Privacy Impact Assessment Update
for the

National Appointment Scheduling System

DHS/USCIS/PIA-057(a)

August 24, 2018

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Citizenship and Immigration Services (USCIS) uses the National Appointment Scheduling System (NASS), a cloud-operated system, to schedule appointments for biometric collections at Application Support Centers (ASCs). The Canada Appointment Scheduler was created to allow individuals seeking an immigration benefit with Canada to schedule a biometrics collection appointment at an ASC. This Privacy Impact Assessment (PIA) is being updated to account for the collection, use, maintenance, and dissemination of personally identifiable information (PII) from individuals who are seeking a Canadian immigration benefit and who schedule a biometric collection appointment at an ASC.

Overview

USCIS offers a fee-based service to international partners to collect biometric and limited biographic information from individuals who are filing immigration-related benefit applications with partner countries and who are physically present in the United States. Section 573 of the Foreign Assistance Act of 1961 (FAA) authorizes U.S. agencies to furnish services to foreign countries, at the President's discretion, in furtherance of their anti-terrorism efforts. USCIS provides this service to certain partner countries for a fee agreed upon by each country and set forth in a Memorandum of Understanding (MOU).

In 2012, legacy Citizenship and Immigration Services Canada (CIC) (now Immigration, Refugees and Citizenship Canada (IRCC)) and USCIS signed an MOU allowing for USCIS to capture biometric and biographic data on behalf of the Canadian Government to determine whether visa applicants for entry to Canada are eligible to obtain visas or other travel documents according to applicable Canadian laws. USCIS used its nationwide network of ASCs to support this biometric collection for Canada, accepting individuals on a walk-in basis. In 2018, Canada expanded the scope of biometrics collection to include applicants for legal permanent residency and updated its MOU with USCIS to account for this new population. Due to the population expansion, Canada anticipates a significant volume increase in individuals using ASC facilities.

Reason for the PIA Update

Following the delegation of authority under Section 573 of the FAA, USCIS captures biometrics on behalf of Canada from individuals who are seeking Canadian immigration benefits and who are physically located in the U.S. The Canada Appointment Scheduler was created to allow these individuals to schedule a biometrics collection appointment at an ASC. USCIS created a front-end interface to allow individuals seeking immigration benefits with Canada to schedule a

biometrics appointment at an ASC.[1] This PIA is being updated to account for the scheduling of biometrics appointments for Canadian applicants at an ASC through the Appointment Scheduler.[2] The purpose of this PIA is to discuss the privacy risks associated with the collection, use, maintenance, and dissemination of PII as part of the NASS-Canada appointment scheduling system enhancement.

Certain individuals seeking an immigration benefit with IRCC are required to provide biometrics for identity verification, as well as fraud detection, security, and health and safety purposes. These individuals must provide their biometrics at an official biometric collection service location within Canada or the United States. Individuals located in the U.S. are authorized to visit an ASC for an appointment where their biometric and limited biographic data can be collected on behalf of Canada. Previously, individuals were processed at ASCs on a walk-in basis. As part of the NASS-Canada appointment scheduling system enhancement, individuals are required to schedule an appointment using Appointment Scheduler in advance.

Canada provides individuals residing in the U.S. and subject to the biometric requirement with notice detailing the requirement and instructions for scheduling a biometric appointment at an ASC. Prior to scheduling an appointment, individuals are issued an IRCC number when they apply for an immigration benefit through IRCC. The IRCC number is a unique personal identifier issued and used by the Canadian government, but is not tied to any personal information in any USCIS system. Once the individual receives the IRCC number from the IRCC, the individual may proceed to Appointment Scheduler by accessing the Appointment Scheduler link shared by IRCC.

To schedule an appointment, individuals are required to enter their IRCC number. Appointment Scheduler provides a Privacy Notice describing why USCIS is collecting personal information from individuals seeking Canadian immigration benefits prior to the collection of any information. Individuals have the right to decline to provide information, but it will prevent them from successfully scheduling a biometric appointment. While USCIS collects the IRCC number, it does not use the IRCC number to identify the individual or associate the number to any Canadian or USCIS records. USCIS collects and uses the IRCC number to assist with reserving an appointment slot and preventing duplicate appointments at an ASC.

The individual is also required to enter his or her zip code or state. Appointment Scheduler uses this information to locate the closest ASC and interfaces with NASS, a cloud-operated system, to retrieve appointment availability at the designated ASC location. Appointment Scheduler displays appointment availability for the individual to select a convenient date and time at the

---

[1] *See* DHS/USCIS/PIA-046 Customer Scheduling and Services, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-css-december2017.pdf.

