

CBP Has Placed Travelers' PII at Risk of Exploitation





OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

July 15, 2021

MEMORANDUM FOR: Troy A. Miller
Senior Official Performing the Duties of the
Commissioner
U.S. Customs and Border Protection

FROM: 
Joseph V. Cuffari, Ph.D.
Inspector General

SUBJECT: *CBP Has Placed Travelers' PII at Risk of Exploitation*

Attached for your action is our final report, *CBP Has Placed Travelers' PII at Risk of Exploitation*. We incorporated the formal comments from U.S. Customs and Border Protection in the final report.

The report contains eight recommendations aimed at improving the security of the Mobile Passport Control (MPC) program. Your office concurred with all eight recommendations. Based on information provided in the response to the draft report, we consider recommendations 1 through 8 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce B. Miller, Deputy Inspector General for Audits, at (202) 981-6000.



DHS OIG HIGHLIGHTS

CBP Has Placed Travelers' PII at Risk of Exploitation

July 15, 2021

Why We Did This Audit

U.S. Customs and Border Protection (CBP) is responsible for securing travelers' data from cybersecurity threats. CBP's Mobile Passport Control (MPC) applications (app) — used by more than 10 million travelers from July 2017 through December 2019 — contained the travelers' personally identifiable information (PII) used to expedite them through CBP's inspection process.

Our audit objective was to determine to what extent CBP protects its MPC apps from cybersecurity threats.

What We Recommend

We made eight recommendations to improve the security of CBP's MPC program.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHSOIG.OfficePublicAffairs@oig.dhs.gov

What We Found

CBP did not always protect MPC applications from cybersecurity threats. Although required to scan MPC app version updates to detect vulnerabilities, CBP did not scan 134 of the 148 (91 percent) updates released from 2016 through 2019. This occurred because CBP officials relied on version updates from app developers but were not always notified when updates occurred. Additionally, CBP did not always identify vulnerabilities detected in scan results because CBP guidance does not require a review of all results.

CBP also did not complete seven security and privacy compliance reviews of MPC apps, as required by the MPC Privacy Impact Assessment, because CBP did not establish a schedule for the reviews or track and centrally store review documentation. In addition, CBP did not obtain the information needed for the reviews, had competing priorities, and did not ensure app developers created a required process CBP needed to perform a mandatory internal audit.

Finally, although required by Department of Homeland Security policy, CBP did not implement specific hardware and software configuration settings on MPC servers to protect them from vulnerabilities because CBP incorrectly believed it could phase in the settings.

Unless CBP addresses these cybersecurity vulnerabilities, MPC apps and servers will remain vulnerable, placing travelers' PII at risk of exploitation.

CBP Response

CBP concurred with all eight recommendations.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Background 2

Results of Audit 5

 CBP Did Not Scan MPC Apps to Detect Vulnerabilities 5

 CBP Did Not Detect Vulnerabilities Identified in Scans 7

 CBP Did Not Complete Security and Privacy Compliance Reviews..... 8

 CBP’s Management of System Configuration Was Inadequate..... 10

Recommendations..... 12

CBP’s Management Response and OIG Analysis 13

Appendixes

Appendix A: Objective, Scope, and Methodology 16

Appendix B: CBP Comments to the Draft Report..... 18

Appendix C: Report Distribution 23

Abbreviations

app	application
CBP	U.S. Customs and Border Protection
DISA	Defense Information Security Agency
MPC	Mobile Passport Control
OIG	Office of Inspector General
OS	operating system
PII	personally identifiable information
RTM	Requirements Traceability Matrix
STIG	Security Technical Implementation Guide



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Background

U.S. Customs and Border Protection (CBP) is responsible for securing U.S. borders and facilitating lawful international travel and trade. CBP continues to modernize efforts to streamline the inspection process, increase officer efficiency, and reduce operating costs to provide enhanced services for travelers entering the United States. As such, CBP facilitated the development of the Mobile Passport Control (MPC) application (app) to assist in expediting travelers through the primary inspection process. Third-party developers create, maintain, and operate the MPC apps, which transmit travelers’ personally identifiable information (PII)¹ upon arrival at participating ports of entry.

Beginning in August of 2014, CBP authorized three apps, which function on two different major mobile operating systems (OS A and OS B) for traveler download and use. See Table 1 for CBP authorized MPC apps.

Table 1. CBP Authorized MPC Apps

App Name	Operating System (OS)	Initial Release Date
App 1	OS A	August 5, 2014
	OS B	July 14, 2015
App 2*	OS A	May 26, 2017
	OS B	May 4, 2017
App 3*	OS A	October 29, 2018
	OS B	November 1, 2018

Source: DHS Office of Inspector General (OIG) analysis of MPC app release dates

* As of June 10, 2021, App 2 and App 3 are no longer in operation.

