Privacy Impact Assessment Update

for the

Automated Passport Control (APC) and Mobile Passport Control (MPC)

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

June 9, 2021

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 automate and streamline the processing of eligible travelers entering the United States. APC and MPC allow travelers to voluntarily answer inspection-related questions using a self-service kiosk (APC) or a mobile device application (MPC) and this data is then transmitted to CBP prior to the CBP Officer (CBPO) inspection process. CBP is conducting this Privacy Impact Assessment (PIA) update to assess the privacy risks and provide notice of 1) an addition to the list of inspection-related questions that travelers using APC kiosks or an MPC mobile application must answer; 2) further deployment of the CBP MPC mobile application, which will be available for use at all MPC-enabled sites; and 3) an internal change to the MPC process, allowing CBPOs to process family members arriving together in one transaction through the MPC mobile application.

Introduction

CBP is charged with protecting U.S. borders while facilitating lawful travel and trade. Technology such as automated kiosks and mobile applications provide alternative approaches that allow CBP to optimize limited officer resources. These technological advances also shift the administrative burden to the traveler, which in turn allows CBPOs the ability to focus on law enforcement functions such as identity verification, admissibility, and questioning to determine the individual's intent of travel. Additionally, the automated kiosks and mobile applications assist airport authorities in facilitating traveler entry processing and reducing wait times.

CBP developed the APC and MPC programs to collect biographic and inspection-related information from travelers. APC and MPC collect and securely transmit information to CBP to vet against CBP and federal databases[1] to locate any derogatory information. The APC and MPC programs reduce the administrative burden on CBPOs and provide a more efficient entry process

[1] 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).

for travelers. Ultimately, the use of these technologies helps reduce inspection time and overall wait times for the travelers.

Automated Passport Control

APC uses free-standing, self-service kiosks to automate the CBP entry process for eligible travelers. The following travelers are eligible to use the kiosks: U.S. citizens, Canadian citizen visitors, U.S. Lawful Permanent Residents (LPR), Visa Waiver Program (VWP) participants entering under the waiver-business (WB) or waiver-tourist (WT) class of admission,[2] and certain other non-immigrants.[3] The kiosks are purchased by terminal operators, airport authorities, seaport authorities, airlines, cruise operators, or ferry operators. The kiosks are installed at select airports and seaports and are maintained by one of several approved vendors to help decrease wait and inspection times.

Using an APC kiosk is free, voluntary, and does not require pre-registration or membership. When single travelers or family units approach the APC kiosk, they first acknowledge the CBP Privacy Policy and other required notices[4] by following the instructions provided on the kiosk screen. Then the traveler scans or swipes his or her passport's machine-readable zone (MRZ), poses for a facial photograph[5] captured by the kiosk and its server, and verifies biographic and flight information on the screen and answers a series of CBP inspection-related questions. If a traveler is arriving with family members, the head of the household completing this initial entry must complete the inspection-related questions for their entire family through the APC kiosk. After the head of the household has entered their information and completed the inspection-related questions for their family members, the system will prompt the head of the household to enter and submit biographic and biometric information (e.g., facial photograph and fingerprints, if applicable) for each additional family member separately through the APC kiosk. Non-U.S. citizen APC kiosk users must also select a class of admission and may be required to provide fingerprints depending on class of admission.

APC kiosk systems use APC Services to transmit biographic information and responses to inspection-related questions to CBP systems which in turn query federal information technology systems for vetting purposes.[6] Once the traveler has completed the required steps, the APC kiosk prints out a receipt that includes some biographic information and the photograph of the traveler. The traveler then presents the receipt to a CBP Primary Officer who reviews the APC kiosk receipt,

[2] Participation in VWP requires enrollment in CBP's Electronic System for Travel Authorization (ESTA) program.
[3] Other non-immigrants include U.S. visa holders entering under the following classes of admission: B1/B2, C1/D, and D1.
[4] Notices include Privacy Act Statement, Intellectual Property Rights, Paperwork Reduction Act, and Section 311 of the Trade Facilitation and Trade Enforcement Act of 2015.
[5] CBP does not use facial recognition technology through the APC and MPC process.
[6] Includes external systems such as NCIC and DHS OBIM's IDENT/HART, and CBP systems such as TECS (PQS and TDED), APIS, ESTA, ATS, and EVUS.

travel documentation, and finalizes the inspection.

Mobile Passport Control

Travelers voluntarily elect to participate in the MPC program through the mobile application. MPC improves CBP processing times by allowing eligible travelers to submit passport information and responses to inspection questions, prior to an inspection by a CBPO. With MPC, U.S. citizens and Canadian citizen visitors may download a CBP-approved mobile application onto their personal smartphone or tablet to automate the entry process into the United States. Additionally, MPC-enabled mobile applications are voluntary and free versions of each application are available to the public. Some applications may offer a premium service for a fee, but CBP will only approve applications that also offer international travelers a free MPC service.

The MPC mobile application is accessible through a separate CBP government mobile application, CBP Mobile Passport Control, or through various third-party vendors. A complete list of each vendor approved MPC-enabled mobile applications is included in Appendix B.

