Privacy Impact Assessment
for the

Scheduling and Notification of Applicants for Processing

December 15, 2008

Contact Point
Donald Hawkins
USCIS Privacy Officer
United States Citizenship and Immigration Services
202-272-8404

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

Abstract

The Department of Homeland Security (DHS) United States Citizenship and Immigration Services (USCIS) has developed the Scheduling and Notification of Applicants for Processing (SNAP) system. SNAP automatically schedules appointments for immigration benefits for applicants/petitioners (hereafter collectively referred to as "applicants") to submit biometric information to USCIS. USCIS is conducting this Privacy Impact Assessment (PIA) because SNAP uses personally identifiable information (PII) to perform its scheduling functions.

Introduction

The USCIS Office of Field Operations (OFO) owns and operates the SNAP system. USCIS OFO oversees and manages the day-to-day operations of the 26 USCIS districts, encompassing 89 local offices and 129 Application Support Centers[1] (ASC) located throughout the continental United States, Alaska, Hawaii, Puerto Rico, Guam and the United States Virgin Islands. The National Benefits Center (NBC) in Missouri, USCIS's hub for completing pre-interview application processing, is also an OFO component.

Individuals seeking immigration benefits submit an application or petition (hereinafter referred to collectively as *application*) for that benefit, plus required fee payments and supporting documentation, to USCIS in hard copy format to the address listed on the application form. If the application is for an immigration benefit other than naturalization, asylum, or refugee status, USCIS enters the application information into the Computer Linked Application Information Management System (CLAIMS 3).[2] CLAIMS 3 is the main case management application used by USCIS to track and process the adjudication of applications for those immigration benefits.

USCIS requires that an applicant undergoes a "background check[3]" in connection with most of the applications for immigration benefits. In order to conduct this background check, applicants must submit their fingerprint/biometric information[4] and biographic information [name, address, date of birth, alien number (A-number) and/or social security number (SSN), country of birth, height, weight, eye color, and hair color] to USCIS by arrival for their appointment at an ASC.

---

[1] ASC: Application Support Center. 131 locations across the United States where applicants have fingerprints and biometric images captured.
NBC: National Benefits Center. Located in Lee's Summit, Missouri. Sends scheduling requests to SNAP for ASC appointments.

SC: Service Center. The four service centers (in Vermont, Texas, Nebraska and California) also send scheduling requests to SNAP for ASC appointments.

[2] See the Privacy Impact Assessment for *USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum* located at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf.

[3] See "Fact Sheet: USCIS Immigration Security Check" - www.uscis.gov.

[4] For purposes of this PIA, "fingerprints" refers to images of all ten fingers sent to the FBI for a criminal history check. "Biometrics" in this context refers to three images (photo, press print and signature) used during Employment Authorization Document (EAD) or Lawful Permanent Resident (LPR) card production.

SNAP is the automated system that schedules appointments for applicants to submit this information at the ASCs. Service Center or NBC personnel run an automated process in CLAIMS 3 that exports the data needed for scheduling from CLAIMS 3 to a batch file. This information is then encrypted and e-mailed as an attachment from the Service Center or NBC to the USCIS SNAP support team, who insert the data into SNAP. Using that information, SNAP automatically schedules applicants' appointments with the appropriate ASC based on each applicant's zip code[5] and the ASC's appointment capacity. The data that is exported from CLAIMS 3 to SNAP includes the applicants' names, A-numbers or SSNs, receipt numbers, dates of birth, form types, mailing addresses, and attorney's names and addresses, if applicable.

USCIS personnel screen scheduling requests to prevent unnecessary ASC appointments, thereby eliminating the default scheduling of applicants who have an existing appointment or have previously provided fingerprints/biometrics. SNAP's internal logic flags unnecessary appointments and prevents duplicate scheduling unless overridden by a SNAP user.

SNAP draws data on existing fingerprints and biometrics contained in the Benefits Biometrics Support System (BBSS). Once the appointment is scheduled, SNAP generates a notice that includes the ASC location, the date and time that the applicant should arrive, and any additional instructions pertinent to that application. USCIS mails the notice to the applicant and the applicant's attorney, if applicable. BBSS records data on which applicants appeared at ASCs; SNAP records data on which applicants were scheduled to appear. SNAP can compare appointment data to BBSS's data on who appeared to determine which applicants did not appear for their appointments, and reschedule them accordingly.