¹ PII is information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

U.S. citizens and Canadian visitors may download and use any one of these apps at 1 of the 29 participating U.S. international airports or 4 seaports of entry. From July 2017 through December 2019,² more than 10 million travelers used the apps to submit PII for expedited travel into the United States. Additionally, from fiscal years 2016 through 2019, CBP expended on average \$639,000³ each year for MPC, funded through its Trusted Traveler Program⁴ enrollment fees.

MPC apps help expedite travel and primary inspections at ports of entry. However, apps are susceptible to vulnerabilities that create security risks. Specifically, apps are susceptible to cybersecurity vulnerabilities⁵ (referred to simply as “vulnerabilities” throughout this report) categorized as either critical, high, medium, or low, with critical representing traveler information at the highest risk for exploitation. When travelers use the app, they transmit their PII to CBP through the app developer server sites, which creates additional risk.

CBP’s MPC Program Office is primarily responsible for overseeing the MPC program for CBP. The office collaborates with CBP’s Offices of Information and Technology, and Privacy and Diversity, as well as the Department of Homeland Security, Office of the Chief Information Officer to complete app security processes. Collaboratively, these offices developed the *Mobile Passport Control (MPC) Business Requirements (July 2019)* (referred to simply as “Business Requirements” throughout this report), which establish procedures and requirements to safeguard systems, servers, and apps against cybersecurity vulnerabilities and mitigate risk. The MPC Program Office relies on Office of Information and Technology specialists, Privacy and Diversity Office staff, CBP Office of Field Operations officers, and contractors to ensure app developers adhere to the Business Requirements prior to authorizing the app for use.

CBP uses a series of security and privacy compliance reviews to ensure the apps adhere with its Business Requirements. CBP’s security review consists of four compliance reviews:

² The Department of Homeland Security would incur a cost to obtain pre-July 2017 app usage information from a third-party storage provider; therefore, our analysis is based on app usage data available to the Department at the time of our audit.

³ We calculated the average using MPC Program expenditures for FYs 2016–2019.

⁴ Trusted Traveler Programs are risk-based programs to facilitate the entry of pre-approved travelers.

⁵ A vulnerability is one or more weaknesses that can be accidentally triggered or intentionally exploited and result in a violation of desired system properties.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

1. The DHS' "AppVet" cybersecurity scan (referred to simply as "scan" throughout this report) consists of multiple commercial, open-source, and government-developed scanning services to assist with detecting vulnerabilities and malware.⁶ The MPC Program Office coordinates with the DHS Office of the Chief Information Officer and CBP's Office of Information and Technology to perform the initial and periodic scans as required by CBP's Business Requirements. Additionally, the MPC Program Office coordinates with the CBP Office of Information and Technology specialists to review the scan results to identify vulnerabilities requiring remediation, which is confirmed by performing a follow-up scan.
2. The Requirements Traceability Matrix (RTM) ensures developer server sites comply with CBP's information system security requirements.
3. The Screenshot compliance review is a screen-by-screen evaluation of the traveler's experience to verify application compliance with privacy requirements.
4. The Functionality test assesses application performance to ensure the traveler receives pop-up notifications before granting the application permission to access the mobile device's camera.

Further, the MPC Program Office, Office of Information and Technology, and Privacy and Diversity Office collaborate and coordinate privacy compliance reviews of MPC program stakeholders.⁷ Collectively, there are three privacy reviews CBP performs on MPC key stakeholders. Specifically, (1) a privacy evaluation to ensure government and commercial partners comply with required privacy protections, (2) internal audits to confirm application developers have privacy and security protections in place, and (3) periodic reviews of internal access logs to verify restricted access of traveler PII to DHS employees and contractors who have completed annual privacy and security training.

In addition, DHS issues configuration management control requirements to its components on how to protect information systems from vulnerabilities. DHS uses the *Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG)* as its configuration standard. STIGs provide

⁶ Malware is software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Types of malware include a virus, worm, Trojan horse, or other code-based entity that infects a host.

⁷ MPC program stakeholders include MPC app sponsors, developers, and CBP personnel.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

necessary technical guidance to secure information systems and software to mitigate potential cybersecurity threats and reduce vulnerabilities.

The security and privacy compliance reviews and configuration management controls requirements must be completed and followed to provide maximum security of traveler data.

We conducted this audit to determine to what extent CBP protects its MPC apps from cybersecurity threats.

