Privacy Impact Assessment
for the

National Appointment Scheduling System

DHS/USCIS/PIA-057

July 28, 2015

<u>Contact Point</u>
Donald K. Hawkins
Office of Privacy
United States Citizenship and Immigration Services
(202) 272-8000

<u>Reviewing Official</u>
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) developed the National Appointment Scheduling System (NASS) to schedule appointments for biometric collections at Application Support Centers (ASC) or Service Centers. NASS replaces the existing operational Scheduling and Notification of Applicants for Processing (SNAP) system. USCIS is conducting this Privacy Impact Assessment (PIA) because NASS uses personally identifiable information (PII) to perform its scheduling functions. All SNAP functionalities and capabilities will be replaced by NASS and the existing SNAP PIA will be retired upon publication of this PIA.

Overview

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States. Individuals seeking immigration benefits submit an application or petition (application) for that benefit, plus the required fee payments and supporting documentation listed on the application form. USCIS then enters the application information into one of its main case management systems to track and process the adjudication of applications for those immigration benefits.

USCIS requires applicants and petitioners for certain immigration benefits to submit their biometric and biographic information to USCIS for a criminal background check. To collect biometrics, USCIS schedules individuals to be fingerprinted at an Application Support Center (ASC) after an application or petition is filed. USCIS uses NASS to schedule applicants for fingerprinting at one of the 161 ASC locations throughout the United States.

NASS centralizes all USCIS biometric appointment scheduling.[1] NASS provides automatic biometric appointment scheduling for applications that are processed by: Computer-Linked Application Information Management System (CLAIMS) 3,[2] CLAIMS 4,[3] USCIS Electronic Immigration System (ELIS),[4] and the Refugee Asylum and Parole System (RAPS).[5] Concurrent with scheduling biometric appointments, NASS also triggers the Notice Generation System (NGS) to create appointment notices for applicants. NASS sends notice data including

[1] USCIS previously used the Scheduling and Notification of Applicants for Processing (SNAP) system for all biometric processing appointments. *See* DHS/USCIS/PIA-020 - Scheduling and Notification of Applicants for Processing (SNAP) (December 15, 2008), *available at* www.dhs.gov/privacy.

[2] *See* DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) (September 5, 2008), *available at* www.dhs.gov/privacy.

[3] *See* DHS/USCIS/PIA-015 Computer Linked Application Information Management System (CLAIMS 4) Update (November 5, 2013), *available at* www.dhs.gov/privacy.

[4] *See* DHS-USCIS-PIA-056 USCIS ELIS: Form I-90 (November 13, 2014), *available at* www.dhs.gov/privacy.

[5] *See* DHS/USCIS/PIA-027(b) Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS) Update (June 5, 2013), *available at* www.dhs.gov/privacy.

the appointment date, time, and place; notice transaction identifier; applicant information; and respresentative information to NGS to generate the notice. NGS then creates the appointment notices and sends them to the Enterprise Print Management System (EPMS) to be printed and then sent to the applicant and representative, if applicable.[6]

Appointment Creation

NASS generates biometric processing appointments automatically and manually. NASS automatically generates appointments on a weekly basis, or USCIS personnel may manually expedite the process by requesting an appointment for certain applicants or petitioners directly in NASS.

Automatic Appointments

NASS performs weekly automatic batch scheduling of all applications requiring biometric appointments from CLAIMS 3, CLAIMS 4, RAPS, and ELIS. When NASS schedules an appointment, the applicant's address information (in CLAIMS 3, CLAIMS 4, RAPS, and ELIS) is mapped to an open appointment in NASS by geographic location based on applicant zip code and available by operator search. There can only be one schedule status for each applicant. If NASS is unable to schedule an appointment, the applicant data is stored in NASS with a status of "not scheduled." For example, if NASS cannot automatically schedule the applicant due to lack of capacity, NASS automatically queues the applicant for scheduling to occur once an appointment is available. NASS schedules appointments on a weekly basis.

