Privacy Compliance Review of the U.S. Customs and Border Protection Southwest Border Pedestrian Exit Field Test

December 30, 2016

Contact Points
Kim A. Mills
Entry-Exit Transformation Office
Office of Field Operations
U.S. Customs & Border Protection
U.S. Department of Homeland Security
(202) 344-3007

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Table of Contents

I. Background

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) conducted the Southwest Border Pedestrian Exit Field Test (Test) to determine whether the collection of biometric information, including facial and iris images, from visitors exiting the United States enhances CBP exit operations with acceptable impacts to the public's travel experience and border processing times. Specifically, this Test evaluated whether the processes and technologies used to collect biometric information would enable CBP to more effectively identify individuals who have overstayed their period of admission, identify individuals who pose or are suspected of posing a law enforcement or national security threat, and improve CBP reporting and analysis of all travelers entering and exiting the United States.

CBP issued a Privacy Impact Assessment[1] (PIA) for this Test on November 6, 2015. Due to the novel technologies and heightened privacy risks involved with the collection of biometrics, particularly with untested biometric modalities, the PIA required the DHS Privacy Office to conduct a Privacy Compliance Review (PCR) at the conclusion of the Test. This PCR is designed to evaluate how the information collected during the Test was used, retained, and destroyed. In keeping with the Test goals of providing an operational feasibility assessment for potential future deployment, the recommendations of this PCR are also intended to provide CBP with best practices and an initial privacy compliance framework for potential future deployments of biometric collection technologies and processes. Additional privacy protections may be required for future biometrics collection programs, as future programs may utilize different technologies or processes that raise additional privacy concerns.

This PCR will be conducted in two parts. The first part focuses on the Fair Information Practice Principles[2] (FIPPs) and addresses how collected information was managed in the standalone database, the use limitations of the information, and how collected information remains separated from other DHS operations. The second part of this PCR will be conducted in June 2017, in accordance with the PIA instruction to assess compliance with the one-year data retention and destruction requirements required after the Test's completion.

CBP has the authority to collect and review certain Border Crossing Information (BCI) from the identity and travel documents that individuals present to CBP when entering or exiting the United States[3]. BCI includes traveler biographic and biometric information and border crossing information such as location, date, and time of admission to or exit from the United States. Generally, CBP collects this information from certain inbound and outbound travelers to determine their admissibility into the United States, whether they have overstayed their period of admission, or whether they pose or are suspected of posing a law enforcement or national security threat.

---

[1] https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-swborderpedestrianexit-november2015.pdf.
[2] Privacy Policy Guidance Memorandum Number: 2008-01/Privacy Policy Directive 140-06, https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[3] U.S. Customs and Border Protection-007 Border Crossing Information System of Records Notice *found at* https://www.regulations.gov/document?D=DHS-2016-0006-0001.

Any biometric data collected as part of this Test was stored in a secure standalone database. CBP made no operational decisions based on the collected biometric data. Rather, the Test results will provide CBP with an operational feasibility assessment report that may lead to the potential deployment of this program or similar programs across the Southwest Border and other Ports of Entry (POE). CBP chose to conduct this Test at the Otay Mesa land POE due to the high volume of pedestrians who enter and exit the United States at that facility.

Scope and Methodology

On July 11, 2016, the DHS Privacy Office launched its PCR of the Southwest Border Pedestrian Exit Field Test by developing and administering a questionnaire to the program, which covered operations from December 10, 2015 (the Test's start date) to July 11, 2016 (the date of the PCR memo). As part of completing this PCR, the DHS Privacy Office reviewed privacy compliance and usage documentation; developed an extensive questionnaire, reviewed all responses to the questionnaire, and provided follow-up questions to the Test program office; reviewed training and governance documents; and conducted site visits with, and received briefings from, Test program and privacy personnel.

The DHS Privacy Office commends CBP and the Test program team for its careful stewardship of this program and for its adherence to privacy protections cited in the PIA.

The PCR was conducted in coordination with CBP's Office of Field Operations (OFO), the CBP Privacy Office, and the CBP Office of Information and Technology (OIT). To assess overall compliance with the existing PIA, the DHS Privacy Office carried out the following activities:

- Reviewed the November 2015 PIA and 2016 Border Crossing Information System of Records Notice update;
- Developed and administered a questionnaire to determine compliance with the PIA and with DHS FIPPs in July 2016;
- Reviewed all responses to the questionnaire and provided follow-up questions to the Test program team in August 2016;
- Conducted a site visit and received a briefing from the Test program team in September 2016;
- Reviewed Test deployment documents; and
- Reviewed Test Standard Operating Procedures (SOP) and Concept of Operations[4] (CONOPS).