Results of Audit

CBP did not always protect MPC applications from cybersecurity threats. Although required to scan MPC app version updates to detect vulnerabilities, CBP did not scan 134 of the 148 (91 percent) updates released from 2016 through 2019. This occurred because CBP officials relied on version updates from developers but were not always notified when updates occurred. Additionally, CBP did not always identify vulnerabilities detected in scan results because CBP guidance does not require a review of all results.

CBP also did not complete seven security and privacy compliance reviews of MPC apps, as required by the MPC Privacy Impact Assessment, because CBP did not establish a schedule for the reviews or track and centrally store review documentation. In addition, CBP did not obtain the information needed for the reviews, had competing priorities, and did not ensure app developers created a required process CBP needed to perform a mandatory internal audit.

Finally, although required by DHS policy, CBP did not implement specific hardware and software configuration settings on MPC servers to protect them from vulnerabilities, because CBP incorrectly believed it could phase in the settings.

Unless CBP addresses these cybersecurity vulnerabilities, MPC apps and servers will remain vulnerable, placing travelers' PII at risk of exploitation.

CBP Did Not Scan MPC Apps to Detect Vulnerabilities

CBP's Business Requirements direct CBP to scan MPC apps prior to their release each time a developer updates an app version to detect vulnerabilities. However, CBP did not always complete the required scans from 2016 through 2019. This occurred because CBP did not track version updates and instead relied on app developers to send ad-hoc notifications informing CBP of newly



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

released app version updates. Moreover, when we conducted the same scans available to CBP, using DHS' Office of the Chief Information Officer, for the six apps available for traveler use on May 13, 2020, and on November 5, 2020, we identified cybersecurity vulnerabilities.

App Version Updates Not Scanned

Even though CBP's Business Requirements mandate that CBP scan each app version to detect vulnerabilities whenever a developer releases an update for traveler use, CBP did not perform the required scans. Specifically, CBP did not scan 134 of the 148 (91 percent) app version updates released from 2016 through 2019.

Additionally, of the 14 scans CBP completed, it scanned 5 app versions several weeks after developers released the version updates to the public, which when used could have contained vulnerabilities exposing travelers' PII. See Table 2 for MPC app scans performed after version release.

Table 2. MPC App Scans Performed after Version Release

App Name	Operating System	Version Number	Release Date	Scan Date
App 1	OS A	1.2.8	8/8/2016	9/23/2016
App 1	OS A	3.4	7/22/2019	8/13/2019
App 1	OS B	2.22	7/23/2019	8/13/2019
App 2	OS A	2.17	7/17/2019	8/13/2019
App 2	OS B	2.17	7/17/2019	8/13/2019

Source: DHS OIG analysis of CBP MPC app cybersecurity testing

This occurred because CBP did not track app version updates. Instead, CBP relied on app developers to inform them of any app version updates prior to release. However, CBP received just 5 notifications of the 148 app version update releases from 2016 through 2019.

Scans Detect Cybersecurity Vulnerabilities

We could not perform scans on the 148 legacy app versions released from 2016 through 2019 due to availability issues. We requested that the DHS Office of the Chief Information Officer scan the six app versions available for traveler use on May 13, 2020, and on November 5, 2020. These scans detected cybersecurity vulnerabilities. The May 13, 2020 scans revealed two app versions contained six high-risk vulnerabilities. For example, one of the apps contained a vulnerability that set incorrect default permissions, which allowed information to read and write to external storage locations unknown to the



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

traveler. The other app contained a vulnerability specific to the storage of sensitive information as “cleartext” — unencrypted information that attackers can potentially read.

In the second round of scans on November 5, 2020, an updated version of the same app identified on May 13, 2020, as having two vulnerabilities contained the same two vulnerabilities. Table 3 shows MPC app scan results.

Table 3. MPC App Scan Results

Mobile App/Version	Scan Date	Operating System	Total	Risk
App 3 V.4.3.4	May 13, 2020	OS B	2	High
App 2 V.2.20	May 13, 2020	OS B	4	High
App 3 V.4.5.1	November 5, 2020	OS B	2	High

Source: DHS OIG analysis of DHS AppVet scan reports

CBP Did Not Detect Vulnerabilities Identified in Scans

According to *Standards for Internal Control in the Federal Government*,⁸ management should design control activities including policies, procedures, techniques, and mechanisms to achieve the entity’s objectives and respond to risks. However, CBP did not identify seven vulnerabilities that scans in 2019 detected in three MPC app versions. Table 4 shows MPC apps with vulnerabilities CBP did not identify.