USCIS personnel also have the ability to manually change an automatically scheduled appointment, if necessary. For example, if an applicant comes into an ASC and needs to reschedule his or her appointment to another date and time, ASC personnel with the proper permissions can manually change the appointment to an available time and date that better suits the applicant.

Manual Appointments

In the course of case review, a USCIS adjudicator may determine to require a biometric collection from an applicant in support of his or her benefit application.[7] To schedule these appointments, USCIS personnel at ASCs and Service Centers import the applicant's name, Alien Number (A-Number) or Social Security number (SSN), receipt number, date of birth, mailing

[6] NASS is only responsible for scheduling appointments. NGS and EPMS are legacy systems that were specifically developed for notice generation and printing purposes. NGS only generates notices and EPMS (subsystem to CLAIMS 3) prints the notices at the Eastern Forms Center and mails these notices directly to the individials. EPMS supports the printing of notices, cards, and booklets for USCIS.

[7] The process for manual appointment creation is complicated.since there are many policies that go around with benefit adjudication process. Some examples of why the adjudicator requests biometrics: (1) This is a new case and requires biometric information; (2) The applicant missed an appointment and request that they come in again; (3) The prints come back from FBI as unclassifiable and need to rescan again; or (4) The fingerprints have expired (after 15 months) and must be retaken.

address, and attorney name and address (if applicable) into NASS. Once the USCIS adjudicator manually requests an appointment, NASS uses that information to automatically schedule the applicant's appointment with the appropriate ASC based on each applicant's zip code and the ASC's appointment capacity. However, only USCIS employees with the Administrator or Power User role can manually schedule and cancel appointments.

After NASS schedules the appointment, NASS sends the appointment date, time, and ASC or Service Center location to the respective case management system (CLAIMS 3, CLAIMS 4, RAPS, or ELIS) either through bulk processing or a direct interface. NASS also sends the information to NGS to generate a biometric appointment notice that includes the applicant information, respresentiative information, ASC location, the date and time that the applicant should arrive, and any additional instructions pertinent to that application. Limited applicant information (i.e., name, address, A-Number, and form type) is printed directly on the appointment notice. The appointment notice also includes a two dimensional (2-D) barcode that includes the following applicant information (visible only when scanned by USCIS personnel):name, address, receipt number, SSN, date of birth, country of citizenship, height, hair color, eye color, race, weight, and A-Number, if available. If an an accredited representative/attorney is listed, a separate appointment letter is sent to the resprentative on file and includes the representative name, firm name, and address and applicant's name. The appointment notices are sent to EPMS to be printed and then sent to the applicant and representative, if applicable. NASS maintains a copy of all notices for the purpose of reprinting.

Appointment Management

Customers are instructed to bring the NGS-generated appointment notice to their appointment. Currently, the only method to manage appointments is via spreadsheet. The customer presents his or her printed appointment notice and a photo identification document at the Service Center or ASC. The Service Center or ASC compares the information included in the notice and spreadsheet to ensure the information matches. The spreadsheets are used for making the transition from legacy SNAP to NASS seamless. Future releases will transition from the use of Excel spreadsheets to a web interface.

Reporting

NASS interfaces with the Standard Management Analysis & Reporting Tool (SMART) to generate a number of statistical reports for productivity in order to conduct workload analysis to properly allocate resources.[8] SMART users query and view PII to generate customizable reports to monitor employee workload and productivity against NASS. These reports may be generated on a broad spectrum to measure productivity trends and average processing time. The information from NASS is transmitted to SMART to create and compile reports. NASS data is

[8] *See* DHS/USCIS/PIA-050 Standard Management Analysis Reporting Tool (SMART), *available at* www.dhs.gov/privacy.

not permanently stored in SMART.