USCIS personnel at the ASCs consults the appointment data in SNAP by logging into a web-based user interface available within the DHS intranet to see appointments scheduled for their facilities.

USCIS personnel can also use SNAP to generate the following reports which in part assists USCIS in determining the workload at different ASCs :

- Bulk Applicant Check by Receipt Number - lists the scheduling status (scheduled, queued, not scheduled) for each receipt number, as well as whether fingerprints have already been taken and whether biometrics images have already been captured for the receipt numbers specified. The report combines scheduling information in SNAP originating in CLAIMS 3 with BBSS data.
- Families Too Large to Auto Schedule - shows groups with too many individuals to be automatically scheduled using SNAP. The families are grouped by common last name and mailing address. Data is originally drawn from CLAIMS 3.
- Customized Report - permits a user to query SNAP based on specific criteria chosen by the user. The data returned includes biographical data originating in CLAIMS 3 and fingerprint and biometrics data drawn from BBSS.
- Missed Appointments Report - Scheduling information in SNAP originating in CLAIMS 3 is compared to BBSS data to determine which applicants in SNAP have not appeared for their appointments.
- View ASC Capacity – provides statistical data relating to numbers of applicants on an ASC-by-ASC basis, a calculation drawn only from SNAP scheduling data, without any PII drawn from CLAIMS 3 or BBSS.

[5] USCIS attempts to schedule appointments at the nearest ASC based on the applicant's zip code.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

The personal information collected and stored in SNAP includes data provided at the time the Service Center/ NBC schedules the appointment.

Names: SNAP maintains full names (first and last) of applicants and their attorneys/representatives to identify the applicant and verify the accuracy of information provided in an application.

Addresses: SNAP maintains applicants' and attorneys' addresses to send information to the applicant regarding the application.

Birth Dates: SNAP maintains birth dates to verify the identity of the applicant.

Social Security Numbers (SSN): SNAP maintains applicants' SSNs where available, in conjunction with other information to verify the identity of the applicant, to determine the applicant's eligibility for certain benefits, and to track applicants through the scheduling process.

Scheduling data: SNAP assigns the appointment date and maintains the date the application is received, date fingerprinted, fingerprint result (N for Non-Ident [no hit], I for Ident [hit], or U for Unclassifiable [low quality fingerprint images which the Federal Bureau of Investigation (FBI) could not properly evaluate]), appointment status, and user ID. In addition, USCIS collects the ASC code, which indicates the scheduled ASC's name, street address, city, state, and zip code. USCIS also collects the "reason" code which indicates whether the applicant's scheduling notice includes references to previously expired or unclassifiable fingerprints. The SC code indicates which Service Center will print an applicant's notice. The Transmission Control Request (TCR) identifies for billing purposes a fingerprint transaction the FBI was unable to classify.

Personal Characteristics: SNAP maintains information regarding the applicant's personal characteristics (hair color, eye color, height, gender, weight, and race) to identify the applicant.

Citizenship/Nationality Information: SNAP maintains the applicants' citizenship information (country of nationality, country of citizenship, country of birth) to identify the applicant and determine his or her eligibility for certain benefits.

Information Regarding Immigration: SNAP maintains applicants' A-Numbers and Receipt Numbers to ensure that the correct record is associated with the correct applicant.

SNAP produces the following reports for ASC-related data:

- Bulk Applicant Check by Receipt Number - lists the scheduling status (scheduled, queued, not scheduled) for each receipt number, as well as whether fingerprints have already been taken and whether biometrics images have already been captured for the receipt numbers specified;
- Configurable Report - an *ad hoc* output report that permits a user to query SNAP based on specific criteria;

- Missed Appointments Report - lists those applicants that have not appeared for their appointment;
- Families Too Large to Auto schedule - shows groups with too many individuals to be handled by the auto scheduler functionality; and
- View ASC Capacity - provides the numbers of applicants who have filed applications at each ASC.