Table 4. MPC Apps with Vulnerabilities Unidentified by CBP

Mobile App/Version	Operating System	Scan Date	Total	Risk
App 1 V.2.18	OS B	3/21/2019	1	High
App 1 V.2.22	OS B	8/13/2019	1	High
App 2 V.2.17	OS B	8/13/2019	5	High

Source: DHS OIG analysis of CBP AppVet scan reports

We identified these seven vulnerabilities in the 2019 AppVet scan results CBP previously obtained from the DHS Office of the Chief Information Officer. Although specialists in CBP’s Office of Information and Technology have the knowledge needed to review the scan results, according to CBP officials, they did not coordinate the scan results review with them to help identify vulnerabilities.

⁸ Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government*, September 2014.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

This occurred because CBP's Business Requirements and MPC standard operating procedures⁹ do not codify scan processes or define the roles and responsibilities as needed to ensure scans are completed as required and Office of Information and Technology specialists review results. CBP policies also do not require review of all scan results to identify vulnerabilities.

CBP Did Not Complete Security and Privacy Compliance Reviews

According to CBP's *Privacy Impact Assessment for Automated Passport Control (APC) and Mobile Passport Control (MPC)* of March 19, 2018 (Privacy Impact Assessment),¹⁰ CBP was required to complete seven security and privacy compliance reviews of MPC apps and servers — four annual compliance reviews and three time-sensitive privacy security reviews. Security compliance reviews ensure app developer server sites adhere to CBP's information system security requirements and MPC apps comply with privacy requirements outlined in CBP's Business Requirements. Specifically, according to the Privacy Impact Assessment, CBP was to complete four annual security compliance reviews — (1) scan, (2) RTM, (3) screenshot, and (4) functionality — to ensure MPC developers did not put travelers' PII at risk. Further, per CBP's Privacy Impact Assessment, within 1 year of its publication, CBP was to complete a privacy evaluation, periodically review system internal access logs to ensure traveler information is restricted, and conduct an internal audit for which the app developer was required to create the process for CBP to execute by the end of 2018.

However, CBP did not complete all required security compliance reviews. Specifically, CBP did not complete 38 of the 64 (59 percent) annual compliance reviews and did not complete any of the three types of privacy and security reviews from 2016 through 2019. See Table 5 for the number of security compliance reviews required, completed, and not completed.

⁹ *Mobile Passport Control Standard Operating Procedures (SOP)*, December 27, 2017.

¹⁰ Privacy Impact Assessments are assessments of technologies, rulemakings, programs, and activities, regardless of their type or classification, to ensure that privacy considerations and protections are incorporated into all activities of the Department in accordance with the Privacy Office's duties under Public Law (P.L.) 107-347 § 208, *E-Government Act of 2002*, P.L. 107-296, *Homeland Security Act of 2002*, and other statutes, as applicable.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table 5. Required Security Compliance Review Status, 2016–2019

Type of Security Compliance Review	Specific Review	Required	Completed	Not Completed
Compliance	Scan	18	12	6
	RTM	10*	2	8
	Screenshot	18	8	10
	Functionality	18	4	14
	Total	64	26	38
Privacy and Security	Internal Access Logs	1**	0	1
	Privacy Evaluation	1	0	1
	Internal Audit	1	0	1
	Total	3	0	3

Source: DHS OIG analysis of CBP security compliance reviews from 2016 to 2019

* RTMs are required by developer server site and are not required for each application; therefore, the annual number of RTMs required varies.

** The Privacy Impact Assessment does not define a periodic review schedule. We requested one internal access log review to assess, and CBP could not provide it because it did not complete any internal access log reviews.

CBP did not complete all these reviews because CBP’s Business Requirements and MPC Standard Operating Procedures do not include processes to conduct reviews on a specific schedule, track reviews completed, and centrally store review documentation. Specifically, CBP did not complete the six scan reviews because it did not follow a scan schedule to ensure annual scans. Instead, CBP conducted these scans inconsistently throughout multiple years and did not track scan completion. Further, CBP did not track completion of 10 of the 18 required annual screenshot reviews and 14 of the 18 required functionality tests. However, according to CBP officials, they agreed to develop a table to begin tracking completion of these tests.

CBP was unable to provide all scan documentation, and the documentation they were able to retrieve was through e-mails as opposed to a central repository for scan documentation storage. For one developer, CBP could not locate and provide us with any functionality tests because they were not stored anywhere.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Additionally, CBP did not always have all information necessary to complete RTM reviews. App developers must provide CBP with a completed RTM questionnaire to ensure their server sites have the necessary physical security protocols¹¹ and required information technology security settings in place. However, CBP was unable to complete 8 of the 10 RTM reviews because it did not receive all RTM results from app developers. Developers submitted just 2 of the 10 required annual RTM reviews from 2016 through 2019, and the 2016 review the developers submitted was incomplete and missing key information, such as the server site code, name, and date. CBP officials agreed standardizing the template for the MPC RTM would help them obtain the information needed to complete the reviews.

