Privacy Impact Assessment

for the

Mobile Passport Control

DHS Reference No. DHS/CBP/PIA-051(b)

November 21, 2023

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), developed the Automated Passport Control (APC) and Mobile Passport Control (MPC) programs to streamline the processing of eligible travelers entering the United States. These programs were built to allow travelers to voluntarily submit their travel document, photograph, and customs declaration information using a self-service kiosk (i.e., APC) or a mobile device application (i.e., MPC) to streamline the traveler's entry process into the United States by reducing passport control inspection time and overall wait time. CBP is publishing this Privacy Impact Assessment (PIA) to document the retirement of APC and document the expansion of MPC.

Introduction

CBP safeguards America's borders by protecting the public from dangerous people and materials while enhancing the nation's global economic competitiveness by enabling legitimate trade and travel. To accomplish the mission, CBP relies on various programs, tools, and processes. CBP developed APC and MPC to collect biographic, biometric, and inspection-related information from travelers.[1] This allows CBP to complete necessary vetting that typically occurs during the primary inspection process to reduce the administrative burden on CBP Officers conducting primary inspection and provides a more efficient entry process for travelers. Ultimately, the use of these technologies helps reduce inspection time and overall wait times for the travelers.

Automated Passport Control (APC)

CBP deployed free-standing, self-service APC kiosks to expedite the CBP entry process for eligible travelers, including U.S. citizens, Canadian visitors, U.S. Lawful Permanent Residents, Visa Waiver Program participants, and other non-immigrant classes of admission. The use of the kiosk was free and did not require membership. These kiosks, purchased by either terminal operators, airports, or seaport authorities, were installed at select airports and seaports and were maintained by one of several approved vendors to help decrease wait and inspection times. Eligible travelers submitted biographic information and responses to inspection-related questions prior to inspection by a CBP Officer. The APC kiosk also collected facial images and fingerprints.

Once the biometric information was captured, the APC kiosk transmitted biographic information and responses to inspection-related questions to CBP systems and other federal information technology systems for vetting purposes (see footnote 6). The kiosk then printed out a receipt with the traveler's face and biographic information for the traveler to present to CBP Officers at primary inspection to make manual comparisons of the newly captured facial images

[1] For more information on initial APC and MPC deployment, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED PASSPORT CONTROL AND MOBILE PASSPORT CONTROL, DHS/CBP/PIA-051, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

with the travelers, which would expedite the inspection process.

Mobile Passport Control (MPC)

MPC improves CBP processing times by allowing eligible travelers to submit passport information and responses to inspection questions prior to an inspection by a CBP Officer. With MPC, U.S. citizens and Canadian B1/B2 citizen visitors[2] may voluntarily choose to download a CBP-approved mobile application onto their personal smartphone or tablet to streamline the entry process into the United States.

After downloading the mobile application, the traveler is prompted to set up a profile using their passport information. The profile, which can be set up at any time prior to travel, includes the traveler's first and last name, gender, date of birth, passport number, passport expiration, passport country issuing authority, and country of citizenship. Once a profile is created, it is securely stored on the traveler's personal smartphone or tablet; there is no option for the user to submit the profile to CBP. Information is not transmitted to CBP until the traveler is ready to go through the inspection process.

When the traveler arrives at participating U.S. airports or seaports, or at an eligible CBP Preclearance location,[3] they launch the MPC mobile application and select "New Trip." The traveler then selects their arrival airport or seaport and terminal, takes a "selfie" photograph, and answers a series of CBP inspection-related questions. After the traveler reviews a summary of their responses and certifies that the information is truthful and correct, they securely submit the information to CBP for vetting. The traveler then receives an electronic receipt with an encrypted Quick Response (QR) code. Travelers take their physical passport and mobile device with the digital encrypted Quick Response-coded receipt to a CBP officer for primary inspection.

Reason for the PIA Update

With this Privacy Impact Assessment update, CBP is documenting changes to include: (1) the retirement of APC and (2) the expansion of MPC.