1.2 From whom is information collected?

SNAP does not collect data relating to the scheduling of fingerprint and/or biometric appointments directly from the applicant; rather, SNAP uses one of two methods to collect the information. In the first method, Service Center or NBC personnel initiate an automated process in CLAIMS 3 that exports the data needed for scheduling from CLAIMS 3 to a batch file. This information is then encrypted and emailed as an attachment from the Service Center or NBC to the USCIS SNAP support team, who upload it into SNAP. The Service Centers use CLAIMS 3 data as the source for the selection of applicants to be scheduled. Under the second method, a USCIS adjudicator, in the course of case review, determines that fingerprints and/or biometric images have not been provided, as required from an applicant in support of their benefit application. The adjudicator will then manually set up the appointment in SNAP or will request that the data-entry staff enter the appointment request.

1.3 Why is the information being collected?

USCIS collects fingerprint biometric information to verify an applicant's identity and to conduct fingerprint-based background checks. The collection of biographic information is necessary in part so that the Appointment Notice can be mailed directly to the applicant or the applicant's attorney.

The SNAP information (biographic and scheduling) collected is used for identity verification and correlation throughout the adjudication process. Without collection of the scheduling/biographic information (which constitutes PII), an applicant could not complete the fingerprints/biometrics application process needed to complete the adjudication process. The USCIS CLAIMS 3 uses either an A-number or the SSN to track the FBI response to criminal background checks. The A-number is used whenever possible while the SSN is only used if an applicant does not have an A-number. Fingerprints captured with neither an A-number nor SSN are of no practical value to USCIS because the USCIS adjudicators cannot view the FBI's response without accessing this response by A-number or SSN. Consequently, SNAP allows applicants to be scheduled using their SSNs.

1.4 How is the information collected?

Information for applicants requiring appointments for fingerprints/biometrics at an ASC is obtained electronically by Service Center staff from CLAIMS 3. This information includes scheduling data and associated biographic information. This information is then encrypted and e-mailed as an attachment from the Service Center or NBC to the USCIS SNAP support team, who load, or manually enter, the data into SNAP.

In addition, SNAP obtains information on applicants who have previously been fingerprinted directly from the BBSS database. SNAP also uses BBSS data to determine which applicants appeared for appointments.

Appointment Notices generated by SNAP are mailed directly to applicants or their attorney/representative.

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

The legal authority to collect this information comes from 8 U.S.C. § 1101 *et seq.* (Aliens and Nationality).

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

Privacy Risk: There is a risk that this system may collect more information than is necessary to perform the system's necessary functions, thus violating the Privacy Act's data minimization requirements.

Mitigation: USCIS limits the information collected in SNAP to that necessary to automatically schedule appointments for immigration benefits applicants so they can submit required biometric information to USCIS. This set of information is the minimum necessary to schedule the appointment. The majority of the data is taken from CLAIMS 3. In order to minimize the data stored in CLAIMS 3, and SNAP, USCIS limits the PII stored to information collected from applicants in USCIS forms. All information requested in USCIS forms is necessary to process requests for benefits. All data elements collected were negotiated with and approved by OMB during Paperwork Reduction Act collection reviews. USCIS also disposes of SNAP information promptly as required by the records retention schedule negotiated with the National Archives and Records Administration (NARA).

Privacy Risk: There is a risk that inaccurate data may be inserted into SNAP from other systems.

Mitigation: Generally, SNAP relies on the accuracy of data uploaded from CLAIMS 3 and BBSS. Both CLAIMS 3 and BBSS rely on information collected directly from the applicant. If, however, the appointment notice contains incorrect information (e.g., because of a transcription error or incorrect information provided by the applicant), the applicant may correct information by contacting USCIS or when appearing for the appointment.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

USCIS uses the SNAP scheduling information to manage fingerprints/biometrics appointments that result in the performance of background checks through FBI Integrated Automated Fingerprint Identification System (IAFIS), United States-Visitor and Immigrant Status Indicator Technology (US-VISIT),

and DHS Automated Biometric Identification System (IDENT). Associated biographic information collected at the time of fingerprint/biometric capture is used to aid in positively identifying the correct individual's records. After the fingerprint/biometric data is collected, CLAIMS 3 uses either an A-number or the SSN to track the FBI response to criminal background checks The A-number is used whenever possible while the SSN is used only if an applicant does not have an A-number. Fingerprints captured with neither an A-number nor SSN are of no practical value to USCIS because USCIS adjudicators can only retrieve pertinent data utilizing an A-number or SSN. For this reason, SNAP allows applicants to be scheduled using their SSNs in addition to their A-number.