[2] This service is being offered to enable USCIS to manage its ASC appointments that are applied to the services provided to our foreign partners. This service is not intended to and cannot be used for USCIS required biometric appointments.

designated ASC location. No other information is collected from the individual to schedule a biometric collection appointment.

Appointment Scheduler provides the individual with an opportunity to review and confirm the entered information and appointment slot. After the individual confirms the appointment, Appointment Scheduler automatically generates and displays an electronic appointment confirmation receipt for the individual to print. The appointment receipt contains the IRCC number, ASC address, and appointment time and date. Individuals are instructed to bring a print out of the appointment confirmation receipt to their appointment. Once an individual successfully schedules an appointment, the individual's scheduled appointment, including the IRCC number, is sent to NASS for management purposes and that appointment slot is no longer available to anyone else.

Individuals may also cancel or reschedule their appointments through Appointment Scheduler by selecting the 'manage an appointment' option. Individuals are then prompted to enter their Canadian-issued IRCC number to retrieve the confirmed appointment. Without the IRCC number, the individual is not able to cancel or reschedule their appointment. The individual then follows the step-by-step instructions to complete the appointment cancellation or rescheduling process

Upon arrival at an ASC, the individual checks in for an appointment at a designated reception counter. The individual presents the printed Appointment Scheduler confirmation appointment receipt, IRCC-issued Biometrics Instruction letter,[3] and a government-issued travel document to the Reception Desk Officer operating the counter. The Reception Desk Officer verifies the appointment in NASS and ensures the documents supplied by the individual match. Biometrics and limited biographic data are then collected from the individual and transmitted to IRCC as described in DHS/USCIS/PIA-048 USCIS International Biometric Processing Services.[4]

Privacy Impact Analysis

Authorities and Other Requirements

Section 573 of the Foreign Assistance Act of 1961 provides USCIS with the authority to conduct this fee-based service on behalf of partner countries in furtherance of their anti-terrorism efforts.

USCIS is only collecting the IRCC number through Appointment Scheduler to schedule and reserve an appointment, and is not linking the IRCC number to an individual's record in any

[3] Individuals who have applied online or by mail for a Canadian immigration benefit and who are required to enroll biometrics receive a Biometrics Instruction letter.
[4] *See* DHS/USCIS/PIA-048 International Biometric Processing Services, *available at* https://www.dhs.gov/publication/dhsuscispia-048-uscis-international-visa-project.

Canadian or USCIS system. Since no personal data for these applicants is maintained by USCIS, USCIS cannot retrieve any PII data using the provided IRCC number, a unique personal identifier. Therefore, no SORN is required to cover this collection because the data is not linked to an individual and is not retrievable by unique identifier.

NASS was issued an authority to operate on April 10, 2014. NASS is part of the Ongoing Authorization (OA) program, for which the security posture is continuously monitored and tested. The NASS Security Plan was last updated on April 10, 2017, and is in the process of being updated to include Appointment Scheduler.

USCIS plans to retain the IRCC number within NASS and associated scheduling data for 120 days for billing and reporting purposes. USCIS also retains audit logs of the transactions within NASS. NASS maintains these logs online for 180 days and then offsite for seven years. This is the standard retention period specified by DHS Security Authorization policy for system audit data; therefore, no NARA retention schedule exists.

USCIS collects scheduling data on behalf of Canada. Therefore, the information collected through Appointment Scheduler is not subject to the Paperwork Reduction Act.

Characterization of the Information

Appointment Scheduler collects the Canadian-issued IRCC number, zip code, and appointment date and time directly from the individual to schedule an appointment at an ASC. Appointment scheduling information is then transferred to and stored in NASS. At the scheduled appointment, USCIS collects biometrics and limited biographic data from the individual and transmits the data to IRCC as described in DHS/USCIS/PIA-048 USCIS International Biometric Processing Services.

Privacy Risk: There is a risk of data inaccuracy.

Mitigation: USCIS mitigates the risk of maintaining inaccurate data by collecting information directly from the individual and by verifying information at the time of the appointment. USCIS relies on the individual to provide accurate information. There are no mechanisms in place at the time of the appointment scheduling process to verify that the IRCC number was issued to the individual by IRCC. USCIS configured Appointment Scheduler to accept a 13-digit numeric value as the IRCC number. However, when an individual makes an ASC appointment, the applicant is asked to bring their appointment confirmation receipt, IRCC-issued Biometrics Instruction letter, and a government-issued travel document to verify the legitimacy of the biometric appointment. At the ASC, the appointment in NASS is matched to the IRCC number shown on the IRCC-issued Biometrics Instruction letter.

