who have "wants" and warrants" issued against them, people involved in illegal gang activity etc.) to the law enforcement community. Information on H-2A and H-2B violating employers and H-2A/H-2B violating aliens is sent to TECS electronically. A USCIS user can also log into TECS directly and conduct an individual search.

External Sources (Outside DHS)

Department of State (DOS). USCIS receives information from the visa portion of the DOS Consular Consolidated Database (CCD) pursuant to a Memorandum of Understanding (MOU) executed in April 2006 and the subsequent 2008 amendment. The information obtained from CCD includes the history of visa applications and adjudications for subjects who apply for immigration and other benefits. USCIS uses this information to compare CCD visa records with an individual's pending USCIS application to verify the application to ensure consistency. USCIS's use of the information derived from this agreement is limited to the formulation, amendment, administration, and enforcement of immigration

and nationality laws. USCIS entered this agreement pursuant to its authority derived from 8 U.S.C. Section 1103. The MOU fully describes the rights and responsibilities of the parties with respect to the information shared, including appropriate safeguards that must be afforded any information disclosed pursuant to the MOU. The MOU also requires updates to ensure data accuracy and training for USCIS users who access the CCD.

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

USCIS collects this information in order to determine whether to approve H-2A and H-2B petitions for employers seeking temporary services of agricultural worker and nonagricultural workers. All information collected from employers seeking benefits via petitions that are processed by CLAIMS 3 is necessary to establish the employer's and worker's identity and history with USCIS, as well as eligibility for the benefit sought. In addition USCIS maintains the information to determine suitability for H-2A and H-2B visas, using criminal, immigration, or terrorism-related history.

1.4 How is the information collected?

USCIS collects the information directly from the H-2A or H-2B employer via completed immigration forms and notifications. USCIS employees and/or its contractors enter information from these forms manually into CLAIMS 3.

1.5 How will the information be checked for accuracy?

All CLAIMS 3 information is checked for accuracy through database technical controls, inherent business logic built into the system, and a manual review process. Improved processes are being put in place for periodic review of PII contained in the system to ensure it is timely, accurate, and relevant as required by the Office of Management and Budget (OMB) and the Privacy Act of 1974. A notification process is also being implemented so that when changes occur (i.e., revisions to PII or the CLAIMS 3 system encounters a major change or is replaced), other resources (e.g., other DHS systems and system users with which/whom information is shared) dependent upon PII contained in this system are alerted.

If upon later review of official correspondence, an employer determines that information submitted is incorrect or outdated (e.g., change of address), the employer may contact the USCIS and request correction. USCIS treats all requests for corrections as Privacy Act requests. Therefore, such a request triggers the Privacy Act review process to evaluate the accuracy of the information. The accuracy of the data entry can also be challenged during the appeals process if a petition is denied or during the interview process when required.

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

The primary legal authority supporting the collection of the information stored in CLAIMS 3 comes from 8 U.S.C. Section 1101 *et seq Immigration and Nationality*. More specifically, 8 U.S.C. Section 1103 charges the DHS Secretary with the duty of administering and enforcing all laws relating to the immigration and naturalization of aliens. The DHS Secretary has delegated these duties to the USCIS

Director pursuant to a departmental management directive. In addition, OMB has approved the content and format of every public form used by USCIS.

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

Risk: Increased scope of information collection in the event of failure to report, abscondment, or early termination.

Mitigation: The information collected as required under the Final Rules for which this is drafted is greater, but not significantly greater than is required by Form I-129. In a required event notification, the employer must include the additional information discussed in Section 1.1 The increased notification requirements center on the actions of individuals whose information is presumably already contained in an I-129 form. In this sense, minimal new PII is collected.

Risk: Addition of Sensitive Financial Data to the Collection

Mitigation: H-2A employers may be assessed fees for non-compliance with the Final Rules for which this is drafted. The Rules request that such payment be made by check to CBP for settlement of the fine. Financial data is sensitive PII in that it gives any individual who has access to the financial data direct access to an individual's financial account(s). This risk is mitigated by the fact that CBP, in the discharge of its Trade Facilitation mission, is accustomed to assessing and collecting duty payments and fines as part of its customs trade enforcement operations. Training, role-based, access security measures, a code of conduct, and a rigorous internal discipline system are in place at CBP to ensure that financial data, such as the payment of fees discussed here, are handled and destroyed appropriately by CBP Officers and employees.