Retirement of APC

After several years of coordinated efforts with port authorities, as of October 31, 2023, CBP has decommissioned all APC kiosks. APC kiosks were initially developed to support the primary inspection process in conjunction with the Traveler Primary Arrival Client,[4] which was

[2] Canadian citizens do not require a visa to visit the United States for periods of less than 180 days. If a Canadian citizen intends to stay in the United States for longer than 180 days, they are required to obtain a B-1 (business) or B-2 (pleasure) visa.
[3] *See* https://www.cbp.gov/travel/preclearance.
[4] The Traveler Primary Arrival Client integrates several primary inspection systems so that CBP Officers can query, capture, and display biographic and biometric information through one single sign-on application. The Traveler

used to process travelers seeking entry to the United States in the air and sea environments. CBP is transitioning from the Traveler Primary Arrival Client to the Simplified Arrival process for primary inspection processing.[5] The use of Simplified Arrival makes the APCs obsolete; therefore, most ports of entry already transitioned away from use of those kiosks. Furthermore, as described below, MPC is being expanded to additional populations thereby reducing the use of and need for the APC.

The APC kiosks did not store any information locally on the kiosk. However, information from the kiosk was transmitted and stored in APC services, the backend database, for 25 months from when eligible travelers submitted their information. CBP plans to retain all information from the kiosks in APC services for 25 months from the month the information was initially collected. When the retention period has been met, CBP will purge the data from APC services. Additionally, the APC kiosk data was historically sent to downstream systems for vetting. That information has been and will continue to be maintained in those systems in accordance with those systems' retention schedules.[6]

Expansion of MPC

In June 2023, CBP expanded the use of MPC beyond U.S. citizens and Canadian citizen visitors to include U.S. Lawful Permanent Residents. CBP will update the appendix to this Privacy Impact Assessment update should MPC use be expanded beyond these populations.[7] The use of

Primary Arrival Client is a subsystem of TECS. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR TECS, DHS/CBP/PIA-009 TECS, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE APPENDIX A ON SIMPLIFIED ARRIVAL, DHS/CBP/PIA-056, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[6] Those databases include the below systems. Privacy Impact Assessments and System of Records Notices for the DHS systems can be found at https://www.dhs.gov/privacy.

- National Crime Information Center (NCIC), via a CBP interface (all travelers) – for more information about the FBI's NCIC, please see https://www.fbi.gov/services/cjis/ncic.
- DHS Office of Biometric Identity Management (OBIM), Automated Biometric Identification System (IDENT) system and successor system, Homeland Advanced Recognition Technology (HART) (foreign travelers aged 14 to 79, except Canadian Passport and Canadian Lawful Permanent Resident travelers);
- CBP Advance Passenger Information System (APIS), flight manifest data (all travelers);
- CBP TECS, Primary Query System (PQS) vetting (all travelers);
- CBP TECS, Travel Document and Enforcement Data (TDED) system (all U.S. documents);
- CBP Electronic System for Travel Authorization (ESTA) (Visa Waiver travelers); and
- CBP Electronic Visa Update System (EVUS) (Chinese 10-Year Visa travelers);
- CBP Automated Targeting System (ATS), vetting (all travelers).

[7] CBP expanded the use of MPC to U.S. Lawful Permanent Residents beginning June 5, 2023. *See* https://www.cbp.gov/travel/us-citizens/mobile-passport-control.

MPC will remain the same regardless of the population using the application.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[8] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002, Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[9]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[10] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems pursuant to the E-Government Act of 2002, Section 208[11] and the Homeland Security Act of 2002, Section 222.[12] Because MPC is a program rather than a particular information technology system, this Privacy Impact Assessment is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This Privacy Impact Assessment examines the privacy impact of MPC as it relates to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

CBP is providing transparency of these changes through the publication of this Privacy Impact Assessment update. CBP also provided notice of these changes through CBP's public-facing website. Travelers who use the MPC application are provided notice regarding the collection, use, dissemination, and maintenance of their information at the point of collection. Travelers obtain immediate notice on the device screen prior to entering their information. This notice informs travelers that the application is voluntary and that they retain the option of proceeding directly to a CBP officer

[8] 5 U.S.C. § 552a.
[9] 6 U.S.C. § 142(a)(2).
[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[11] 44 U.S.C. § 3501 note.
[12] 6 U.S.C. § 142.

