Privacy Impact Assessment
for the

Trusted Worker Program System (TWP)

DHS/CBP/PIA-062

January 24, 2020

Contact Point
John R. Maulella
Office of Field Operations (OFO)
U.S. Customs and Border Protection (CBP)
(202) 344-2605

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

Abstract

The U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is responsible for vetting and monitoring the eligibility of workers applying for access to sensitive CBP-controlled areas or positions. CBP uses the Trusted Worker Program System (TWP), which is a subsystem of the e-Business cloud and is hosted on the CBP Amazon Web Services (AWS) Cloud East (CACE), to facilitate enrollment and vetting of applicants for eBadge, Bonded Worker, and Broker's License. In 2019, CBP migrated the data and vetting of trusted workers from the Global Enrollment System (GES) Trusted Worker (TW) to TWP. CBP has developed this overarching Privacy Impact Assessment (PIA) to: (1) document the creation of a new privacy sensitive system, TWP, (2) and provide notice of a web-service interface data exchange mechanism between CBP and the Transportation Security Administration (TSA) Transportation Vetting System (TVS) for the eBadge program.

Overview

CBP is responsible for vetting and monitoring the eligibility of workers applying for access to sensitive CBP-controlled areas or positions. CBP created TWP as the primary repository for program enrollment and background investigation data related to Trusted Worker programs. CBP has three trusted worker programs: (1) eBadge, which is responsible for vetting and credentialing third party workers who have access to secure areas at CBP facilities such as domestic airports and foreign preclearance facilities;[1] (2) Bonded Worker, which is responsible for vetting individuals associated with bonded warehouses; and (3) Broker's License, which is responsible for vetting applicants for a Broker's License. TWP provides CBP with the ability to centralize many of the program applications and enrollment functions, standardize the risk assessment process for programs, and offer a more efficient approach in the administration of these programs. Previously, the Global Enrollment System housed all information related to the trusted worker population.[2]

CBP has developed this overarching PIA to: (1) document the creation of a new privacy sensitive system, TWP, (2) and provide notice of a web-service interface data exchange mechanism between CBP and the Transportation Security Administration (TSA) Transportation Vetting System (TVA) for the eBadge program.

[1] CBP Preclearance provides for the U.S. border inspection and clearance of commercial air passengers and their goods in certain foreign countries. A preclearance inspection is essentially the same inspection an individual would undergo at a U.S port of entry. Visit https://www.cbp.gov/border-security/ports-entry/operations/preclearance for a list of CBP preclearance locations.

[2] *See* DHS/CBP/PIA-002(c) Global Enrollment System (GES) (November 1, 2016), *available at:* www.dhs.gov/privacy.

CBP migrated all trusted worker program data from GES to TWP, which is an operational subsystem under the e-Business Cloud.[3] The e-Business Cloud resides in the CBP Amazon Web Services (AWS) Cloud East (CACE) environment and consolidates a number of cloud native, web-based systems into a single Security Authorization Package (SAP). CACE provides a secured facility, network, databases, and necessary encryption to protect the confidentiality, integrity, and availability of the user data. The data, including PII, is attributable to various DHS/CBP systems hosted in CACE. CBP conducted the migration from GES to TWP in order to separate trusted worker vetting from trusted traveler vetting and better handle the differing workloads.

TWP offers a flexible, efficient, and scalable platform for data storage to operate CBP's IT capabilities and solutions. Only CBP personnel provisioned under a specific role have access to and are the primary users of TWP. Future modifications of TWP will include a public portal. Applicants will be able to access this portal and submit applications for Trusted Worker programs electronically. CBP will document all future modifications to TWP in subsequent TWP PIAs.

eBadge Program

The eBadge program is only available to applicants applying for access to domestic and foreign preclearance airports. CBP continues to operate the eBadge program in conjunction with TSA and commercial service providers that process airport badges and credentials, such as the American Association of Airport Executives. TSA requires name-based Security Threat Assessments (STA) for all individuals seeking or holding airport identification badges or credentials in order to identify potential or actual threats to transportation or national security. The name-based STA involves recurring checks against federal terrorism, immigration, and law enforcement databases. Commercial service providers support airport authorities by channeling airport badge and credential PII to TSA for the STA.

The eBadge program allows CBP to perform additional screening using the Automated Targeting System (ATS) Unified Passenger (UPAX),[4] which includes checks against CBP databases, on the TSA-cleared airport employees seeking access to a Customs Security area, also referred to as a Federal Inspections Services (FIS) area, at any airport accommodating international air commerce designated for processing passengers, crew, their baggage and effects arriving from or departing to foreign countries, as well as the aircraft deplaning and ramp area and other restricted areas designated by the port director.[5] CBP officers review the vetting results in order to

[3] e-Business Cloud is a CBP major system that houses a variety of CBP cloud-based systems. e-Business Cloud does not have any user interfaces and simply acts as the overarching architecture to house certain CBP cloud systems, which are all separately covered with their own privacy compliance documentation. e-Business Cloud currently holds e-APIS Cloud and Trusted Worker Program System.