Section 2.0 Uses of 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.

The information on Form I-129 is used to process H-2A and H-2B non-immigrant worker visas, specifically to determine suitability for such a visa, including criminal, immigration, or terrorism-related history.

Notification and fee information is used to update information on existing H-2A and H-2B workers in the United States, as well as assess fines on non-compliant employers, and investigate H-2A/H-2B workers who have violated the terms of their visas.

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

USCIS does not use CLAIMS 3 (and therefore H-2A or H-2B data) to perform complex analytical tasks resulting in, among other types of data matching, relational analysis, scoring, reporting, or pattern analysis. The system does not make available new or previously unavailable data from newly derived information. DHS has other systems, covered by separate PIAs available on www.dhs.gov/privacy, which may use CLAIMS 3 data to conduct analysis, such as the USCIS Fraud Detection and National Security (FDNS) system and the ICE Pattern Analysis and Information Collection (ICEPIC).

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

USCIS does not use commercially or publicly available data in CLAIMS 3.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Risk: Individuals who have legitimate access to PII could exceed their authority and use the data for unofficial purposes.

Mitigation: DHS Management Directive System (MD) Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, May 11, 2004, provides guidance for the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information in both paper and electronic records (including CLAIMS 3). Additionally, all DHS employees are required to take annual computer security training, which addresses this issue. DHS also maintains rules of behavior for employees who use DHS systems.

USCIS also employs Standard Operating Procedures (SOPs) at the service centers to ensure accurate data entry and proper handling and appropriate use of information. Disciplinary rules are in place to ensure appropriate use of CLAIMS 3 (and therefore H-2A and H-2B) information. USCIS also limits access to PII by employing role-based access (only allowing access to users who need particular PII to perform their duties). USCIS also deploys user logs to ensure users are only accessing information related to their job functions.

Section 3.0 Retention

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

3.1 How long is information retained?

For H-2A and H-2B I-129 forms, National Archives and Records Administration (NARA)

approved the following schedules: Form I-129 documents are sent to the Federal Records Center one year from last action date and are destroyed when six years old. Form I-129S documents are destroyed two years after file becomes inactive.

Generally, information located in CLAIMS 3 is maintained and disposed of in accordance with the criteria approved by the National Archives and Records Administration (NARA). Information in the master file is destroyed 15 years after the last completed action with respect to the application. System documentation (e.g., manuals) is destroyed when the system is superseded, obsolete, or no longer needed for agency business. Electronic records extracted from immigration benefits applications other than naturalization, asylum, or refugee status completed by applicants is destroyed after the data is transferred to the electronic master file and verified. Daily reports generated by associated information technology systems are maintained for 15 years by the service center that generated the reports and then destroyed.

Information collected and shared with component agencies and within the individual component systems, may vary, yet is done so in accordance with the retention schedules for each system.

3.2 Has the retention schedule been approved by the component records officer and NARA?

NARA approved the retention schedule for I-129 forms on March 20, 1996. NARA approved the retention schedule for CLAIMS 3 on March 25, 2007.

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

Risk: Keeping data in CLAIMS 3 longer than necessary would violate the Fair Information Practice that requires the retention of the minimum amount of information necessary to perform relevant governmental functions.

Mitigation: Although there is always risk inherent in retaining data for any length of time, Form I-129 and the CLAIMS 3 data retention periods identified in the NARA schedules are consistent with the concept of retaining data only for as long as necessary to support the agency's mission. The schedules proposed and approved by NARA comply with the requirements of the Federal Records Act and the stated purpose and mission of the systems. The time periods in the NARA schedules were carefully negotiated between USCIS and NARA to ensure that data is retained for the minimum time needed to process the application and make the information available for other USCIS benefits that might be sought by an applicant.

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 organization(s) is the information shared, what information is shared and for what purpose?

CLAIMS 3 exchanges data with several systems internal to DHS in order to process applications. For a full discussion of CLAIMS 3 sharing please see the PIA for the USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum. H-2A and H-2B information specifically is shared with the following organizations.

Sharing Within U.S. Citizenship and Immigration Services (USCIS)

USCIS Verification Information System (VIS). VIS is a nationally accessible internal USCIS database containing selected immigration status information. VIS verifies citizenship and immigration status of individuals seeking government benefits, and allows employers, utilizing a secure public interface, to determine whether a newly hired employee is authorized to work in the United States. VIS directly downloads USCIS CLAIMS 3 change of status and extension of status information on non-citizens and non-immigrants to help determine whether a non-citizen is eligible for any public benefit, license, or credential based on citizenship and immigration status.