The 2016 PCR assessed implementation of privacy protections stated within the 2015 PIA and considered program activities against the DHS FIPPs, which serve as Department policy for analyzing all DHS programs. This report discusses the DHS Privacy Office's review of the Test

[4] CONOPS marked FOUO, Not for Public Distribution.

against these requirements and our recommendations of best practices for potential future biometric information collections.

II. Findings

A. Summary

The DHS Privacy Office finds that CBP managed this Test with privacy-protective objectives, and with sensitivity to privacy and data aggregation risks. The DHS Privacy Office recommends that CBP consider the following 10 best practices for any future biometric exit tests to further improve its ability to demonstrate compliance with privacy requirements:

Recommendation 1: CBP should create an annual auditable process to ensure users requesting access to the information continue to meet the role-based criteria and continue to have a need-to-know in order to access the information.

Recommendation 2: CBP should provide sufficient notification to travelers prior to and upon entry that biometric collections will take place during both entry and exit. Such notification could be provided through bilingual mediums similar to those employed during the Test, including the Fact Sheet, Tear Sheet, awareness signage, and CBP's website. CBP should also provide sufficient notification of when biometric collections at departure will be made mandatory.

Recommendation 3: In the event that CBP operationalizes biometric collection upon exit, CBP should carefully review and articulate its relevant authorities given that 8 CFR 215.8(a)(1) authorizes only "pilot programs."

Recommendation 4: If CBP cannot demonstrate that exit operations or the match rate are significantly better than using existing biographic information, CBP should consider an alternate process for collecting biometrics.

Recommendation 5: CBP should ensure that both physical and electronic processes, as well as Officer training conducted to promote the data quality and integrity of biometric records, align with similar processes designed to protect biographic information. In addition, CBP should ensure that information on all exemptions is kept current.

Recommendation 6: If CBP continues the practice of duplicating biographic information to match biometric information, CBP should ensure that appropriate access, use limitation, and data retention protocols are linked to the copied information.

Recommendation 7: A mechanism should be created, in addition to OIT's oversight, to alert the core management team of any unauthorized access, use, or other suspicious activity.

Recommendation 8: If CBP decides to share any information from this Test or any future biometrics collection programs with DHS Office of Biometric Information Management (OBIM), DHS Science and Technology Directorate (S&T), or any other entity, CBP should enter into a written agreement with the entity in question that spells out how each office will appropriately protect the information. Such an information sharing agreement would be subject to DHS Privacy Office oversight and possible review.

Recommendation 9: CBP should build in an audit mechanism to ensure no inappropriate access or use of biographic and biometric information.

Recommendation 10: CBP should consider requiring program-specific privacy training as a prerequisite to access.

Below is a discussion of each FIPP requirement, how the DHS Privacy Office reviewed the Test for compliance, our findings, and our specific recommendations to CBP in response to these findings.

B. Use Limitation

Requirement: The Use Limitation FIPP requires that Personally Identifiable Information (PII) be used solely for the purpose(s) specified in notice documentation. This can be analyzed for compliance by the types of users authorized to use the PII for official purposes.

The 2015 Test PIA identifies the "Field Test team" as those with authorized access to the data. Responses to the PCR questionnaire explain that the Test employs role-based access wherein access to Test data is limited to pre-approved personnel with privileged user/Administrator accounts via Personal Identity Verification (PIV) card. Only eight authorized personnel designated by the program manager had access to the Test data. These personnel included Test team users, authorized program management officials, and select CBP OIT personnel. OIT holds the system administrator role and maintains access control in accordance with existing departmental and DHS processes and policy. For future biometrics collections, careful consideration should be taken to minimize the number of users with access to the system by ensuring that all authorized users individually have a need-to-know the information.

The biometrics collected in this Test were stored in a standalone database at CBP's National Data Center and were not run against existing government databases for law enforcement purposes. Consistent with the CONOPS and PIA, the collected biometrics were used to evaluate the ability to match those from a given traveler upon entry with the biometrics collected when that traveler departed the country. This match would enable CBP to verify the identity of an individual using a travel document. Biographic data was used in the Test to determine potential overstays and persons of law enforcement interest.