[4] *See* DHS/CBP/PIA-006 (e) Automated Targeting System, which describes the super query function in detail. *This PIA is available at:* www.dhs.gov/privacy.

[5] 19 CFR § 122.181, Customs Duties; Part 122. Air Commerce Regulations, Subpart S. Access to Customs Security

determine the individual's eligibility for a Customs Access Seal (CBP Seal).[6] Upon successful CBP screening, CBP advises the commercial service providers to direct the airport authority to affix a CBP Seal to the individual's TSA-approved Security Identification Display Area (SIDA) badge, which then authorizes the individual access to the FIS areas.[7]

All individuals submitting initial applications must appear in person with proper government-issued documents at the CBP Airport Security Program office to establish identity and verify employment eligibility. Individuals who have not first received clearance by TSA are not eligible to apply for the CBP Seal.

TWP will be modified in the future to include a public facing web page, which eBadge applicants will be able to use to electronically submit CBP Form 3078 to CBP. The public portal will allow eBadge applicants to enter information that CBP does not receive from the CBP/TSA interface exchange.

eBadge Applicant Requirements

CBP operates the eBadge program in the airport environment. TWP receives the application via the new TSA Transportation Vetting System (TVS)[8] interface as well as from an applicant directly submitting CBP Form 3078 to the CBP Airport Security Program Office at the airport where they wish to work. At this time, CBP still requires applicants to submit CBP Form 3078 even when CBP receives information via the TSA TVS interface. Additionally, the applicant's employer must submit a letter of intent to the CBP Airport Security Program office. The letter of intent informs CBP what activities the applicant will be conducting in the FIS and provides information on the employer. This letter includes proof of citizenship and identification. A CBPO reviews the letter of intent and verifies information against the data received from TSA TVS. CBP Officers (CBPOs) manually enter the information from CBP Form 3078 into TWP prior to submitting information to ATS UPAX for vetting. Port locations will securely store the paper copy for reference for 5 years. Additionally, both the CBP Form 3078 and employer letter of intent are scanned and uploaded into TWP by the CBPO.

Once the CBPO submits information into the ATS UPAX system, the ATS UPAX system begins to run queries (i.e., ATS super query searches) on the applicant and to flag derogatory information. The CBPO receives from TWP all derogatory information flagged in ATS UPAX. The CBPO must evaluate the ATS UPAX vetting results provided in TWP and adjudicate the eBadge application. CBPOs working in the CBP Airport Security Program Office are responsible

---

Areas.

[6] 19 CFR § 122.182, Customs Duties; Part 122. Air Commerce Regulations, Subpart S. Access to Customs Security Areas.

[7] *See* DHS/TSA/PIA-020 Security Threat Assessment for Airport Badges and Credential Holders (SIDA), *available at:* www.dhs.gov/privacy.

[8] *See* DHS/TSA/PIA-030(e) Traveler Vetting System, *available at*: www.dhs.gov/privacy.

for reviewing applicant data. After the vetting results conclude on the applicant, the Port Director will review the local CBP Airport Security Program Office policy and determine if an interview is necessary. CBPOs conduct interviews with applicants identified to be at a higher risk threshold and/or individuals that require additional information or documentation to determine their eligibility for the program. CBPOs will reach out to the applicant to conduct an interview, at the applicant's duty station only, to review the eBadge application information and ensure all biographic information entered on the CBP Form 3078 is correct. The port director has final discretion on CBP Seal approvals, denials, and revocations.

eBadge Application: Approval, Denial, and Revocation

Upon successful screening/vetting of the applicant, CBPOs will adjudicate the application in TWP and advise the employer and employee of the results.[9] Applicants approved for the CBP Seal will receive a decal, which is affixed to their SIDA badge. The CBP Seal allows the employee to access secure CBP areas at airports. Badge access areas and requirements may vary between locations (i.e., zones, ports of entry); however, the eBadge vetting standards CBP has established for airports of entry are consistent and determined under 19 CFR 122.182, Security Provisions.[10] CBP has the authority to deny any application if derogatory information is uncovered on the applicant during the vetting process.