Future Enhancements

NASS is a growing and expanding project. This system is limitied to biometric collections. Future releases will include additional processing, including oath ceremonies, interviews, and field appointments. As future enhancements and functionality are developed, USCIS will update this PIA to address these expansions. In addition, the DHS Privacy Office will initiate a Privacy Compliance Review on the ASC process, including NASS, within a year of publishing this PIA.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The authority to collect information is found within the Immigration and Nationality Act (INA).[9]

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The information collected and used by NASS to create appointments is covered by the Asylum Information and Pre-Screening,[10] Benefit Information System,[11] and Electronic Immigration System-2 Account and Case Management SORNs.[12] The biometric data collected at the scheduled appointment is stored in the Customer Profile Management Service (CPMS) and is covered by the Background Check Service[13] and Biometric Storage System[14] SORNs.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

USCIS is working with NARA to develop a records retention schedule to cover the

[9] 8 U.S.C. §§ 1101, 1103, 1201, and 1255.

[10] *See* DHS/USCIS-010 Asylum Information and Pre-Screening, 75 FR 409 (Jan. 5, 2010).

[11] *See* DHS/USCIS-007 Benefits Information System, 73 FR 56596 (Sept. 29, 2008).

[12] *See* DHS/USCIS-015 Electronic Immigration System-2 Account and Case Management System of Records, 78 FR 20673 (Apr. 5, 2013).

[13] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).

[14] DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (Apr. 6, 2007).

appointment scheduling records. USCIS plans to propose a 99 year retention period because the relationship between an applicant and USCIS may span the applicant's entire life.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information maintained by the case management systems from which NASS retrieves information may be subject to the PRA and is described in their respective PIAs.

Section 2.0 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.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

NASS collects applicant information from USCIS case management systems to schedule a biometric appointment and to pass information to CPMS for applicant vetting. The information in NASS may include:

- Name (first and last);
- Addresses;
- Birth Dates;
- Immigration Information (A-Number, SSN, and Receipt Number);
- Citizenship/Nationality Information (country of citizenship and country of birth);
- Scheduling Data (appointment date, time, and ASC/Service Center code, which indicates the scheduled office's name, street address, city, state, zip code, and Federal Bureau of Investigation Transaction Control Number (TCN)). NASS also maintains the date the application was received, appointment status, and appointment confirmation notice with appointment details; and
- Personal Characteristics (hair color, eye color, height, gender, weight, race, and ethnicity from the respective USCIS case management system).

2.2 What are the sources of the information and how is the information collected for the project?

NASS does not collect information directly from individuals. NASS offers two methods to schedule biometric appointments. In the first method, USCIS personnel may initiate an automated process in the case management system that exports the data needed for scheduling to a batch file. The data is exported from applications requiring biometric appointments stored in CLAIMS 3, CLAIMS 4, RAPS, and ELIS. In the second method, a USCIS adjudicator, in the course of case review, may determine the biometric collection is required from an applicant in support of his or her benefit application. The adjudicator then manually sets up the appointment request in NASS. This process to manually set up an appointment requires power user permissions within NASS.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

NASS vets uploaded applicant requests through a series of quality assurance checks. NASS connects to the CPMS ASC Encounter Data Query Service to determine if USCIS has existing photos or fingerprints on file.[15] The CPMS Encounter Query Service maintains and tracks details about Application Support Center visit history. The queries performed on the applicant data include a receipt check, biometric check, and fingerprint background check.[16] CPMS returns a message to NASS indicating if biometric data is on file for the applicant and whether the existing biometric data may be reused for the applicant. This allows NASS to schedule appointments only when USCIS needs to collect biometric data for the applicant.

NASS creates, updates, and archives biometric appointment schedule data. Service Centers submit appointment requests via a spreadsheet to NASS. NASS 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 storage. NASS validates the fields in the uploaded spreadsheet through a set of quality checks and submits any errors back to the Service Center. The Service Center then views field validation errors online and fixes all errors. All manually created biometric appointments are checked for accuracy through a manual review process and technical controls. The data fields in the input screen are configured to limit the possibility of entering incomplete data (e.g., the system rejects 00/00/00 birthdates). Data entry

[15] CPMS serves as the centralized repository of biometrics captured by USCIS used for biometric based background checks. *See* the forthcoming PIA for CPMS for more information, *available at* www.dhs.gov/privacy.