USCIS sends the appointment notices containing SSNs or A-numbers produced by SNAP to the applicants and/or their attorneys.

USCIS adjudicators reprint SNAP notices when a case is denied for abandonment and place the notice in the applicant's A-File. Immigration judges in some cases ask for a SNAP notice to be reprinted and presented to the court.

USCIS Service Center operations management uses the scheduling data stored in SNAP to create reports that provide an accurate profile of the scheduling capacities and capabilities that are available to USCIS OFO program management. With this uniformly presented information, USCIS is able to actively and effectively manage these processes, identify issues before they become problems, and strategically plan and implement new measures to support USCIS' broader mission.

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

SNAP data will not be used for data mining. USCIS personnel use SNAP to generate reports that identify previously unknown administrative areas of concern, such as whether a particular ASC is booked for appointments over capacity, or whether a particular applicant has previously been scheduled for an appointment. These functions are designed to help USCIS more efficiently schedule applicants' appointments, and do not analyze data about the applicants themselves beyond basic scheduling. SNAP users may pull data from BBSS to report the number of "no shows" or abandonment cases.

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

Service Center or NBC personnel run an automatic process in CLAIMS 3 that exports the data needed for scheduling from CLAIMS 3 to a batch file. This process eliminates transcription error. Data is checked by a series of automated tests that are executed for consistency that verify the proper formatting of data fields prior to uploading the data. As discussed in Section 1.2, in the case where data-entry at the Service Center is performed per the request of an adjudicator, the Service Center staff uses visual verification to check the data for accuracy and proper formatting at the time of data-entry.

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

Privacy Risk: The collection of information presents inherent privacy risks including the possible misuse and inappropriate dissemination of data, including loss of control of data and data breaches.

Mitigation: This system was created to improve the accuracy and efficiency of scheduling appointments for applicants in order to facilitate the proper and timely submission of their biometric information for background checks. The system centralizes scheduling information into one system that is available in all USCIS field locations. This centralized approach to scheduling permits greater control over the security and management of PII. This centralization also allows more accurate and efficient audit log monitoring to ensure that data is not misused or inappropriately disseminated.

USCIS ensures that the scheduling and biographic information match the relevant applicant file by verifying that the ASC schedule of applicants matches the appointment notice and photographic identification that the applicant is required to bring to their appointment. As noted above, the majority of the data in SNAP originates from CLAIMS 3; therefore, SNAP relies on the integrity of the information imported from CLAIMS 3. USCIS conducts integrity checks at all points of data processing to ensure that USCIS has accurately matched the appropriate records and properly formatted the records before being stored. The Service Centers conduct the integrity checks by verifying each field in SNAP. USCIS may manually correct identified errors. Further, all information will reside on secured networks and servers with access limited to authorized personnel only. SNAP's import logic prevents duplicate scheduling of batches or duplicate records within batches. Lastly, USCIS maintains audit logs in order to track and identify unauthorized use of system information. Information, including the user's name, date, and time of every transaction, will be stored in a log. If USCIS suspects misuse of data, these logs can be used to review and analyze all activity in SNAP. Reporting from employee and/or system monitoring could identify the misuse of data. All SNAP users are notified that SNAP stores these logs and USCIS management can use them to review all activity in SNAP.

Section 3.0
Retention

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

SNAP stores data for no longer than 15 months from the last recorded action.

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

USCIS has proposed the following retention schedule: USCIS will delete or destroy inputs after the data has been transferred to the master file and verified. USCIS will delete or destroy the Master File 15 months from the last recorded action in SNAP. Outputs and system documentation are destroyed or deleted when no longer needed for agency business.

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

This information is needed for the indicated time because the relationship between an applicant requesting a particular benefit and USCIS may span the maximum of 15 months after the last recorded action in SNAP. For example, USCIS reprints SNAP notices when denying a case for abandonment, and places the SNAP notice in the applicant's A-File.

The SNAP data retention periods identified in the NARA schedule 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

4.1 With which internal organizations is the information shared?

USCIS personnel at the ASCs reference the appointment data in SNAP to see appointments scheduled for their facilities by logging into a web-based user interface available within the DHS intranet.