If an applicant is ineligible for the CBP Seal, he or she will receive a denial letter in the mail. The denial letter includes information on why CBP denied the application and may include specific derogatory information that CBP uncovered during vetting. The letter also informs the applicant of his or her right to appeal the denial before it becomes final. If the applicant choses to appeal the denial, the applicant must file a written appeal within 10 days of receipt of the letter. A written appeal, filed in duplicate, must contain evidence to overcome the reason for denial, and must be sent to the port director's address noted in the denial letter. Within thirty days of the receipt of the appeal, CBP must make a final decision on the appeal.

In some situations, CBP may revoke a CBP Seal, per the grounds in 19 CFR § 122.187, and the affected individual will receive a revocation letter in the mail.[11] Reasons for revocation include: probable cause to believe seal was obtained through fraud; probable cause to believe the

[9] This disclosure is consistent with DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, which permits disclosures pursuant to Routine Use J: "to third parties during the course of a law enforcement investigation or background check to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure."

[10] 19 CFR § 122.182, Air Commerce Regulations; Subpart S. Access to Customs Security Areas, Section 122.182-Security Provisions.

[11] 19 CFR §122.187, Air Commerce Regulations; Subpart S. Access to Customs Security Areas, Section 122.187-Revocation or suspension of access.

employee committed certain crimes;[12] and misuse of seal. The individual has the right to appeal the revocation. If the individual chooses to appeal the revocation, he or she must file a written appeal within 10 days from receipt of the letter. A written appeal, filed in duplicate, must contain evidence to overcome the reason for revocation, and must be sent to the port director's address noted in the revocation letter. Within thirty days of the receipt of the appeal, CBP must make a final decision on the appeal.

eBadge: Web Service Data Exchange

CBP conducts a background check on a subset of the Aviation Worker[13] population through the eBadge program. Previously, employees seeking unescorted access to CBP-controlled FIS (i.e., secure areas of airports and aircraft) had to undergo two separate background checks (by TSA and CBP, respectively) with slightly different adjudication standards but similar data requirements.

TSA and CBP developed a web-service interface to share biographic and biometric data (i.e., fingerprint images) between agencies electronically. Individuals undergoing a background check by TSA submit their biographic and biometric data to TSA during the SIDA badge process. The web service then transmits the biographic and biometric data from TSA TVS to CBP TWP. CBP uses this information to adjudicate eBadge applications without having to collect certain biometric and biographic data separately. For now, aviation workers will still be required to submit Form 3078 to cover additional information not initially captured by TSA, but CBP is working with TSA to create a standardized collection. The data transmitted through the network will be limited to CBP and TSA network unclassified operational and administrative data. The transmission of data across government agencies reduces duplicative efforts on aviation workers to enter data, and lessens the administrative burden on CBPOs, who previously entered the applicant's information manually in to the CBP Global Enrollment System (GES).

Bonded Worker Program

The Bonded Worker program applies to individuals who work at locations where bonded warehouses, facilities, or designated areas operate under CBP supervision.[14] This program applies only to warehouse proprietors, Foreign Trade Zone (FTZ) operators, officers, and recordkeeping

---

[12] For a list of disqualifying offenses see 19 CFR § 122.183 (a)(4) Denial of access, *available at*: https://www.govinfo.gov/app/details/CFR-2012-title19-vol1/CFR-2012-title19-vol1-sec122-183.

[13] The aviation worker population refers to an individual employed in, or applying for, a position as a security screener under section 44935(e), or a position in which the individual has unescorted access, or may permit other individuals to have unescorted access, to aircraft of an air carrier or foreign air carrier, or a secure area of an airport in the United States the Administrator designates that serves as an air carrier or foreign air carrier. *See* 49 U.S. Code § 44936, Employment investigations and restrictions.

[14] 19 U.S.C. § 1555, Bonded Warehouses. A Customs bonded warehouse is a building or other secured area in which imported dutiable merchandise may be stored, manipulated, sorted, repacked, cleaned, or undergo manufacturing operation without payment of duty for up to 5 years from the date of importation.

employees of a corporation that has been granted the right to operate the bonded facility. CBP has the authority to vet these individuals under the Bonded Worker program, and to revoke or suspend the bonded status of a warehouse proprietor, operator, or any officer of a corporation that holds the right to operate a bonded warehouse or an FTZ, upon conviction of certain crimes.[15]

An applicant seeking to establish a bonded warehouse must submit a written application to the local CBP port director nearest to where the warehouse is located, describing the premises, the location, and the class of warehouse under development. Additional information and steps required to be taken by the applicant can be found in 19 CFR § 19.2, Applications to bond. After the applicant successfully completes the application process, the port director shall promptly notify the applicant in writing of the decision to approve or deny the application to bond the warehouse.