[16] The CPMS Encounter Query Serivce allow users to see details about Application Support Center visit history. The receipt check determines if the schedule request has already been processed and if biometrics are already in CPMS. The biometric check determines if biometrics exist in CPMS for the applicant and whether they have been collected within 5 years. If the biometrics are recent enough, a follow-up request is sent to CPMS to "clone" the existing biometrics to the new receipt number. The fingerprint background date check determines if a fingerprint background check was already performed on an applicant, and returns the Federal Bureau of Investigation Transaction Control Number (TCN) and date of that prior transaction to NASS.

personnel are provided with the opportunity to review and edit information prior to and after its submission. USCIS personnel may also manually correct identified errors.

CPMS vetting is a batch job that runs every five minutes. The batch job is triggered and scheduled internally from NASS. The batch job processes the applicant data by automatically sending information to CPMS to undergo the CPMS vetting process. Any new appointment requests received since the previous run of CPMS vetting are picked-up and sent to CPMS to determine if biometrics may be reused. NASS contains logic that calculates capacity to schedule appointments for applicants to appear at an ASC. The applicant data accuracy is ensured by the CPMS Vetting process.[17]

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information stored in NASS is inaccurate because NASS relies on connections from other USCIS case management systems, many of which rely on manual data entry, or USCIS employees manually enter information into NASS.

Mitigation: This risk is partially mitigated. First, all manually created biometric appointments are checked for accuracy through a manual review process and technical controls. Second, the data fields in the input screen are configured to limit the entry of incomplete data (e.g., the system rejects 00/00/00 birthdates). Third, data entry personnel are provided with the opportunity to review and edit information prior to and after their submission. USCIS personnel may also manually correct identified errors.

NASS also vets all applicant data via the CPMS Vetting process. CPMS Vetting is a batch job that runs every 5 minutes. Any new appointment requests received since the previous run of CPMS Vetting are picked-up and sent to CPMS to determine if biometrics may be reused.

Privacy Risk: There is a risk that NASS collects more information than is necessary to schedule a biometrics appointment.

Mitigation: This risk is partially mitigated. Although NASS only receives a subset of information from the case management system, more information is sent to NASS than is needed to schedule a biometrics appointment. NASS requires some of that information to verify the applicant's identity when he or she arrives at the ASC or to ensure CPMS is searching for the

[17] *See* forthcoming CPMS PIA. The CPMS vetting process includes three separate checks including a receipt check, biometric check, and fingerprint background date check. The receipt check determines if the schedule request has already been processed and if biometrics are already in CPMS. The biometric check determines if biometrics exist in CPMS for the applicant and whether they have been collected within 5 years. If the biometrics are recent enough, a follow-up request is sent to CPMS to "clone" the existing biometrics to the new receipt number. The fingerprint background date check determines if a fingerprint background check was already performed on an applicant, and returns the TCN and date of that prior transaction to NASS. If the date of the prior background check is older than the configured setting (12 months is currenty the default), a follow-up request is sent to CPMS to resubmit the TCN to the FBI to refresh the background check.

correct applicant in its database. However, instead of passing the necessary information to CPMS and deleting it, NASS maintains the individual's country of birth and country of citizenship, which are only used by CPMS.

Privacy Risk: There is a risk of data duplication to complete the biometrics scheduling process.

Mitigation: This risk is not mitigated. NASS collects limited information from the benefits application from CLAIMS 3, CLAIMS 4, RAPS, and ELIS. NASS then sends notice data including the appointment date, time, and place, notice transaction identifier, applicant information, and respresentative information to NGS to generate the notice. NGS then creates the appointment notices and sends them to the EPMS to be printed and then sent to the applicant and representative, if applicable.[18] In addition to these three different systems, NASS does not have the capability to produce daily tracking reports, which are currently run on spreadsheets daily.

Privacy Risk: There is a risk that more information than is necessary to alert applicants to their scheduled appointment is sent to EPMS and included on the printed notice.

Mitigation: Limited applicant contact information is printed directly on the appointment notice. Other identitying information (such as SSN, A-Number, ethnicity, race, eye color, hair color, weight, etc) is included in a 2D barcode on the appointment notice. A 2-D barcode is a stores the information within the symbol. The barcode is only machine-readable and a Livescan scanner is used to read the information in the barcode and autopopulate into Livescan, which is used to capture biometric and biographical information from applicants at the ASC and Internationally.