CBP also could not obtain the information needed to periodically review system internal access logs. Such reviews ensure system access to traveler information is restricted to DHS employees and contractors who have a legitimate need to have access to the information and ensure all parties complete annual privacy and security training prior to accessing the information. However, Office of Information and Technology specialists did not complete the internal access log review because they could not retrieve access logs from the systems that store traveler border crossing information.

Moreover, CBP's Privacy and Diversity Office did not complete the required privacy evaluation, because, according to a CBP official, the component prioritized a highly visible congressionally mandated initiative over completing the required privacy evaluation.

CBP also prioritized app security enhancements for making apps more secure at ports of entry over performing internal audits. In addition, CBP relied on the app developers to create the process to execute the required internal audit, but because the developers did not create such a process, CBP could not perform the required audits.

CBP's Management of System Configuration Was Inadequate

According to *DHS' Change 13.1.1 to Department of Homeland Security Sensitive Systems Policy Directive 4300A*, dated October 2, 2019, CBP is required to implement specific hardware and software configuration settings on computer servers to protect them from vulnerabilities. CBP is also required to implement configuration settings identified by DHS for each of the three DISA STIG categories. The STIGs are categorized based on the severity of the risk of the

¹¹ Servers should be stored in a locked room where physical access is controlled and monitored.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

setting failing — Category I, as most severe, to Category III, as least severe. Additionally, if CBP is unable to implement all configuration settings because a specific setting is an operational necessity, it may submit a waiver request to the Department.

CBP did not implement all required DHS configuration settings on servers supporting MPC operations. Specifically, as of July 2, 2020, CBP had not implemented 139 of the 236 required DISA STIG configuration settings tested on all 6 CBP servers supporting MPC operations. In addition, CBP did not have waivers for any of the non-compliant settings from the DHS Office of the Chief Information Security Officer. See Table 6 for DISA STIG control category testing results.

Table 6. DISA STIG Control Category Testing Results

Control Category	STIGs Tested	STIG Compliance	STIG Non-Compliance
Category I	29	25	4
Category II	193	69	124
Category III	14	3	11
Total	236	97	139

Source: DHS OIG analysis of testing it conducted on CBP servers

According to a CBP official, to comply with DHS policy, CBP only needed to implement the 29 Category I DISA STIG settings, which have the most operational impact if any of these settings are compromised. However, CBP did not implement 4 of the 29 Category I settings. After discussing our results with CBP, as of November 16, 2020, the component implemented one of the four non-compliant Category 1 settings and was working toward implementing the remaining three.

Further, according to a CBP official, the DHS Chief Information Security Officer Council allowed CBP to implement Categories II and III DISA STIG configuration settings using a phased-in approach. However, CBP could not provide documentation from the DHS Chief Information Security Officer Council verifying its deviation from the requirement or allowing CBP to use a phased-in approach.

Without CBP addressing the scan requirements to detect vulnerabilities, reviewing results to identify vulnerabilities, completing the security and privacy reviews, and implementing required configuration settings, CBP continues to place travelers' PII at risk for exploitation.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendations

Recommendation 1: We recommend the Executive Assistant Commissioner for the Office of Field Operations and Executive Assistant Commissioner for the Office of Enterprise Services collaborate and update the policies and procedures in *Mobile Passport Control Business Requirements* and *MPC Standard Operating Procedures* to ensure CBP scans all app update versions and that they are scanned prior to release by developers.

Recommendation 2: We recommend the Executive Assistant Commissioner for the Office of Field Operations and Executive Assistant Commissioner for the Office of Enterprise Services collaborate and update the policies and procedures in *Mobile Passport Control Business Requirements* and *MPC Standard Operating Procedures* to codify scan processes and define the roles and responsibilities necessary to ensure scans are complete as required, and that CBP Office of Information and Technology specialists review all Mobile Passport Control app scan results for vulnerabilities.

Recommendation 3: We recommend the Executive Assistant Commissioner for the Office of Field Operations and Executive Assistant Commissioner for the Office of Enterprise Services collaborate and update the policies and procedures in *Mobile Passport Control Business Requirements* and *Mobile Passport Control Standard Operating Procedures* to include processes to conduct required security and privacy compliance reviews on a specific schedule and timeframe, track reviews completed, and centrally store review documentation.