for a traditional examination instead of using the MPC application. Accordingly, there are no new risks to transparency.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

There are no changes to the principle of individual participation because of this update. MPC continues to be a voluntary mobile application for eligible travelers to use to streamline the their entry process into the United States. Additionally, this update does not impact how access, redress, and correction may be sought through CBP.[13]

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The purpose for which the information is collected remains unchanged. MPC allows travelers to voluntarily choose to download and use a CBP-approved mobile application to streamline the entry process into the United States. There are no changes to CBP authorities and other requirements with this Privacy Impact Assessment update.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

CBP continues to collect and maintain the information previously outlined in the Automated Passport Control/Mobile Passport Control Privacy Impact Assessment series.[14] However, with this update, CBP is expanding the population that is eligible to use MPC, to include U.S. Lawful Permanent Residents. Additionally, CBP is working with the National Archives and Records Administration (NARA) on a records retention schedule to ensure all APC records are

[13] For detailed instructions on how to file a Freedom of Information Act (FOIA) request, Privacy Act request, or redress request through DHS Traveler Redress Inquiry Program (TRIP), *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED PASSPORT CONTROL AND MOBILE PASSPORT CONTROL, DHS/CBP/PIA-051 (2018 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[14] *Id.*

properly destroyed after 25 months from initial collection. There are no new risks to data minimization.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

There are no changes to the use of information because of this update. MPC allows travelers to voluntarily choose to download and use a CBP-approved mobile application to streamline the entry process into the United States. This advance collection of traveler related information allows CBP to complete necessary vetting that typically occurs during the inspection process to reduce the administrative burden on CBP officers and provide a more efficient entry process for travelers. There are no new risks to the use of information.

In the original Privacy Impact Assessment, the CBP Privacy Office noted its intention to conduct a CBP Privacy Evaluation within one year of publication of the Privacy Impact Assessment to ensure that CBP and its commercial partners were in compliance with required privacy protections. Following implementation of the program, however, the CBP Privacy Office assessed that it was not as privacy sensitive as originally thought. Since 2015, CBP has conducted sixteen (16) Privacy Threshold Analyses on MPC and APC to assess any changes in privacy compliance requirements. With the decommission of the APC program, CBP will continue to assess and monitor MPC privacy compliance, including through required Privacy Threshold Analyses.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

There are no changes to the principle of data quality and integrity because of this update.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

There are no changes to the principle of security because of this update.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

There are no changes to auditing and accountability because of this update. MPC continues to locally store user profile information within the MPC mobile application, and no information is shared with CBP until the user submits the information. The MPC mobile application allows travelers to securely store personally identifiable information within their profiles on their own device for future travel, or the traveler may delete their profile information after a single use or at any subsequent point.

Conclusion

With this Privacy Impact Assessment update, CBP is documenting changes to the Automated Passport Control and Mobile Passport Control Privacy Impact Assessment series to discuss: (1) the retirement of APC and (2) the expansion of MPC. CBP is expanding the use of MPC beyond U.S. citizens and Canadian citizen visitors to include U.S. Lawful Permanent Residents. CBP will update the appendix to this Privacy Impact Assessment update should use of MPC be expanded beyond these populations.

Contact Official

Matthew Davies
Executive Director, Admissibility and Passenger Programs
Office of Field Operations
U.S. Customs and Border Protection

Responsible Official

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
privacy.cbp@cbp.dhs.gov

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

APPENDIX A: Populations Eligible to use Mobile Passport Control

(last updated 9/18/2024)

- U.S. citizens
- U.S. Lawful Permanent Residents
- Canadian citizens admitted under the B1, B2, TN, TD, L, P, O Class of Admission
- Returning VWP visitors
- Bahamian citizens under the B1/B2 COA that meet current visa-exempt criteria[15]

[15] Visa exempt criteria includes: (1) Departure out of the Nassau Pre-clearance port of entry; (2) Have no criminal record nor any legal ineligibility or inadmissibility; and (3) Have a Police Certificate issued within the past six months if 14 years of age or older).