Information collected and stored in SNAP is not shared internally with other components in DHS.

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

There is no internal sharing of SNAP information between USCIS OFO and other internal DHS components. Therefore, this section is not applicable.

4.3 How is the information transmitted or disclosed?

There is no internal sharing of SNAP information between USCIS OFO and other internal DHS components. Therefore, this section is not applicable.

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

There is no internal sharing of SNAP information between USCIS OFO and other internal DHS components. Therefore, this section is not applicable.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

USCIS reprints SNAP notices when denying a case for abandonment, and places the SNAP notice in the applicant's A-File. Often the contents of an applicant's A-file, including a SNAP notice, will be requested by a Department of Justice immigration judge that is presiding over an alien's immigration proceeding. In those instances, a hard copy of the notice may be provided to the immigration court.

5.2 What information is shared and for what purpose?

The SNAP notice may be shared with an immigration judge for use in abandonment cases.

5.3 How is the information transmitted or disclosed?

The SNAP notice is transmitted in hard copy to the immigration judge.

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

An MOU is not in place with any immigration court or judge in order for a court of competent jurisdiction to receive a copy of a SNAP notice at issue in an immigration proceeding. As a court of competent jurisdiction, it is within its authority to request, for review, such a document from USCIS.

5.5 How is the shared information secured by the recipient?

Judges and clerks of courts must, at a minimum, obey legal ethical standards pertinent to their respective jurisdictions relating to the use, storage and maintenance of court documents, i.e., copies of SNAP notices.

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

USCIS does not require immigration judges be trained in handling the information contained in the SNAP notice. However, all government personnel and contractors must adhere to the OMB guidance provided in OMB Memoranda, M-06-16 "Protection of Sensitive Agency Information," dated June 23, 2006, setting forth the standards for the handling and safeguarding of personally identifying information.

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

Privacy 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, including unauthorized forward on disclosure and/or the loss of control of the data.

Mitigation: The external SNAP sharing arrangements with immigration judges are consistent with existing routine uses or performed with the consent of the individual whose information is being shared. These routine uses limit the sharing of information from the system to the stated purpose of the original collection. As required by DHS procedures and policies, all SNAP routine uses are consistent with the original purpose for which the information was collected. These routine uses and public notices of SNAP information use are reflected in limitations placed on external sharing arrangements.

Regarding unauthorized forward on disclosure and/or loss of control of the date, USCIS recognizes that all immigration judges are subject to federal information handling guidelines and ethics codes.

Section 6.0
Notice

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

SNAP does not collect information directly from individuals. The information is uploaded from CLAIMS 3 and BBSS. Applicants are provided notice prior receiving the appointment notice. Individuals who apply for USCIS benefits are presented with a Privacy Act Statement as required by Section (e)(3)[6] 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 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 also provided general notice through the Benefits Information System (BIS) SORN

[6] The USCIS Privacy Policy can be found at http://www.uscis.gov and on the instructions that accompany each form.

(73 FR 56596).

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

Applicants who are scheduled for USCIS benefits appointments have an opportunity and/or right to decline to provide information. If, however, applicants decline to provide required information, they will not be able to complete their request for benefits, thus resulting in the denial of their benefit application.

USCIS benefit applications require that certain biographic information be provided and require scheduling appointments for the submission of fingerprints and biometrics. 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 and thus precludes the applicant from receiving the benefit. Therefore, through the scheduling process and the application process, individuals have consented to the use of the information (including background investigations) submitted for adjudication purposes.

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

Individual benefits applicants have the right, but no current need to consent to particular uses of the SNAP information. SNAP only uses the information to schedule required appointments. The information is not shared internally. For the external sharing with immigration judges, a routine use was published to support such sharing, and individual consent would be sought for all sharing in addition to the uses described in the SORN.

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

The collection of PII is required as part of the scheduling process that must occur prior to the granting of an immigration benefit. 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. In addition, 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 USCIS Benefits Information System SORN (which covers the information in SNAP) provides additional notice to individuals by specifying the routine external uses of the CLAIMS 3 and CLAIMS 4 systems.