Recommendation 4: We recommend the Executive Assistant Commissioner for the Office of Field Operations and Executive Assistant Commissioner for the Office of Enterprise Services ensure the offices receive all necessary information from developers to complete the Requirements Traceability Matrix questionnaire and update the Requirements Traceability Matrix template to capture Mobile Passport Control-relevant information.

Recommendation 5: We recommend the Executive Assistant Commissioner for the Office of Enterprise Services develop a capability to review access logs, define the periodic review time frame, and perform the required reviews according to the defined time frame.

Recommendation 6: We recommend the Executive Director for the Privacy and Diversity Office complete the required privacy evaluation review.

Recommendation 7: We recommend the Executive Assistant Commissioner



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

for the Office of Field Operations in collaboration with the Office of Information and Technology and Privacy and Diversity Office update the policies and procedures in *Mobile Passport Control Business Requirements* and *Mobile Passport Control Standard Operating Procedures* to include developing a process to conduct internal audits and perform the required audits.

Recommendation 8: We recommend the Executive Assistant Commissioner for the Office of Enterprise Services adhere to DHS policy and fully implement the *Defense Information Systems Agency Security Technical Implementation Guide* control categories for the servers supporting the Mobile Passport Control program, request waivers as appropriate, or fully document any exception obtained from the Department when deviating from policy requirements.

CBP's Management Response and OIG Analysis

CBP concurred with all eight recommendations and provided comments to the draft report. CBP recognizes the need and intends to form a dedicated oversight team in fiscal year 2022 that will monitor and ensure all MPC applications comply with policy and regulations, including policies related to the protection of PII. We included a copy of CBP's management comments in its entirety in Appendix B. CBP also provided technical comments to our draft report and we made changes to incorporate these comments as appropriate.

All recommendations will remain open and resolved until CBP provides additional documentation to show that actions taken fully meet the intent of the recommendation(s).

CBP Response to Recommendation 1: Concur. CBP OFO [Office of Field Operations] will update the MPC Business Requirements to reflect the Enterprise Services, OIT [Office of Information Technology] policies regarding the scanning of applications and subsequent approval process governing the vendor's version release.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CBP provides MPC Business Requirements reflecting the updates.

CBP Response to Recommendation 2: Concur. CBP OFO and Enterprise Services OIT will collaborate to codify and define organizational roles and responsibilities necessary to ensure cybersecurity scans are completed by Enterprise Services OIT, as required by its policy. A signed memorandum will formalize each stakeholders' (OFO/OIT/Vendors) responsibilities, policies and



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

timelines associated with the scans. This information will be added to the MPC Business Requirements.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CBP provides updated MPC Business Requirements reflecting the updates.

CBP Response to Recommendation 3: Concur. CBP OFO and Enterprise Services OIT will collaborate on the development of its internal processes to: (1) conduct the required security and privacy compliance reviews on schedule; (2) track progress; and (3) store documentation. OFO will also support OIT's stakeholder engagement to facilitate the receipt of relevant security and privacy documentation.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CBP provides evidence of CBP OFO and Enterprise Services OIT's collaboration and its updated internal processes.

CBP Response to Recommendation 4: Concur. CBP OFO will support Enterprise Services OIT by facilitating requests for vendors to supply OIT with all information necessary to complete, review the RTM questionnaires, and update the RTM templates. OFO will draft templates for stakeholders' engagement. Business sponsors and vendor profiles will be created to identify the proper points of contact, addresses, and related information.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CBP provides evidence of the updated RTM template, business sponsor and vendor profiles, and the implemented changes provide the offices with the necessary information to complete the RTM questionnaire.

CBP Response to Recommendation 5: Concur. CBP Enterprise Services OIT will work with the current vendors to identify a process for reviewing logs on a regular basis.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CBP provides evidence of a completed internal access log review, and its review process, including a defined review timeframe.

CBP Response to Recommendation 6: Concur. CBP Privacy and Diversity Office will conduct a Privacy Evaluation of the MPC program's current



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

operations, with a focus on how data is collected, used, and shared between the agency and application development partners. The review will include an assessment of the program's established Privacy Compliance documentation, program policies, and operating procedures that support the use of this technology.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CBP provides evidence of a completed privacy evaluation review.

CBP Response to Recommendation 7: Concur. CBP OFO will collaborate with the Privacy and Diversity Office and Enterprise Services OIT to update internal documents that describe an internal process to perform the required audits. In addition, OFO will assign personnel to support Enterprise Services OIT's dedicated audit team and will provide documentation of this process.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CBP provides evidence of internal documents detailing the internal audit process and completion of the internal audits.