Upon arrival at a ASC, a customer checks in for an appointment and presents the printed appointment notice and a photo ID. These data elements are compared against the ID card to verify identity of the individual when he or she comes into the ASC.   The same information is transmitted to the LiveScan and along with the prints are forward to FBI for verification.   FBI conduct background checks to determine if the individual has any criminal activity. This technology greatly enhances USCIS' ability to quickly and accurately intake biometric appointments at the USCIS ASC facilities for fingerprint processing.

[18] NASS is only responsible for scheduling appointments. NGS and EPMS are legacy systems that were specifically developed for notice generation and printing purposes. NGS only generates notices and EPMS prints the notices at the Eastern Forms Center and mails these notices directly to the individials.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

NASS collects applicant information from USCIS case management systems to schedule a biometric appointment and to pass information to CPMS for applicant vetting. The information in NASS may include:

Names: NASS maintains the full name (first and last) of the applicant and his or her attorney or representative to identify the applicant and verify the accuracy of information provided in an application.

Addresses: NASS collects applicant and attorney addresses to identify the closest USCIS ASC and send information to the applicant and his or her attorney regarding the biometric appointment.

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

Immigration Information: NASS maintains the applicant's A-Number, SSN, and Receipt Number to ensure that the correct record is associated with the correct applicant.

Citizenship/Nationality Information: NASS maintains country of citizenship and country of birth. The FBI requires this information to perform its background checks on the applicant. NASS provides this information to CPMS for applicant vetting.

Scheduling Data: NASS assigns the appointment date, time, and ASC/Service Center code, which indicates the scheduled office's name, street address, city, state, zip code, and Federal Bureau of Investigation TCN. NASS also maintains the date the application was received, appointment status, and appointment confirmation notice with appointment details.

Personal Characteristics: NASS recieves applicant data on hair color, eye color, height, gender, weight, race, and ethnicity from the respective USCIS case management system. The physical descriptors serve two purposes 1) identity verification at ACS 2) to allow the FBI to perform background checks. Biographic data elements on race, sex, and national origin are required by the FBI to perform background checks and background checks are required for benefit eligibility. Those data elements have been collected at the ASC for many years on FBI Form FD-258 and they are now collected electronically. To streamline submission of benefit requests that require biometric services, USCIS collects that data up front on the form to reduce the time customers must spend at the ASC.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to

use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information stored in NASS may be used for purposes outside of the original purpose of scheduling biometric appointments.

Mitigation: This risk is partially mitigated. While USCIS uses NASS primarily for scheduling appointments, USCIS also uses the personal description information maintained in NASS to verify the applicant's identity when he or she arrives at the ASC. USCIS also uses NASS to pass information to CPMS for applicant vetting. All of these uses, while not the original purpose of collection, are related to the benefits adjudication process. USCIS does not use information stored by NASS for purposes beyond benefits adjudication.

Privacy Risk: There is a risk that unauthorized users may access information stored in NASS.

Mitigation: A standard warning banner is displayed on the NASS homepage to inform users that they are about to access a DHS owned computer system. NASS displays a warning banner on the login screen to advise authorized and unauthorized users about proper and improper use of the data, that the system may be monitored to detect improper use, and the consequences of illicit use of the data. Lastly, the system's auditing capability records users' activities in the system and the system's audit logs are reviewed on a regular basis by system administrators to ensure that the system is being used appropriately.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

USCIS presents all individuals seeking immigration benefits with a Privacy Act Statement on the instructions of the application and petition. The Privacy Act Statement is located on each form's instructions. The Privacy Act Statement located on the instructions for each form notifies the individuals of USCIS's authority to collect information, and the purposes, routine uses, and consequences of declining to provide the information to USCIS prior to the collection of information.

Individuals do not interact directly with NASS, therefore USCIS cannot provide notice at the point of NASS collection. However, USCIS provides general notice to individuals through this PIA and Asylum Information and Pre-Screening,[19] Benefit Information System,[20] and Electronic Immigration System-2 Account and Case Management SORNs.[21].