User Account Audits

As previously stated, the Test employed role-based access to which access to Test data is limited to pre-approved personnel with privileged user/Administrator accounts via PIV card. Only authorized personnel designated by the program manager may access the data, and users cannot modify data. CBP should continue to employ role-based access requirements and audit the continued need-to-know for authorized users.

Review: The DHS Privacy Office reviewed questionnaire responses and the November 2015 CONOPS regarding authorized users. CBP also provided the DHS Privacy Office with additional explanations about authorized users from the Test team and biometric/biographic collection during a September 2016 on-site demonstration.

Findings: During the Test, there were eight authorized users of Test data, who were defined by the specific role they played in the Test and who also possessed a legitimate need-to-know. For a user to receive access, a service request is submitted through CBP OIT, with approval granted if the user holds an existing privileged account.

> *Recommendation 1*: CBP should create an annual auditable process to ensure users requesting access to the information continue to meet the role-based criteria and continue to have a need-to-know in order to access the information.

C. Transparency

Requirement: The DHS Transparency FIPP states that DHS should provide notice to an individual when it collects, uses, disseminates, and/or maintains that person's PII. The Test PIA and relevant SORN are posted on the DHS website.

Review: We reviewed publicly available documents that described and discussed the privacy impact of the Test. In addition to the 2015 Test PIA, we reviewed copies of the Test's bilingual Fact Sheet, bilingual Tear Sheet, bilingual awareness signage, and November 2015 Federal Register Notice. CBP met with Mexican and Californian government officials and held public press events at the Otay Mesa Port of Entry to discuss the rationale behind CBP's biometrics collection and the new procedures before biometric entry and biometric exit collections began. On-site attendants were available during the Test to address any questions or concerns from the traveling public.

Findings: CBP initiated a thoughtful outreach campaign to raise the traveling public's awareness as well as that of Mexican and Californian government leaders. Sufficient printed information and on-site assistance was provided to explain the new technologies, processing procedures, and redress options. These efforts proved valuable, so scaling such efforts is likely to ensure continued positive reception. CBP's Customer Service Information Center received no complaints and there were no DHS Traveler Redress Inquiry Program requests submitted during the Test period.

D. Individual Participation

Requirement: The DHS Individual Participation FIPP states that when possible, DHS should seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Review: We reviewed the Test Fact Sheet and Tear Sheet that provide travelers with additional information on the Test's procedures and options for access, correction, and redress. We also reviewed the Test's SOPs that provide instructions to Officers on how to handle travelers that do not wish to participate. Additionally, we requested access to all Freedom of Information Act (FOIA)[5] or Privacy Act requests, as well as all DHS responses.

Findings: The 2015 Test PIA states that "For information available in standard CBP law enforcement systems used to inspect and admit travelers into the United States, DHS allows persons, including foreign nationals, to seek access under the Privacy Act and the Freedom of Information Act." No information collected during the Test became part of a case file for a law enforcement investigation or an encounter. There were no Privacy Act or FOIA requests or DHS Traveler Redress Inquiry Program submissions during the review period.

While there were no redress inquiries during the Test or review periods, CBP has a process in place to provide access and redress and includes instructions in its public documents. While the Secretary of Homeland Security has exempted certain Border Crossing Information (BCI) from the notification, access, and amendment procedures of the Privacy Act, the BCI Systems of Records Notice states that CBP "will consider individual requests to determine whether or not information may be released." The DHS Privacy Office strongly encourages CBP to provide access and redress to the greatest extent possible.

CBP has the authority to collect BCI from all individuals entering and exiting the United States, including from U.S. citizens.[6] Entry into the United States may be regarded as giving constructive consent to biometric collection upon exit: if a traveler does not consent to the collection of biometrics upon exit, then the alternative is to not enter in the first place. The Test demonstrated why sufficient notice is necessary to allow for genuine individual consent, especially as it applies to, for instance, U.S. citizens departing the country for the first time, since constructive consent upon entry would not apply. For those travelers not wishing to participate, Test SOPs instructed POE Officers to allow these individuals the option of exiting via the San Ysidro POE. However, that option does not seem reasonable to pedestrian travelers without sufficient advance notice since the San Ysidro POE is approximately 10 miles away. Given the

[5] 5 U.S.C. § 552.
[6] Immigration and Naturalization Act, Section 215(b) "Citizens: Except as otherwise provided by the President and subject to such limitations and exceptions as the President may authorize and prescribe, it shall be unlawful for any citizen of the United States to depart from or enter, or attempt to depart from or enter, the United States unless he bears a valid United States passport."

even higher consequences of non-participation if biometric collections were to be operationalized at additional or all POEs, sufficient advance notice of changes in exit-based biometric collection policies is necessary to allow for meaningful individual consent.