Sharing With Other DHS Components

Customs and Border Protection (CBP):

TECS. USCIS administers the benefit processing of H-2A and H-2B petitions for temporary agricultural and temporary nonagricultural workers. A worker or employer may violate[4] the terms of the visa classification when an H-2A or H-2B worker fails to report to work within 5 work days of the employment start date; when the services for which H-2A and H-2B workers were hired is completed more than 30 days early; or when H-2A or H-2B workers abscond from the worksite or are terminated prior to the completion of services for which they were hired. Once the determination for violation is made by USCIS, appropriate TECS entries are made on the workers (if their identity is known) and, where applicable, on the employers. USCIS shares the TECS entry numbers for H-2A violators and/or violating employers discussed above with CBP for the purpose of collecting liquid payable debt payment from the employer for non-compliance with the H-2A reporting requirements.

In addition, CBP users at border crossings have read-only access to petition and application information in CLAIMS 3 via the Central Index System mainframe.

DHS, Immigration and Custom's Enforcement's (ICE): ICE users have read-only access to petition and application information found in CLAIMS 3 via the Central Index System mainframe. USCIS shares the TECS entry number discussed above for the purpose of investigating non-compliance

[4] The employer is found to violate the terms if he or she fails without good cause, as determined by USCIS, to notify USCIS within 2 days of the events listed below.

with H-2A/H-2B requirements.

DHS Intelligence and Analysis (I&A). DHS I & A analysts may access benefits application data for national security purposes.

4.2 How is the information transmitted or disclosed?

All internal sharing is conducted over a secure DHS electronic interface. This interface utilizes secure network connections on the DHS core network. Federal government employees and their agents must adhere to the OMB guidance provided in OMB Memoranda, M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006, and M-06-16 *Protection of Sensitive Agency Information*, dated June 23, 2006, setting forth the standards for the handling and safeguarding of PII. Contractors must also sign non-disclosure agreements that require them to follow departmental transmission and disclosure limitations. All data shared between agencies will be transmitted or disclosed via secured communications.

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

Risk: The main risk associated with internal information sharing is unauthorized access to PII in CLAIMS 3.

Mitigation: All users must authenticate using a user ID and password in order to access the system. Computer security concerns are minimized by the fact that the information shared internally remains within the DHS environment. Role-based access is used to limit the number of persons who access PII. User access logs track changes to information in the system.

Risk: There is a risk that with the sharing of complex sets of data end users from DHS components who do not have immigration analysis background and training may misinterpret the data.

Mitigation: USCIS is careful to share data with other DHS components that have a need to know, and put the information to a use that is compatible with USCIS System of Records Notices (SORNs). USCIS trains analysts examining immigration data to understand the data and have professional experience examining that type of data and trusts that other DHS components provide similar training to analysts with similar immigration experience.

DHS internal data sharing is necessary to comply with statutory requirements for national security and law enforcement. This data must always be kept secure, accurate, and appropriately controlled. Privacy risks are mitigated through relevant data sharing agreements that require physical, technical, and administrative controls. For information regarding risks and mitigations surrounding the sharing, disclosure, or transmission of PII collected in accordance with this project and retained in IDENT and ADIS, please refer to the published PIAs and SORNs for each system.

Section 5.0 External Sharing and Disclosure

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

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

CLAIMS 3 exchanges data with several systems outside of DHS in order to process applications, is discussed in detail in the USCIS *Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum* PIA.. For purposes of this PIA, a discussion of the external sharing of H-2A and H-2B information follows.

External Sharing (Outside DHS)

Department of State (DOS). CLAIMS 3 shares H-2A and H-2B information with the DOS.

An interface between the CLAIMS 3 Mainframe and the DOS NIV provides USCIS Benefits information (i.e. an approved Petition for a Non-Immigrant Worker [Form I-129,]) to the DOS DataShare system (DataShare is the name for the DOS Interagency Data Exchange Application [IDEA]). The Datashare system was developed in 1996 as part of a cooperative effort between the former INS, the former U.S. Customs Service, and a number of other interested federal agencies to share immigration benefits information electronically. The purpose of this initiative is to share information regarding persons arriving at our borders, to efficiently produce green cards, and to assist persons who have obtained a USCIS benefit if they have trouble at the border and require confirmation of their status.