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

NASS is not the original point of collection; therefore, NASS does not provide individuals the opportunity to consent to use or decline to provide the information. USCIS provides notice at the original point of collection that the individual may decline to provide the requested information, but it will result in the denial of the applicant's benefit request.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Since NASS is not the source system of collection, there is a risk that individuals will not receive notice of the purpose for which NASS uses his or her information.

Mitigation: At the original point of collection, through a Privacy Act Statement on each form's instructions, USCIS provides notice to individuals applying for benefits that USCIS uses their information to determine whether they are eligible for their respective benefit. In addition, USCIS has published information on its website about its biometric appointment process.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

USCIS has not yet developed a records retention schedule to cover the appointment scheduling records.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is privacy risk that there is no proposed retention schedule for NASS information, which leads to information being retained longer than required, and increases

[19] See DHS/USCIS-010 Asylum Information and Pre-Screening, 75 FR 409 (Jan. 5, 2010).
[20] *See* DHS-USCIS-007 Benefits Information System, 73 FR 56596 (Sept. 29, 2008).
[21] *See* DHS/USCIS-015 Electronic Immigration System-2 Account and Case Management System of Records, 78 FR 20673 (Apr. 5, 2013).

the amount of harm resulting from an unauthorized disclosure of information.

Mitigation: This risk is not mitigated. USCIS plans to propose a 99 year retention period because the relationship between an applicant and USCIS may span the applicant's entire life. Until USCIS completes a NARA-approved retention schedule, USCIS will maintain all records indefinitely. All data is protected from unauthorized disclosure and access by using appropriate technical, physical, and administrative controls.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

No.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Not applicable.

6.3 Does the project place limitations on re-dissemination?

Not applicable.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Not applicable.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no risk to external information sharing because NASS does not share information outside of DHS.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

An individual seeking access to his or her information may gain access to his or her USCIS records by filing a Freedom of Information Act (FOIA) or Privacy Act request and submitting the requests to following address:

USCIS National Records Center
Freedom of Information Act/Privacy Act Program
P. O. Box 648010
Lee's Summit, MO 64064-8010

Further information for Privacy Act and FOIA requests for USCIS records can also be found at http://www.uscis.gov.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may direct all requests to contest or amend information to the FOIA/PA Office at USCIS. Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, the proposed amendment, and clearly mark the envelope "Privacy Act Amendment."

7.3 How does the project notify individuals about the procedures for correcting their information?

USCIS application instructions, the USCIS website, this PIA, and the associated SORNs notify individuals of the procedures for correcting their information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that USCIS may not afford an individual adequate opportunity to correct data maintained in NASS**.**

Mitigation: The information in NASS is derived from other USCIS systems. Individuals are given numerous opportunities during and after the completion of the benefit request process to correct information they have provided and to respond to information received_from other sources. USCIS does not claim any Privacy Act exemptions for NASS; therefore, individuals may submit a redress request as stated in the applicable SORN.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

USCIS ensures that the information is used in accordance with the stated practices in this PIA by leveraging training, policies, rules of behavior, and auditing and accountability practices. USCIS established access and security controls to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. DHS security specifications require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All USCIS employees and contractors are required to complete annual privacy and security awareness training. The Culture of Privacy Awareness training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). The Computer Security Awareness training examines appropriate technical, physical, personnel, and administrative controls to safeguard information. In addition, USCIS provides NASS users with training on the uses of NASS prior to being approved for access.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

NASS user accounts are managed through Identity, Credential and Access Management (ICAM). Users authenticate through ICAM to gain access to NASS. ICAM deploys user role-based access controls and enforces a separation of duties to limit access to only those individuals who have a need-to-know in order to perform their duties. Each operational role is mapped to the set of system authorizations required to support the intended duties of the role. The mapping of roles to associated authorizations enhances adherence to the principle of least privilege. Authorized users are broken into specific classes with specific access rights. This need-to-know is determined by the respective responsibilities of the employee. Only necessary user identities are created and access rights assigned to NASS. These are enforced through DHS and USCIS access request forms and procedures.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

USCIS does not routinely share information collected through NASS with organizations within or outside of DHS. However, USCIS has formal review and approval process in place for new sharing agreements. The NASS Buiness Owner, Office of Information Technology, Office of Privacy, Office of Chief Counsel must approve any new use of information or new access requests for the system.