> *Recommendation 2*: CBP should provide sufficient notification to travelers prior to and upon entry that biometric collections will take place during both entry and exit. Such notification could be provided through bilingual mediums similar to those employed during the Test, including the Fact Sheet, Tear Sheet, awareness signage, and CBP's website. CBP should also provide sufficient notification of when biometric collections at departure will be made mandatory.

E. Purpose Specification

Requirement: The DHS Purpose Specification FIPP requires DHS to specifically articulate the authority that permits the collection of PII and the purpose (or purposes) for which the PII is intended to be used for all programs.

Under CBP's authorities[7] to collect information at the border, the Test's purpose was to evaluate the feasibility of using biographic and biometric data in an operational border environment to enhance CBP entry and exit operations with acceptable impacts to the traveling public and processing times, while providing CBP Officers with tools to identify travelers that pose or are suspected of posing law enforcement or national security threats. CBP used biometric information collected upon entry and exit to evaluate the quality of the data collection in a non-real time manner to assess the ability to use the data for identity purposes and to support CBP's mission. The Test was not designed to use the collected data for predictive pattern or anomaly analysis, or like analyses. Biometric data collected during the Test was not used to make operational decisions at the POE. On-site Officers and Agents were not presented biometric data and did not receive the results of biometric operations.

Review: We reviewed responses to the PCR questionnaire and interviewed CBP Entry/Exit Transformation (EXT) officials.

Findings: The DHS Privacy Office found that CBP specifically articulated the authorities allowing it to collect biometrics at the border by citing to 8 CFR 215.8. However, although 8 CFR 215.8(a)(1) provides the regulatory authority for this Test, the regulatory language allows for only "pilot programs at land border ports of entry, and at up to fifteen air or sea ports of entry border authorities." Any operational expansion of this program across the Southwest Border or to other land/air/sea POEs would require a careful review and re-articulation of relevant authorities,

[7] 8 CFR 215.8 - Requirements for biometric identifiers from aliens on departure from the United States; Enhanced Border Security and Visa Entry Reform Act of 2002 (Pub. L. 107-173, 116 Stat. 543 (2002)); the Aviation and Transportation Security Act of 2001 (Pub. L. 107-71, 115 Stat. 597); the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458, 118 Stat. 3638 (2004)); the Immigration and Nationality Act, as amended (8 U.S.C. §§ 1185 and 1354); and the Tariff Act of 1930, as amended (19 U.S.C. §§ 1322-1683g, including 19 U.S.C. §§ 66, 1433, 1454, 1485, 1624 and 2071).

as a full-fledged operational deployment of biometrics collection programs would no longer be considered a "pilot program".

Recommendation 3: In the event that CBP operationalizes biometric collection upon exit, CBP should carefully review and articulate its relevant authorities given that 8 CFR 215.8(a)(1) authorizes only "pilot programs."

F. Data Minimization

Requirement: The DHS Data Minimization FIPP requires DHS to only collect PII that is directly relevant and necessary to accomplish the specified purpose(s), and only retain PII for as long as it is necessary to fulfill the specified purpose(s) of all programs.

Data Subjects

CBP confirmed steps were taken to ensure biometrics were only taken from non-U.S. Citizens and non-exempt aliens[8]. Officers stationed at the POE directed travelers through the POE depending on what travel document was presented. Travel documents were electronically scanned to determine which travelers were exempted and what biographic information CBP was authorized to collect. Biographic, but not biometric, information was collected from U.S. Citizens and exempted travelers.

Biometric Collection

The PIA notes one purpose of the Test was to determine if biometric collection, coupled with biographic data collection, enhances CBP exit operations in various modalities and with acceptable impacts to the public's travel experience and border processing times. At the time of our review, analysis was underway to determine whether this objective was met. The DHS Privacy Office notes that if there is no material improvement in exit operations and CBP mission needs, CBP should consider an alternate process for collecting biometrics. CBP should also consult with other stakeholders to respect cultural sensitivities in collecting biometrics while meeting the program's objectives.

Retention

DHS Privacy will evaluate CBP's data retention and deletion practices after July 2017, one year following completion of the Test as required.

Review: To assess compliance with the data minimization requirements, we reviewed PCR questionnaire responses; met with CBP program, privacy, and disclosure officials; and received a demonstration of the POE screening process.