CLAIMS 3 tracks aliens who apply to extend their stay in the U.S. As stated in the DOS-USCIS sharing arrangement, the CLAIMS Mainframe notifies DOS when any alien has a benefit pending, or has had a benefit approved, or denied. This interface provides information that is loaded into the CCD where it is accessible to the DOS systems issuing non-immigrant visas at overseas posts. When retrieved, this data permits consular officers to verify the validity of the I-129 (Petition for a Non-Immigrant Worker) presented to consular posts.

An MOU exists between USCIS and DOS that fully outlines the responsibilities of the parties, including security standards applicable to the information. USCIS provides DOS with electronic read-only access to CLAIMS 3 and 4.

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

The current SORN for CLAIMS 3 titled United States Citizenship and Immigration Services Benefits Information System SORN, hereafter Benefits Information Systems, was published in the Federal Register at 73 FR 56596, simultaneously with the publication of the USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum PIA. The routine uses, which identify how PII in CLAIMS 3 is shared externally are listed in the SORN. All sharing is compatible with the purpose for which the information was originally requested.

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

Information in CLAIMS 3 is tightly controlled and access is granted only to individuals (internally and externally) who have a specific need to access the system in order to perform their duties. Each transmission of data from CLAIMS 3 to an internal or external system is covered by an Interface Control Document (ICD) that describes the electronic system interface, the levels of authentication and access control that are needed, the data to be shared, and the format and syntax of the data passing through the interface. The ICD also describes the security controls that protect the interface.

None of these external entities has uncontrolled access to the CLAIMS 3 database and associated systems (e.g., external entities have read only access). Once the data is shared, however, the receiving agency is responsible for safeguarding and assuring proper use of the data within its organization. Each of these sharing arrangements is covered by an appropriate routine use in the Benefits Information Systems SORN.

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

Risk: The primary privacy issue in external sharing is the sharing of data for purposes that are not in accord with the stated purpose and use of the original collection.

Mitigation: All external CLAIMS 3 sharing arrangements are consistent with existing published routine uses (in the SORN for this system of records) or performed with the consent of the individual whose information is being shared. In all immigration forms processed in CLAIMS 3, applicants are advised that USCIS may provide information from their application to other government agencies. As required by DHS procedures and policies, all CLAIMS 3 routine uses and current external sharing arrangements are consistent with the original purpose for which the information was collected.

Information transferred to external agencies that is made part of a system of records is subject to the Privacy Act accuracy, timeliness, relevance, and completeness requirements at the receiving agency.

Risk: There is a risk that with the sharing of complex sets of data such as that in CLAIMS 3 and associated systems, end users from DHS components who do not have immigration analysis background and training may misinterpret the data.

Mitigation: USCIS is careful to share data with external agencies that have a need to know, and put the information to a use that is compatible with USCIS SORNs. USCIS trains analysts examining immigration data to understand the data and have professional experience examining that type of data and trusts that the external agencies provide similar training to analysts with similar immigration experience.

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?

Individuals who apply for USCIS benefits are presented with a Privacy Act Statement as required by Section (e)(3) of the Privacy Act and sign a release authorization on the benefit application/petition. The Privacy Act Statement details the authority to collect the information requested and uses to which USCIS will put information the applicant provides on immigration forms and in support of an application. The notice is located in the form instructions, which are available via a separate download on the same USCIS site that links to the form. The forms also contain a provision by which an applicant authorizes USCIS to release any information received from the applicant as needed to determine eligibility for benefits.

Individuals are provided general notice through the Benefits Information System SORN published in the Federal Register 73 FR 56596. Notice regarding the collection of biographic and biometric information from H-2A and H-2B visa holders is being provided through the issuance of this PIA.

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

Providing information on immigration forms is a voluntary act on the part of the employer filing on behalf of the alien. The employer, however, must submit a complete application in order to receive USCIS benefits. Employers may decline to provide the required information; however, it may result in the denial of the benefit. This condition is clearly stated on each USCIS form.