Uses of the Information

USCIS uses the IRCC number and associated scheduling information to schedule and reserve a biometrics appointment at an ASC, where biometrics are collected in support of an individual's Canadian immigration benefit request. The IRCC number is used to identify the individual when he or she arrives for the appointment, as well as for reporting and billing purposes. The zip code or state is used to locate the ASC closest to the individual scheduling the appointment.

Privacy Risk: There is a risk that the information collected may be used for purposes other than scheduling an appointment and for reporting purposes.

Mitigation: USCIS does not use the information collected beyond reserving a biometric appointment timeslot and for reporting and billing purposes. USCIS collects the IRCC number from the individual to schedule and reserve an appointment. This number is generated by the Canadian government and is not tied to any information in USCIS systems. Because USCIS does not retain this information for an extended period of time, USCIS cannot use the data for any reason other than the stated purposes. This risk is also mitigated by the terms of the agreements with Canada which limit USCIS' use of information to the purposes outlined in this PIA.

Notice

USCIS is providing general notice about the NASS-Canada appointment scheduling system enhancement through this PIA update. IRCC provides notice to appear at an ASC for biometrics collection and instruction about how to schedule an appointment in the IRCC Biometrics Appointment letter. A Privacy Notice is provided to notify individuals of USCIS's authority to collect information on behalf of Canada, and the purposes of the collection, routine uses of the information, and consequences of declining to provide the information to USCIS on behalf of Canada. There are no privacy risks associated with notice since both USCIS and IRCC provide notice to individuals.

Data Retention by the project

USCIS plans to retain the IRCC number within NASS and associated scheduling data for 120 days for billing and reporting purposes. USCIS also retains audit logs of the transactions within NASS. NASS maintains these logs online for 180 days and then offsite for seven years. NARA General Records Schedule 30 [DAA-GRS2013-0006-0003] covers the retention of audit data.

Information Sharing

USCIS provides a fee-based scheduling and biometric collection services to Canada and Canada is required to pay for the scheduling and biometric collection services. USCIS shares monthly reports from NASS detailing scheduled appointments for biometrics collection services with IRCC. The monthly reports detail the IRCC numbers, date, time, and ASC location.

Privacy Risk: There is a risk of unauthorized disclosure.

Mitigation: The risk of unauthorized disclosure is mitigated. USCIS and Canada operate under a signed MOU between the Deputy Minister of Citizenship and Immigration Canada, and the Director of U.S. Citizenship and Immigration Services. The MOU outlines the limitations on dissemination and the steps needed in order for parties to appropriately disseminate information outside of USCIS, if applicable. Additionally, all users that handle the data associated with this project must conform to appropriate security and privacy policies, follow established rules of behavior, and receive training regarding the security of DHS systems.

Redress

USCIS does not offer redress or data correction for individuals scheduling biometric appointments as part of the NASS-Canada appointment scheduling system enhancement. The IRCC is solely responsible for granting or denying applications and any redress requests. The IRCC determines as a result of a redress request whether to change any of the information that was initially provided by the USCIS ASC, and whether the request would have any impact on the adjudication process of the IRCC. The appeals process for handling inaccurate or erroneous information on behalf of the IRCC is solely the responsibility of Canada and is available on the IRCC website.[5] There are no privacy risks since IRCC is responsible for providing redress to these individuals.

Auditing and Accountability

USCIS ensures that practices stated in this PIA comply with Federal, DHS, and USCIS standards, policies and procedures, including standard operating procedures, rules of behavior, and auditing and accountability procedures. NASS is maintained in the Amazon Web Services (AWS), which is a public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational and technical controls) that are used by USCIS to protect data in accordance with federal security guidelines. AWS is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host PII. FedRAMP is a U.S. government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.

USCIS employs technical and security controls to preserve the confidentiality, integrity, and availability of the data, which are validated during the security authorization process. These technical and security controls limit access to USCIS users and mitigates privacy risks associated with unauthorized access and disclosure to non-USCIS users. Further DHS security specifications also require auditing capabilities that log the activity of each user in order to reduce the possibility

[5] For more information, *see* https://www.canada.ca/en/immigration-refugees-citizenship/services/application.html.

of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify 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.

Privacy Risk: The data maintained by AWS for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is mitigated. USCIS is responsible for all PII associated with NASS, whether on a USCIS infrastructure or on a vendor's infrastructure, and it therefore imposes strict requirements on vendors for safeguarding PII data. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security