[8] Exempted aliens are those travelers exempted under paragraph (a)(2) of 8 CFR Part 215.8 and Canadian citizens under Section 101(a)(15)(B) of the Immigration and Nationality Act who are not otherwise required to present a visa or have been issued Form I-94 or Form I-95 upon arrival into the United States.

Findings: CBP effectively implemented the process to limit biometric data collection to non-U.S. Citizens and non-exempt aliens during the Test. Officer and technical reviews ensured only the minimum amount of data necessary to complete the task was collected.

> *Recommendation 4:* If CBP cannot demonstrate that exit operations or the match rate are significantly better than using existing biographic information, CBP should consider an alternate process for collecting biometrics.

G. Data Quality and Integrity

Requirements: The DHS Data Quality and Integrity FIPP requires that DHS, to the extent practicable, ensures that PII is accurate, relevant, timely, and complete.

The primary purpose of the Test was to assess new technologies and processes to "provide assurance of traveler identity on departure." Specifically, the collection of biometrics information was intended to help CBP accurately verify the identity of travelers and help close any biographic gaps in the pedestrian exit process. CBP intended to evaluate the accuracy of the collected biometric exit data maintained in a secure standalone database environment by matching it against the individual's previously obtained biometric entry data.

To that end, CBP has built data quality and integrity into the Test's operations. The 2015 PIA and the Test SOPs stated that an Officer reviews a traveler's documents for accuracy at the time of collection during inbound and outbound processing. A traveler cannot advance from one step to the next until cleared by the kiosk and the Officer has received the required information to properly process the traveler. Only non-U.S. citizens and non-exempt aliens had their biometrics collected upon exit. Supporting documents also described procedures to acquire quality biometrics. If any information appears inconsistent during processing, the Officer may refer the traveler for secondary screening to clarify or resolve the inconsistency. If there were discrepancies between the biometrics collected and biographic data, the Officer followed current CBP/DHS processes for mitigating those discrepancies. CBP further ensures accuracy by not co-mingling the biometric data in the standalone database with BCI or other information not associated with the Test population.

These procedures were demonstrated during the site visit.

Erroneous Information – Biometric v. Biographic

Because biometric data was not presented to the CBP Officer or Border Patrol Agent during the Test, no operational decisions were taken based on what may have been erroneous information. Officers and Agents were operationally unaware of the biometric process and subsequent results.

If there were discrepancies with biographic data, Officers and Agents would follow their training and existing CBP processes for resolution consistent with current inbound and outbound processing at POEs.

Review: We reviewed responses to the Test questionnaire (including the CONOPS and SOPs), interviewed representatives from OFO and OIT, and received a demonstration of the equipment used at the POE and what information an Officer or Agent would have access to at the POE.

Findings: We find that CBP has employed tools and technical controls to maintain a high level of data quality and integrity within the system, and that the CONOPS and SOPs are comprehensive.

> *Recommendation 5:* CBP should ensure that both physical and electronic processes, as well as Officer training conducted to promote the data quality and integrity of biometric records, align with similar processes designed to protect biographic information. In addition, CBP should ensure that information on all exemptions is kept current.

H. Security

Requirements: The DHS Security FIPP requires DHS to protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The most important security step taken during the Test is the fact that CBP stored the biometric data in a secure standalone database environment that was not connected to any other DHS system or network. During our interviews, CBP explained that the Test database is encrypted and stored in a secure area of the CBP space within DHS data centers. Access is limited to approved personnel with privileged user/Administrator accounts via PIV cards. CBP stored the biometric data collected during the Test in this secure standalone database and processed the remaining biographic information through appropriate procedures in TECS.[9] As part of the Test, CBP also stored a copy of biographic BCI matched to the corresponding collected biometric information in the standalone database. The same use limitation and data retention requirements apply to this copy. No residual PII is stored on any hardware located at the POE. The Test operated within the TECS enterprise architecture and security boundary under an approved Authority to Operate and System Security Plan.

The 2015 PIA stated that when the Test was complete, CBP would share the Test biometric data maintained in the standalone database with the DHS Office of Biometric Information Management (OBIM) and DHS Science and Technology Directorate (S&T) to support development of iris and facial algorithms associated with an initiative aimed at expanding

[9] Not an acronym. The TECS Platform facilitates information sharing among federal, state, local, and tribal government agencies, as well as with international governments and commercial organizations. https://www.dhs.gov/publication/dhscbppia-021-tecs-system-platform

biometric processing capabilities. However, during our review, CBP confirmed no Test data was shared with OBIM or S&T.