In the USCIS website Privacy Notice,[7] individuals are also notified that electronically submitted information is maintained and destroyed according to Federal Records Act requirements, NARA

[7] Available at http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=da3489eef3d4b010VgnVCM10000045f3d6a1RCRD&vgnextchannel=da3489eef3d4b010VgnVCM10000045f3d6a1RCRD

regulations, NARA records schedules, and, in some cases, 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.

Section 7.0
Individual Access, Redress and Correction

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

Any individual seeking to access information maintained in SNAP 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).

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 erroneous information?

All data in SNAP is obtained from previously entered data in CLAIMS 3. Prior to the mailing of an applicant's appointment notice, Service Center staff can manually edit, update, and then reprint the scheduling notice. When an applicant appears at an ASC, they have an opportunity to correct any information in their benefits application.

In addition, the process for requests to contest or amend information can be found at 6 Code of Federal Regulations, Section 5.21. Requests for records amendments may also be submitted to the USCIS 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. The requestor should also clearly mark the envelope, "Privacy Act Amendment Request." 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.

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

SNAP scheduling notices invite applicants to call the USCIS Customer Service Center if they have any questions. The Customer Service Center can inform applicants how to correct their information in USCIS systems. In addition, all benefits applicants are notified verbally at the ASCs for SNAP that they have the opportunity to correct their information.

The Benefits Information System SORN 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 redress is provided, are alternatives are available?

Normal USCIS procedure for redress is provided to applicants as outlined in Sections 7.1 and 7.2.

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

SNAP is not the original collector of personal data. CLAIMS 3 and BBSS provide SNAP with all data it uses to conduct scheduling. Accordingly, any information requests or requests for alteration of records should be made to CLAIMS 3 and BBSS, not SNAP. In some instances, the United States Postal Service will return a notice that the applicant moved. In that case, the information is changed in SNAP and a new appointment card is sent with the new address. Previously established procedures for changing biographical information may be followed to correct known erroneous information, for example requesting a manual correction to change an applicant's address and have a new benefit card or document produced. If the applicant suspects erroneous information but does not know which part of the information is incorrect, the applicant can file a FOIA/PA request as detailed in section 7.1.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Access will be limited to authorized USCIS employees and contractors. SNAP will offer the following three levels of access: Query, Data-Entry, and Administrator, which are all detailed in Section 8.3. System access will be commensurate with job function. SNAP does not offer public access.

8.2 Will contractors to DHS have access to the system?

Contractors who maintain systems and provide technical support and contractors working at the ASCs will have access to the system. All contractors are required to pass a background check before receiving access to a DHS building or system. All information technology (IT) based contracts must have Privacy Act compliance language presented before being awarded according to DHS contracting guidelines based on the Federal Acquisition Regulation and other Executive Orders, public law and national policy. All access to the SNAP system follows the logical access controls set up for access to USCIS computer systems. Access controls are applied to contractors and to federal employees equally.

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

USCIS uses role-based access to assign SNAP user privileges. There are three application user classes for SNAP:

- Class 1 – Query – Users requiring read only access to all data stored in the system, and can reprint an applicant's scheduling notice;
- Class 2 – Data-Entry – Users requiring access to view, enter, and modify scheduling and/or biographic data, and can schedule and reschedule applicants; and
- Class 3 – Administrator – Users requiring all standard functions, can override default settings, and can create new user accounts, reset passwords, and change users' roles.

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

For each USCIS location, the user must request and receive approval to access SNAP from the USCIS OFO specific site management (Service Center Director, District Office (DO) Director, and/or ASC Manager). USCIS OFO program management maintains documentation on all assignments of roles at the Service Centers, DOs, and ASCs.

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

All user actions tracked via audit logs. Reports can be run to verify that a user's activity is consistent with his job duties and access level. Many users have legitimate job functions that require them to query the database for record sets meeting certain criteria. This work is performed under supervisory oversight.

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).

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

In order to reduce the possibility of misuse and inappropriate dissemination of information, DHS security specifications require auditing capabilities that track and log all user activity. As discussed in Section 8.5, SNAP audit logs 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.