CBP Response to Recommendation 8: Concur. CBP Enterprise Services OIT will work to implement the DISA STIG control categories for the servers supporting the MPC program.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CBP provides evidence supporting the full implementation of the DISA STIG control categories for the servers supporting the MPC program, including any waivers or exceptions obtained from the Department when deviating from policy requirements.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

Our objective was to determine to what extent CBP protects its MPC apps from cybersecurity threats. To accomplish our objective, we reviewed Federal laws and regulations related to securing mobile apps and CBP internal control processes, policies, procedures, and guidance associated with MPC apps.

We also reviewed and analyzed applicable Federal requirements regarding management's responsibility for internal controls. We assessed the design of these internal controls, as well as CBP's implementation and operating effectiveness. We identified internal control deficiencies that could affect CBP's ability to effectively and efficiently ensure MPC apps are secure from cybersecurity threats. We discussed these internal control deficiencies in the body of the report. However, because we limited our review to internal controls regarding CBP's processes to secure MPC apps from cybersecurity threats, we may not have identified all internal control deficiencies.

We conducted interviews with CBP personnel from the Office of Field Operations, Office of Information and Technology, Privacy and Diversity Office, three U.S. airports of entry and two seaports of entry, and the DHS Office of the Chief Information Officer. Additionally, we conducted interviews with MPC app developers. We conducted our interviews remotely using available technology due to the ongoing COVID-19 pandemic.

We interviewed the DHS Office of the Chief Information Officer and reviewed CBP's Mobile App Security Review compliance review documentation, including AppVet scan summary and service reports. In addition, we requested that the DHS Office of the Chief Information Officer perform AppVet scans on the six MPC apps available for traveler use on May 13, 2020, and November 5, 2020. We reviewed the AppVet scan summary and service reports from the scans. In total, we reviewed AppVet scan results for 26 MPC app versions, which included 136 AppVet summary and service reports.

We tested the reliability of the data we obtained from the DHS Office of the Chief Information Officer for MPC app AppVet scans initiated by CBP from January 2016 through December 2019 and our scans conducted on May 13, 2020, and November 5, 2020, by comparing key data elements with information that CBP's Office of Field Operations verified. Specifically, we



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

traced scan dates to and from source documentation provided by the DHS Office of the Chief Information Officer. We determined the data were sufficiently reliable for the purposes of our audit.

We observed virtually CBP conduct technical testing of six CBP TECS Red Hat Enterprise Linux 7 servers. We analyzed testing results to assess CBP's configuration management program and determine the effectiveness of configuration setting implementation. This security testing provided CBP and us with an assessment of their security configuration compliance to applicable *Defense Information Systems Agency Security Technical Implementation Guide* configuration management security settings.

We conducted this performance audit between March 2020 and April 2021 pursuant to the *Inspector General Act of 1978, as amended*, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
CBP Comments to the Draft Report

1300 Pennsylvania Avenue, NW
Washington, DC 20229

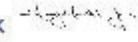


**U.S. Customs and
Border Protection**

June 22, 2021

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Henry A. Moak, Jr.
Senior Component Accountable Official
U.S. Customs and Border Protection

X 
Signed by: HENRY A. MOAK JR.

6/22/2021

SUBJECT: Management Response to Draft Report: "CBP Has Placed
Travelers' PII at Risk of Exploitation"
(Project No. 20-007-AUD-CBP)

Thank you for the opportunity to comment on this draft report. U.S. Customs and Border Protection (CBP) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

As one of the world's largest law enforcement organizations charged with keeping terrorists and their weapons out of the U.S., while also facilitating lawful international travel and trade, CBP is pleased the OIG report notes that CBP continues to modernize efforts to streamline the inspection process, increase CBP officer efficiency, and reduce operating costs to provide enhanced services for travelers entering the United States.

In support of our mission, CBP engaged with non-governmental entities in the development of commercial market based Mobile Passport Control (MPC) applications to expedite travelers through the primary inspection process, as the MPC application provides a more efficient in-person inspection between the CBP officer and the traveler. Since the administrative tasks are performed by the traveler prior to the passport control inspection, MPC reduces passport control inspection time and overall wait times.

Third-party developers (i.e., vendors) created, maintain, and operate the MPC applications, which transmit travelers' personally identifiable information (PII) prior to arrival at participating ports of entry. While the security of these applications is ultimately the responsibility of the vendors, CBP recognizes the need for dedicated oversight efforts to continue operations and ensure compliance with security policy and regulations. The CBP Offices of Information and Technology (OIT), Field Operations



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

(OFO); and the Privacy and Diversity Office (PDO) will collaborate to form a dedicated oversight team in fiscal year 2022 that will monitor and ensure all MPC applications comply with policy and regulations, including policies related to protection of PII.