Responsible Officials

Donald K Hawkins
United States Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX A: NASS Additional Functionalities

Enterprise Gateway Integration Services (EGIS) Reference Data as a Service (RefDaaS) system

System Overview:

Enterprise Gateway Integration Services (EGIS)[22] Reference Data as a Service (RefDaaS) is a USCIS enterprise-wide service that acts as a central repository for reference data (i.e., zip code) so an authorized USCIS system with a business need does not have to create and store its own reference data through an application programming interface (API).[23] These data elements have been combined in a service accessible by all other EGIS components with reference data only and does not collect or hold personally identifiable information (PII).

NASS began ingesting new/modified zip codes generated by the U.S. Postal Service via EGIS's RefDaaS system. This is a two-way/bi-directional integration between NASS and RefDaaS in which NASS also publishes zip codes and Field Office Directorate (FOD) mappings to EGIS RefDaaS. This makes the mapping available for other USCIS systems to use/access depending on the system operational need. Since RefDaaS is considered the official source of reference data, this integration allows NASS to comply with both obtaining and publishing reference data via the official USCIS repository.

Ingesting new/modified zip codes and presenting this information ensures that NASS administrators are aware of the new/modified zip codes so that they can map them appropriately. It also reduces effort and errors since the zip codes are automatically ingested. Publishing the zip code mappings allows other USCIS systems to consume this information without the need for a direct connection to NASS.

Data Elements:

- Zip Codes; and
- FOD mappings.

Sources of Information:

This bi-directional interface allows NASS to import new and modified zip codes from RefDaaS (which receives updates from the U.S. Postal Service) and publish zip code/ FOD mappings to RefDaaS for other USCIS systems to access.

[22] EGIS serves as the foundation infrastructure that hosts and supports USCIS business services and provides the service-oriented architecture platform for USCIS. *See* DHS/USCIS/PIA-080 Enterprise Gateway and Integration Service (EGIS), *available at* www.dhs.gov/privacy.
[23] An application programming interface (API) is a connection between computers or between computer programs. It is a type of software interface, offering a service to other pieces of software.

Information Sharing:

RefDaaS is a repository for reference data only (zip codes and FOD mappings). No PII is collected or used.

System Access:

NASS users (i.e., individuals seeking to make biometric capture appointments) do not have access to RefDaaS. NASS and RefDaaS talk only via the secure API. Only authorized USCIS employees with an official need-to-know and supervisory approval have access to NASS. Access rights and privileges are monitored regularly, and user access is revoked once it is identified they do not need the information to perform their official duties.

Applicable System of Records Notice(s):

DHS/USCIS-007 Benefits Information System, which covers the collection, use, and maintenance of information for adjudication and appointment scheduling.[24]

Retention Period:

Zip codes and Field Office Directorate (FOD) mapping information are updated daily in RefDaaS, so there is no retention requirement for this type of information.

Notice:

USCIS provides notice through this NASS PIA appendix, and the EGIS Privacy Impact Assessment, which covers the use of RefDaaS to provide ordinal and index data in existing EGIS functions (e.g., U.S. Postal Service zip codes).

Correction and Redress:

An individual may file a FOIA/PA request to review his or her USCIS record by sending the request to the following address:

U.S. Citizenship and Immigration Services National
Records Center, FOIA/PA Office
P.O. Box 648010
Lee's Summit, MO 64064-8010

The information requested may, however, be exempt from disclosure under the Privacy Act because files may contain law enforcement sensitive information, and the release of such information could compromise ongoing criminal investigations. Further information for Privacy Act and FOIA requests for USCIS records can also be found at http://www.uscis.gov.

[24] *See* DHS/USCIS-007 Benefits Information System (BIS), 84 FR 54622 (October 10, 2019).