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

USCIS I-129 benefit application requires that applicants provide signatures in addition to other information requested in an application. This information is critical in making an informed adjudication decision to grant or deny a USCIS benefit. The failure to submit such information prohibits USCIS from processing and properly adjudicating the application/petition and thus precludes the applicant from receiving the benefit. Therefore, during the application process, individuals consent to the use of the information submitted for adjudication purposes. Specifically, all USCIS immigration forms include a Privacy Act Statement and require the applicant's signature authorizing "the release of any information from my records that USCIS needs to determine eligibility for the benefit." USCIS forms also contain a statement notifying applicants that their information may be shared with other federal agencies as well. This information is also conveyed in the SORN for this system and in the Privacy Act Statement on the application itself. Applicants are provided an opportunity to review how their information will be used and shared. Individuals grant consent to the collection and use of the information when they sign the

application.

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

Applicants for USCIS benefits are made aware that the information they are providing is being collected to determine whether they are eligible for immigration benefits. Each immigration form contains a provision by which an applicant authorizes USCIS to release any information from the application as needed to determine eligibility for benefits. Applicants are also advised that the information provided will be shared with other Federal, state, local and foreign law enforcement and regulatory agencies during the course of the investigation. The SORN provides additional notice to individuals by specifying the routine external uses to which the information will be put. In the USCIS website Privacy Notice,[5] individuals are also notified that electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act, NARA regulations and records schedules, and in some cases may be covered by the Privacy Act and subject to disclosure under the Freedom of Information Act (FOIA). OMB approved all Privacy Act Statements used when collecting data. See the response to Section 1.1 for a discussion of the manner in which USCIS uses H-2A and H-2B data.

Section 7.0 Access, Redress and Correction

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

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

USCIS treats all requests for amendment of information in a system of records as Privacy Act amendment requests. Any individual seeking to access H-2A and H-2B information maintained in CLAIMS 3 should direct his or her request to the USCIS FOIA / Privacy Act (PA) Officer at USCIS FOIA/PA, 70 Kimball Avenue, South Burlington, Vermont 05403-6813 (Human resources and procurement records) or USCIS National Records Center (NRC), P. O. Box 648010, Lee's Summit, MO 64064-8010 (all other USCIS records). The process for requesting records can be found at 6 Code of Federal Regulations, Section 5.21. Requests for records amendments may also be submitted to the service center where the application was originally submitted. The request should state clearly the information that is being contested, the reasons for contesting it, and the proposed amendment to the information. If USCIS intends to use information that is not contained in the application or supporting documentation (e.g., criminal history received from law enforcement), it will provide formal notice to the applicant and provide them an opportunity to refute the information prior to rendering a final decision regarding the application. This provides yet another mechanism for erroneous information to be corrected.

---

[5] Available at http://149.101.23.2/graphics/privnote.htm

Requests for access to records in this system must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Access Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity (full name, current address, and date and place of birth) in accordance with DHS regulations governing Privacy Act requests (found at 6 Code of Federal Regulations, Section 5.21), and any other identifying information that may be of assistance in locating the record.

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

Requests to contest or amend H-2A or H-2B information contained in CLAIMS 3 should be submitted as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, and the proposed amendment. The requestor should also clearly mark the envelope, "Privacy Act Amendment Request." The record must be identified in the same manner as described for making a request for access.

If the particular USCIS process requires a personal interview by a USCIS examiner in order to adjudicate a benefit application, the applicant also has the opportunity to make changes during the interview.

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

The Privacy Act SORN for this system provides individuals with guidance regarding the procedures for correcting information. This PIA also provides similar notice. Privacy Act Statements, including notice of an individual's right to correct information, are also contained in immigration forms published by USCIS.

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

Applicants are provided opportunity for redress as discussed above.

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

Risk: The main risk with respect to redress is that the right may be limited by Privacy Act exemptions or limited avenues for seeking redress.

Mitigation: The redress and access measures offered by USCIS are appropriate given the purpose of the system. Individuals are given numerous opportunities during and after the completion of the applications process to correct information they have provided and to respond to information received from other sources. USCIS does not claim any Privacy Act access and amendment exemptions for this system so individuals may avail themselves to redress and appeals as stated in the DHS Privacy Act

regulations (found at 6 Code of Federal Regulations, Section 5.21).