The draft report contained eight recommendations, with which CBP concurs. Attached find our detailed response to each recommendation. CBP previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

**Attachment: Management Response to Recommendations
Contained in Project No. 20-007-AUD-CBP**

OIG recommended that the Executive Assistant Commissioners (EAC) for OFO and Enterprise Services (ES):

Recommendation 1: Collaborate and update the policies and procedures in *Mobile Passport Control Business Requirements* and *MPC Standard Operating Procedures* to ensure CBP scans all app update versions and that they are scanned prior to release by developers.

Response: Concur. CBP OFO will update the MPC Business Requirements Document (BRD) to reflect the ES, OIT policies regarding the scanning of applications and subsequent approval process governing the vendor's version release. Estimated Completion Date (ECD): September 30, 2021.

Recommendation 2: Collaborate and update the policies and procedures in *Mobile Passport Control Business Requirements* and *MPC Standard Operating Procedures* to codify scan processes and define the roles and responsibilities necessary to ensure scans are complete as required, and that CBP Office of Information Technology specialists review all Mobile Passport Control app scan results for vulnerabilities.

Response: Concur. CBP OFO and ES OIT will collaborate to codify and define organizational roles and responsibilities necessary to ensure cybersecurity scans are completed by ES OIT, as required by ES OIT policy. A signed memorandum will formalize each stakeholders' (OFO/OIT/Vendors) responsibilities, policies and timelines associated with the scans. This information will be added to the MPC BRD. ECD: December 31, 2021.

Recommendation 3: Update the policies and procedures in *Mobile Passport Control Business Requirements* and *Mobile Passport Control Standard Operating Procedures* to include processes to conduct required security and privacy compliance reviews on a specific schedule and timeframe, track reviews completed, and centrally store review documentation.

Response: Concur. CBP OFO and ES OIT will collaborate in the development of ES OIT's internal processes to: (1) conduct the required security and privacy compliance reviews on schedule; (2) track progress; and (3) store documentation. OFO will also support OIT in stakeholder's engagement in order to facilitate the receipt of relevant security and privacy documentation. ECD: December 31, 2021.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

OIG recommended that the EAC for the OFO:

Recommendation 4: Ensure the office receives all necessary information from developers to complete the Requirements Traceability Matrix [RTM] questionnaire and update the Requirements Traceability Matrix template to capture Mobile Passport Control-relevant information.

Response: Concur. CBP OFO will support ES OIT by facilitating requests for vendors to supply OIT with all information necessary to complete, and review, the RTM questionnaires and update the RTM templates, as appropriate. OFO will draft templates for stakeholder's engagement. Business sponsors and vendor profiles will be created in order to identify the proper points of contact, addresses and related information. ECD: December 31, 2021.

OIG recommended that the EAC for ES:

Recommendation 5: Develop a capability to review access logs, define the periodic review time frame, and perform the required reviews according to the defined time frame.

Response: Concur. CBP ES OIT will work with the current vendors to identify a process for reviewing logs on a regular basis. ECD: December 31, 2021.

OIG recommended that the Executive Director for the Privacy and Diversity Office:

Recommendation 6: Complete the required privacy evaluation review.

Response: Concur. CBP PDO will conduct a Privacy Evaluation of the MPC program's current operations, with a focus on how data is collected, used, and shared between the agency and our application development partners. The review will include an assessment of the program's established Privacy Compliance documentation, program policies, and operating procedures that support the use of this technology. ECD: June 30, 2022.

OIG recommended that the EAC for OFO, in collaboration with the OIT and PDO:

Recommendation 7: Update the policies and procedures in *Mobile Passport Control Business Requirements* and *Mobile Passport Control Standard Operating Procedures* to include developing a process to conduct internal audits and perform the required audits.

Response: Concur. CBP OFO will collaborate with PDO and ES OIT to update internal documents that describe an internal process to perform the required audits. In addition, OFO will assign personnel to support ES OIT's dedicated audit team and will provide documentation of this process. ECD: December 31, 2021.

OIG recommended that the EAC for ES:



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 8: Adhere to DHS policy and fully implement the *Defense Information Systems Agency Security Technical Implementation Guide* control categories for the servers supporting the Mobile Passport Control program, request waivers as appropriate, or fully document any exception obtained from the Department when deviating from policy requirements.

Response: Concur. CBP ES OIT will work to implement the Defense Information Systems Agency Security Technical Implementation Guide control categories for the servers supporting the MPC program. ECD: December 31, 2021.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Commissioner of CBP
Audit Liaison, CBP

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at:
www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General
Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.



OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305