SNAP's audit trail capabilities are also used to examine an originally submitted scheduling appointment request along with the associated biographic information. These audit trails ensure that the scheduling appointment data is not duplicated. Batches are checked to prevent the import of duplicate batches or duplicate records within batches. All SNAP transactions are subject to monitoring and review to ensure that the original requests or results data are not lost, manipulated, or compromised in any manner.

Additionally, the USCIS offices using SNAP are required to follow USCIS application intake SOPs. Corresponding audits ensure that local processes and procedures are consistent across the enterprise. Within SNAP, there are many business rules that ensure data integrity and consistency.

Lastly, data will be transmitted within USCIS via secured DHS networks to ensure that data has not been tampered with and to prevent unauthorized personnel from viewing the data. Remote access to SNAP is allowed only through an encrypted virtual private network (VPN), access to which is controlled by numerical authentication tokens.

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

Training on the SNAP system is provided to Service Center, DO, and ASC users. This training addresses appropriate privacy concerns as well as methodology for the proper safeguarding of PII. These users have previously undergone federally approved clearance investigations and signed appropriate documentation in order to obtain the appropriate access levels. In addition, every Federal employee and contractor is required to complete computer security awareness training annually.

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

The USCIS OFO and the contractor have completed the Certification and Accreditation process with the appropriate USCIS Office of Information Technology security staff. The system has an Authority to Operate (ATO) to maintain its current operational status that was completed July 18, 2007.

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

Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Authorized users will be broken into specific classes with specific access rights. Audit trails will be kept in order to track and identify any unauthorized use of system information. The audit logs are reviewed periodically to ensure compliance. Data encryption will be employed at every appropriate step to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. As stated above, the batch information is emailed as an encrypted attachment from the Service Center or National Benefits Center to the USCIS SNAP support team Further, SNAP complies with DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack, and unauthorized information dissemination.

USCIS developed and implemented SNAP in accordance with DHS approved information security guidelines. Only users who need the information to perform their job functions have access to SNAP. All authorized users must go through an approval process and can only access SNAP using DHS approved equipment (i.e., DHS Intranet).

The SNAP system is operated within the DHS network. Users must authenticate to SNAP using a unique user ID and password. All SNAP users only have rights to work on those records that are specific to their respective ASC site. Personnel are screened prior to allowing access to the SNAP system.

USCIS screens users prior to giving them access to system information or resources. This screening is consistent with the types of information and resources that the individual needs to have access to perform his/her function. DHS policy requires: (1) Components shall ensure the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels, (2) No government employee shall be granted access to DHS systems without having a favorably adjudicated Minimum Background Investigation (MBI) as defined in DHS MD 11050.2, Personnel Security Program, (3) No contractor personnel shall be granted access to DHS systems without having a favorably adjudicated background Investigation as defined in DHS MD, Suitability Screening Requirements for Contractor Employees, (4) Only government and contractor personnel who are U.S. citizens shall be granted access to DHS systems processing sensitive information. An exception to the U.S. citizenship requirement may be granted by the Component Head or designee with the concurrence of the Office of Security and the DHS CIO or their designees.

USCIS OFO screens USCIS ASC, SC, DO, and NCSC employees and contractors prior to granting access to SNAP with each individual in accordance with DHS security policies.

In accordance with DHS MD, Suitability Screening Requirements for Contractor Employees, contractors are not granted access to SNAP until the contractor has a favorable adjudicated background investigation.

Lastly, all authorized users of SNAP go through the approval process (GA-872). All USCIS users must complete the Computer Security Awareness Training (CSAT) and the Privacy 101 training. Adjudicators at the USCIS Service Centers who use SNAP during the adjudication process have received the Federal Law Enforcement Training Center (FLETC) Freedom of Information Act/Privacy Act (FOIA/PA) BASIC training authored by the FLETC Legal Division.

Section 9.0 Technology

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

The system was designed with both commercial off-the-shelf products and custom designed software, databases, and user interfaces.

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

SNAP developers followed the System Development Life Cycle 6.0 security guidelines in the design and development of SNAP. The USCIS Office of Information Technology (OIT) Security has reviewed and approved all SNAP security documentation. Scheduling requests and biographic records will be attributed to the correct applicant by verifying the applicant's appointment notice at the time of appointment at the ASCs. SNAP data integrity checks were designed based on a detailed analysis of data sources (see Section 1.2) and specific data elements coming into SNAP. In addition to these integrity controls, the system was designed to acknowledge successful and failed data deliveries to ensure that data is never lost in transit. Furthermore, for interaction with CLAIMS 3, all requests will contain a correlation identifier that will be used to match the results with the proper request.