Section 8.0 Technical Access and Security

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

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

CLAIMS 3 is the IT system associated with these Final Rules, so any information used by these rules will follow CLAIMS 3 protocols. In compliance with federal law and regulations, users have access to CLAIMS 3 on a need to know basis. This need to know is determined by the individual's current job functions. Users may have read-only access to the information if they have a legitimate need to know as validated by their supervisor and the system owner and have successfully completed all personnel security training requirements. System administrators may have access if they are cleared and have legitimate job functions that would require them to view the information. Developers do not have access to production data except for specially cleared individuals who perform systems data maintenance and reporting tasks. Access privileges (for both internal and external users) are limited by establishing role-based user accounts to minimize access to information that is not needed to perform essential job functions.

Criteria, procedures, controls, and responsibilities regarding CLAIMS 3 access are contained in the Sensitive System Security plan for CLAIMS 3. Additionally, there are several department and government-wide regulations and directives that provide additional guidance and direction.

8.2 Will Department contractors have access to the system?

Contractors maintain the CLAIMS 3 Mainframe, LAN applications, and associated systems under the direction of the USCIS Office of Information Technology (OIT). Access is provided to contractors only as needed to perform their duties as required in the agreement between USCIS and the contractor and as limited by relevant SOPs. In addition, USCIS employees and contractors who have completed a G-872A & B form (see Section 8.4) and granted appropriate access levels by a supervisor are assigned a login and password to access the system. These users must undergo federally approved clearance investigations and sign appropriate documentation in order to obtain the appropriate access levels.

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

USCIS provides training to all CLAIMS 3 users. This training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements, etc.). Each USCIS site has the responsibility to ensure that all federal employees and contractors receive the required annual computer security awareness training and Privacy Act training.

All DHS personnel, including government personnel and contractors, are required to take mandatory computer security awareness and privacy training conducted by their DHS component.

8.4 Has Certification & Accreditation (C&A) been completed for the system or systems supporting the program?

In July of 2008, the CLAIMS 3 LAN obtained a three year Authority to Operate (ATO) from the USCIS Chief Information Officer (CIO) after completing DHS C&A requirements. The USCIS Office of Chief Information Officer (OCIO) granted the ATO upon due consideration of the findings and recommendations contained in the independent Security Evaluation Report and the recommendations of the USCIS Information System Security Officer (ISSO).

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

When privileges expire, user access is promptly terminated. After termination of employment at USCIS, access privileges are removed as part of the employee exit clearance process (signed by various persons before departure). Many users have legitimate job duties that require them to query the database for record sets meeting certain criteria. This work is performed under supervisory oversight. Each employee is given annual security awareness training that addresses their duties and responsibilities to protect the data. CLAIMS 3 also records History Action Codes that provide a record of significant case processing actions including the user ID of the individual performing these actions. Browsing by the general user community is not permitted. In order to reduce the possibility of misuse and inappropriate dissemination of information, DHS security specifications require auditing capabilities that log user activity. All user actions are tracked via audit logs.

The PII received by DHS is subject to appropriate technical safeguards and audit capabilities of the systems in which the PII is stored. All systems must comply with the requirements of DHS information technology security policy, specifically the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attach A to DHS Management Directive 4300.1).

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

Risk: Given the scope of the personal information collected in CLAIMS 3, the security of the information on the system is of critical importance. Due to the sensitive nature of this information, there are inherent security risks (e.g., unauthorized access, use and transmission/sharing) that require mitigation.

Mitigation: Access and security controls have been established to identify and mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Role-based user accounts are used to minimize the number of persons who have access to the system. Audit trails are kept in order to track and identify any unauthorized changes to information in the system. CLAIMS 3 has a comprehensive audit trail tracking and maintenance function that stores information on who submits each query, when the query was run, what the response was, who received the response, and when the response was received. Data encryption is employed where appropriate to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Further, CLAIMS 3 complies with DHS and FISMA/NIST security requirements, which

provide criteria for securing networks, computers, and computer services against attack and unauthorized information dissemination. Each time CLAIMS 3 is modified the security engineers review the proposed changes and if required, perform Security Testing and Evaluation (ST&E) to confirm that the controls work properly. All personnel are required to complete annual online computer security training.

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 What type of project is the program or system?

This program is part of the rulemaking process. The rulemaking process in this instance affects a USCIS information technology system, CLAIMS 3.

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

This rulemaking is in the Final Rule state of the rulemaking process. CLAIMS 3 is at the operations and maintenance phase of the DHS system development life cycle.

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

CLAIMS 3 only contains information related to the application and adjudication of benefits. The system does not have the technology or the ability to monitor the activities of individuals or groups beyond that required to adjudicate applications and petitions.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security