Review: We reviewed responses to the Test questionnaire (including the CONOPS and SOPs), interviewed representatives from EXT, OFO, and OIT, and received a demonstration of how information is stored and used in the standalone database.

Findings: CBP has taken the necessary steps to prevent the loss, unauthorized use, and inappropriate disclosure of information.

Recommendation 6: If CBP continues the practice of duplicating biographic information to match biometric information, CBP should ensure that appropriate access, use limitation, and data retention protocols are linked to the copied information.

Recommendation 7: A mechanism should be created, in addition to OIT's oversight, to alert the core management team of any unauthorized access, use, or other suspicious activity.

Recommendation 8: If CBP decides to share any information from this Test or any future biometrics collection programs with DHS Office of Biometric Information Management (OBIM), DHS Science and Technology Directorate (S&T), or any other entity, CBP should enter into a written agreement with the entity in question that spells out how each office will appropriately protect the information. Such an information sharing agreement would be subject to DHS Privacy Office oversight and possible review.

I. Accountability and Auditing

Requirements: The Accountability and Auditing FIPP holds DHS accountable for complying with the other privacy principles previously noted, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

CBP provided specific project implementation and control training to Officers at the POE, IT employees, and others, including information on the inbound and outbound processes as well as the appropriate use of handheld devices to collect fingerprints. Because Officers did not have access to biometrics collected during this Test, no additional training was provided on this topic. CBP demonstrated steps taken to conduct a careful analysis and evaluation of the effectiveness of the Test, its impact on traveler throughput, and its operational impact. While annual privacy training on the appropriate protection of PII is required of all DHS employees, there was no program-specific privacy training offered in connection with this Test. If biometric exit collection programs are expanded beyond this initial Test, CBP should consider creating and implementing program-specific privacy training for any and all personnel involved with the operation.

Suspicious Events and Auditable User Activity Logs

Standard CBP services for operations and maintenance of the standalone database were in place during the Test, which includes standard database monitoring for any suspicious events. Numerous audits were conducted to monitor activity and troubleshoot any issues with the operation of the kiosks.

While the 2015 PIA states that the "Test team maintains audit trails and or logs and reviews all user activity," audits were not conducted on individual user activity during the Test. While the pool of authorized users was very small during this Test, CBP should consider implementing technological mechanisms to notify appropriate management staff of any suspicious events, including inappropriate access or changes in a user's access privileges, and regularly review user access authorizations to determine a continued need to know.

Review: To assess compliance with auditing and accountability controls, we reviewed responses to the Test questionnaire, reviewed training documents, and interviewed EXT and OIT staff on the system's auditing capabilities.

Findings: We find that CBP has robust audits to review the operational impact of the Test, but cannot determine whether there are adequate auditing and accountability controls on the appropriate use of PII.

> *Recommendation 9*: CBP should build in an audit mechanism to ensure no inappropriate access or use of biographic and biometric information.
>
> *Recommendation 10*: CBP should consider requiring program-specific privacy training as a prerequisite to access.

III. Conclusion

The DHS Privacy Office commends CBP for taking serious steps to protect the biometric information collected at the Otay Mesa, California, Port of Entry. The careful stewardship of collected information exhibited during this Test should be emulated in similar projects going forward. Protective and appropriate use measures should be fully embedded within any expansion of this Test or the operationalization of any other biometric collection technologies or procedures, or if CBP shares any information from this Test or any future biometrics collection programs with other entities. The recommendations of this PCR are intended to provide CBP with best practices and an initial privacy compliance framework for any potential future biometric programs derived from this Test or any other biometric collection technologies or processes. Additional privacy protections may be required for future biometrics collection programs, as future programs may utilize different technologies or processes that raise additional privacy concerns.

We discussed these 10 recommendations with EXT program officials, CBP Privacy Office staff, and the DHS Privacy Office Compliance Team. The DHS Privacy Office looks forward to working with CBP in 2017 to review Test data retention practices as part of the second half of this PCR, and providing any and all necessary support for the implementation of these recommendations in this or other biometric collection programs.

IV. Privacy Compliance Review Approval

Responsible Official

Kim A. Mills
Entry-Exit Transformation Office
Office of Field Operations
US Customs & Border Protection

Approval Signature

Original on file at Privacy Office

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security