After eligible travelers download an authorized app from the Google Play Store or Apple App Store, travelers will be prompted to acknowledge the Privacy Policy and create a profile with their passport information. Travelers can set up a profile in the application any time prior to arrival to the United States, and once a profile has been established, they do not need to redownload the mobile application each time they arrive. In order to create a profile, the individual must create a PIN number, which will be stored locally on the individual's mobile device. The PIN number is not retained by the MPC application or CBP.

CBP has improved the MPC process by allowing families to use one device to create multiple profiles and submit a single transmission to CBP for processing. The profile includes the traveler's name, gender, date of birth, country of citizenship, and a self-taken photo. When the traveler lands in the United States, he or she begins the inspection process using the application by selecting his or her arrival airport, and answering a set of CBP inspection-related questions, including confirming biographic and flight information. After the traveler reviews a summary of his or her responses and certifies that the information is truthful and correct, he or she securely submits the information to CBP. Once the traveler submits their transaction through MPC, the traveler will receive an electronic receipt with an Encrypted Quick Response (QR) code. Travelers then bring their physical passport and mobile device with their digital QR-coded receipt to a CBPO to finalize their inspection for entry into the United States.

Reason for the PIA Update

CBP is conducting this PIA update to assess the privacy risks and provide notice of 1) an addition to the list of inspection-related questions that the travelers using APC kiosks or an MPC mobile application must answer; 2) further deployment of the CBP MPC mobile application, which will be available for use at all MPC-enabled sites; and 3) an internal change to the MPC process, allowing CBPOs to process family members arriving together in one transaction through the MPC mobile application.

New Inspection Question

CBP updated the inspection-related questions via the APC and MPC to include a new biological research materials question. The new question is as follows, "Do I (we) have any disease agents, cell cultures, or biological research materials?" The responses to the CBP questions are saved for 24 months in a CBP backend database and then purged. As with all responses to APC and MPC questions, a positive response to this question may lead to additional questioning and processing by a CBPO.

MPC Internal Process Change

In the past, family members arriving together as a group at a CBP Primary inspection area would use an MPC mobile application to enter the information for each traveling family member from their group and the MPC mobile application would generate a separate QR code for each family member. As the family entered a primary inspection area, they would present all QR codes assigned to their family to the CBPO. The CBPO would then scan each individual QR code to verify the authenticity of the receipt, which would display a referral code, along with responses to the inspection questions. The CBPO would then review the information and process each traveling family member individually, via multiple transactions, through their CBP workstation screen. This process was inefficient and increased wait times at CBP Primary inspection areas.

In an effort to streamline this process, CBP can now link all QR codes assigned to family members traveling together under a single scan on a CBPO's workstation. This will assist CBPOs as they will be able to quickly process family members arriving together in a single transaction on their CBP workstation, rather than having to create multiple transactions for family members traveling together. The CBP system will now recognize the family members are traveling together as their QR codes would be linked with the same transaction and each family members information would be displayed on the CBPO's workstation for individual adjudication. This change only affects the CBPOs' workstation screen view and the MPC process will not affect the traveler's experience.

CBP Mobile Passport Control mobile application

Recently CBP developed a new public-facing government-owned and operated mobile

application, "Mobile Passport Control (MPC) by U.S. Customs and Border Protection," which provides travelers a new mobile option, through a federal government mobile application, to access the MPC program and streamline entry into the United States. Eligible travelers can download this free government mobile application from the Google Play Store or Apple App Store and use it to submit their passport information and answers to inspection-related questions to CBP via a smartphone or tablet prior to inspection. The CBP MPC streamlines the border inspection process upon entry into the United States and mirrors the functionality of the existing MPC external (vendor owned) mobile applications.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[7] 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.[8]

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.[9] 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[10] and the Homeland Security Act of 2002, Section 222.[11] Given that MPC is a mobile application rather than a particular information technology system, this PIA is conducted as it relates to the DHS's construction of the Fair Information Practice Principles. This PIA examines the privacy impact of APC and MPC as they relate to the Fair Information Practice Principles.

---

[7] 5 U.S.C. § 552a.
[8] 6 U.S.C. § 142(a)(2).
[9] 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.
[10] 44 U.S.C. § 3501 note.
[11] 6 U.S.C. § 142.

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.

There is no change to transparency with this PIA update. Travelers who use the APC kiosks or 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 kiosk or device screens prior to entering their information. Both notices inform travelers that the use of these approaches is purely voluntary and that they retain the option of proceeding directly to the CBPO for the more traditional examination instead of using the APC kiosk or the MPC app.

Additional information about the APC and MPC programs can be found here: https://www.cbp.gov/travel/us-citizens/apc and https://www.cbp.gov/travel/us-citizens/mobile-passport-control.

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 as a result of this update. Although CBP is now grouping MPC transactions, this is a backend feature and does not change how the traveler inputs or views information.

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 collected from travelers for transmission to CBP via the APC and MPC processes remains the same as previously described and analyzed in full in the 2018 APC and MPC PIA.[12] CBP's use of the APC kiosk or MPC mobile application does not

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED PASSPORT CONTROL (APC) AND MOBILE PASSPORT CONTROL (MPC), DHS/CBP/PIA-051 (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

change the purpose for which the information collected or the manner in which it is used, and the use of information is consistent with the existing border inspection process.