9.3 What design choices were made to enhance privacy?

SNAP will be available to USCIS employees and USCIS contractors with appropriate security and access controls who need to access the data as part of their official duties at USCIS. The general public will not have access to the system. Protection and integrity of data, security and privacy are of paramount concern. The system follows all DHS Security guidelines for enhanced security, including the Certification and Accreditation security documents, Federal Information Processing Standards (FIPS) 199, Federal Information Security Management Act (FISMA), Trusted Agent-Federal Information Security Management Act (TA-FISMA), Office of Management and Budget (OMB) memoranda, and the National Institute of Standards and Technology (NIST) security guidelines.

The system provides continued efficient management of USCIS scheduling of fingerprint-based and biometrics background check processes by supporting a centralized system to hold USCIS OFO scheduling data and associated biographic data. The ability to track data and user activities though audit logs on a consolidated system is far easier and provides better accountability than tracking information across multiple systems.

Conclusion

SNAP facilitates the USCIS scheduling process for the applicant to submit fingerprint and biometrics to USCIS for required background check processes by providing a centralized electronic storage and scheduling application. SNAP produces scheduling appointment notices along with associated biographic information. The applicant data used during scheduling for fingerprint and biometrics appointments is transmitted directly from data capture at a Service Center to an ASC.

SNAP addresses privacy concerns in many ways, including the following:

- Consolidating multiple data storage locations to one centralized repository that will be easier to secure, manage, and monitor;
- Granting access to pre-approved and cleared USCIS employees and contractors;
- Auditing transaction records to ensure that requested information and result data are not manipulated or compromised;
- Providing SNAP users with training that addresses privacy concerns; and
- Publishing a PIA that states USCIS' intentions for the use of the private information data collected from USCIS applicants.

SNAP is a growing and expanding project that is currently in production. As future enhancements and components are developed, this PIA and associated SORN will be revised to address those updates as necessary.

Responsible Officials

Donald Hawkins, USCIS, Privacy Officer

Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix

Privacy Policy

Thank you for visiting our Website and reviewing our privacy notice. We remind you that if you link to a site outside of the Department of Homeland Security, you are subject to the policies of the new site.

Privacy

Here is how we handle information about your visit to our Website:

Information Collected and Stored Automatically

If you visit our site to read or download information, we collect and store the following information about your visit:

The name of the Internet domain (for example, "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you are connecting from a university's domain) and the IP address (a number that is automatically assigned to your computer when you are using the Internet) from which you access our site;
The type of browser and operating system used to access our site;
The date and time you access our site;
The Internet address of the Website from which you linked directly to our site; and
The pages you visit and the information you request.

This information is primarily collected for statistical analysis and technical improvements to the site. This government computer system uses software programs to create summary statistics, which may be used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas. In certain circumstances, however, we may take addtional steps to identify you based on this information and we may share this information, including your identity, with other agencies.

If You Send Us Personal Information

If you choose to provide us with personal information, such as by sending an e-mail or by filling out a form and submitting it through our Website, we will use that information to respond to your message or to fulfill the stated purpose of the communication. Remember that e-mail is not necessarily secure against interception. If you communication is sensitive or includes personal information you may prefer to send it by postal mail instead.

We may share the information you give us with another government agency if your inquiry relates to that agency. In other limited circumstances, such as responses to requests from Congress and private individuals, we may be required by law to disclose information you submit. Before you submit personal information, such as on an online form, you may be given more specific guidance as to how your personal information may be used. Electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act and the regulations and records schedules of the National Archives and Records Administration, and in some cases may be covered by the Privacy Act and subject to the Freedom of Information Act.

Cookies

"Cookies" are small bits of text that are either used for the duration of a session ("session cookies"), or saved on a user's hard drive in order to identify that user, or information about that user, the next time the user logs on to a Website ("persistent cookies"). This Website does not use persistent cookies, but does use session cookies to provide streamlined navigation throughout the site. These session cookies are deleted from the server soon after your session ends and are not collected or saved.