The APC kiosk and MPC mobile application will collect a new inspection question from travelers. The question is as follows, "Do I (we) have any disease agents, cell cultures, or biological research materials?" This answer to this question must be entered by the traveler and submitted through the APC kiosk or MPC mobile application. Once the traveler has completed the required information, the APC kiosk prints out a receipt that includes answers to each inspection question. The traveler then presents the receipt to a CBPO. Travelers who choose to not use the APC kiosk or MPC mobile application may use the traditional CBP border inspection process, which involves a CBPO conducting a primary examination on a traveler without the aid of APC/MPC technology.

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).

The APC and MPC records retention schedule remains unchanged. The APC kiosk vendor collects transactional data through the APC kiosk and this transactional data is stored on the vendor's servers. The vendor does not store any PII, including biographic or biometric information on their servers.

MPC-enabled mobile applications, however, allow travelers to voluntarily securely store PII within their MPC profiles on their own device for future travel. Travelers using the MPC mobile application can set up a profile in the application any time prior to arrival to the United States. In order to create a profile, the individual must create a PIN number, which will be stored locally on the individual's mobile device. The PIN number is not retained by the MPC application or CBP.

CBP recently updated the inspection-related questions via the APC and MPC to include a new biological research materials question. The new question is as follows, "Do I (we) have any disease agents, cell cultures, or biological research materials?" The responses to the CBP questions are saved for 24 months in a CBP backend database and then purged.

Presently, if the APC kiosk receipt is free of declarations, it is retained for only three (3) years and destroyed. If the receipt contains dutiable declarations, it is retained for six (6) years and destroyed. CBP is working with the National Achieves and Records Administration (NARA) to create a records schedule specifically for the APC and MPC programs and for the APC kiosk receipts. CBP is proposing a one-year retention period for the APC kiosk receipts.

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 principle of use limitation as a result of this update.

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 as a result 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 as a result 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 the principle of accountability and auditing as a result of this update.

Conclusion

CBP updated this PIA to document several changes to the APC-MPC program. Those changes included an addition to the inspection questions collected from travelers through the APC kiosk and MPC application. CBP also created a method for families using MPC to only scan one single QR code for their entire family to be displayed and adjudicated rather than each family member having to scan a QR code. Finally, CBP updated the list of approved MPC applications, including a new CBP built MPC application called “Mobile Passport Control by U.S. Customs and

Border Protection." CBP continues to use the APC-MPC program to automate and streamline the processing of eligible travelers entering the United States while ensuring adequate privacy protections are in place.

Contact Official

Matthew S. 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.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

APPENDIX A: Mobile Application Security Review Process

There are no changes to Appendix A as a result of this update.

APPENDIX B: Approved Mobile Applications

DHS analyzed the MPC-enabled applications below to assess overall security and identify potential vulnerabilities, according to the process outlined in Appendix A of the 2018 APC and MPC PIA. The application developer addressed each reported issue and implemented recommendations. CBP incorporated the final security analysis and the developer's functional requirements into current and future business requirements. CBP approved the following MPC-enabled mobile applications for deployment:

- Airside Mobile, in cooperation with the Airports Council International-North America (ACI- NA), Mobile Passport App
    - Available at all MPC-enabled sites for both Android and iOS/Apple users
- Clear, in cooperation with Delta Airlines, ClearPass for CBP Mobile Passport Control
    - Available at all MPC-enabled sites for iOS/Apple users

CBP currently has 34 MPC-enabled sites across the country:

- Baltimore/Washington International Thurgood Marshall Airport (BWI)
- Boston Logan International Airport (BOS)
- Chicago O'Hare International Airport (ORD)
- Dallas/Fort Worth International Airport (DFW)
- Daniel K. Inouye International Airport (HNL)
- Dulles International Airport (IAD)
- Denver International Airport (DEN)
- Fort Lauderdale-Hollywood International Airport (FLL)
- Houston George Bush Intercontinental Airport (IAH)
- John F. Kennedy International Airport (JFK)
- Kansas City International Airport (MCI)
- Los Angeles International Airport (LAX)
- Miami International Airport (MIA)
- Miami Seaport
- Minneapolis-Saint Paul International Airport (MSP)

- Newark Liberty International Airport (EWR)
- Oakland International Airport (OAK)
- Orlando International Airport (MCO)
- Palm Beach Seaport
- Philadelphia International Airport (PHL)
- Phoenix Sky Harbor International Airport (PHX)
- Pittsburgh International Airport (PIT)
- Port Everglades Seaport
- Portland International Airport (PDX)
- Sacramento International Airport (SMF)
- Salt Lake City International Airport (SLC)
- San Diego International Airport (SAN)
- San Francisco International Airport (SFO)
- San Jose International Airport (SJC)
- San Juan Airport (SJU)
- San Juan Seaport
- Seattle-Tacoma International Airport (SEA)
- Tampa International Airport (TPA)
- William P. Hobby Houston International Airport (HOU)