Applicants seeking to work in an approved bonded warehouse or facility must complete CBP Form 3078 and submit it to the port director of the port nearest to where the facility is located. As with eBadge, CBPOs manually enter CBP Form 3078 into the TWP and background vetting is then conducted through ATS UPAX. The vetting conducted for bonded warehouse workers is the same as for eBadge applicants. Port locations will keep the paper copy of Form 3078 for reference and store the document in a locked drawer for 5 years.

See the *Characterization of the Information* section below for the data requirements pertaining to the Bonded Worker program.

Broker's License Program

Customs brokers are private individuals, partnerships, associations, or corporations licensed, regulated, and empowered by CBP to assist importers and exporters in meeting federal requirements governing imports and exports.[16] Customs brokers submit necessary information and appropriate payments to CBP on behalf of their clients and charge the clients a fee for this service. Customs brokers must have expertise in the entry procedures, admissibility requirements, classification, valuation, and applicable rates of duties, taxes, and fees for imported merchandise.

The Broker's License program applies to individual applicants, officers, and principals of customs brokerage firms whose primary responsibility is filing required documentation to import goods into the United States. A Broker's License applicant must be a U.S. citizen who is not an officer or employee of the U.S. Government and is of good character, who has attained 21 years of age prior to submission of the application and has passed a Customs broker exam within 3 years of the submission of the application. Applicants must complete a Broker's License application at

[15] 19 CFR § 19.2, Bonded Warehouses; Applications to bond; and 19 CFR § 19.3, Bonded Warehouses; alterations; relocation; suspensions; discontinuance.
[16] "Customs broker" means a person who is licensed under 19 CFR § 111 to transact customs business on behalf of others.

a CBP port of entry (PoE)[17] and undergo a CBP background investigation.[18] This vetting process adheres to regulatory requirements and verifies that the applicant does not have a history of activity that would make him or her unsuitable to carry out the responsibilities entrusted to a customs broker.[19] Applicants must complete CBP Form 3124-Application for Customs Broker's License and submit it to a CBP POE for manual entry into TWP.[20]

See the *Characterization of the Information* section below for the data requirements pertaining to the Broker's License program.

Trusted Worker Programs: New Applicant Vetting Process

CBP uses ATS-UPAX to vet travelers in CBP's Trusted Worker programs: eBadge, Bonded Worker, and Broker's License.[21] CBPOs enter applicant information manually into TWP. TWP creates a Person ID, which is associated with the new applicant, and initiates the screening process. The screening process consists of a standard series of queries run in ATS UPAX on the applicant, including automated queries against the CBP TECS System,[22] which contains traveler history data for airport and land borders. This is conducted on all applicants regardless of the program for which they are applying. Applicants for the eBadge program undergo additional vetting, which will be discussed separately.

CBPOs review the applicants' information in ATS UPAX or TWP using a Risk Assessment Worksheet (RAW), which is created in ATS UPAX from ATS UPAX information. As part of the screening process, CBP may also conduct an interview with the applicant and may retain a photograph and fingerprints of the applicant.[23] CBPOs adjudicate the applicants in either ATS UPAX or TWP. The RAW with the assigned pass/fail, generated from ATS UPAX, is

[17] Port of Entry (PoE) is a place where one may lawfully enter a country (i.e., international airports, road and rail crossings on a land border, and seaports where a dedicated customs presence is posted). The eBadge program is available to domestic and foreign preclearance airports. The eBadge program is not currently available at U.S. land ports and seaports.
[18] 19 CFR § 111.11, Customs Brokers; Subpart B. Procedure To Obtain a License or Permit, Section 111.11- Basic Requirements for a Broker's License.
[19] 19 CFR § 111.12, Customs Brokers; Subpart B. Procedure To Obtain a License or Permit, Section 111.12- Application for License.
[20] CBP Form 3124, *available at*: https://www.cbp.gov/document/forms/form-3124-application-customs-broker-license.
[21] *See* DHS/CBP/PIA-006(e) Automated Targeting System, *available at:* www.dhs.gov/privacy.
[22] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at*: www.dhs.gov/privacy.
[23] Photographs and fingerprints of trusted workers are maintained in the Automated Biometric Identification System (IDENT) and covered by the existing DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities System of Records Notice, 73 FR 77753 (December 19, 2008). For more information on IDENT see DHS/OBIM/PIA-001 Automated Biometric Identification System, *available at:* www.dhs.gov/privacy. DHS is retiring IDENT and replacing it with the Homeland Advanced Recognition Technology System (HART), which will be discussed in a forthcoming PIA.

automatically associated with the applicant's TWP record. CBP then uses TWP to complete the applicant's processing.

Trusted Worker Programs and ATS UPAX Applicant Process Flow

1. Applicant applies for Trusted Worker Programs status.
2. Applicant information transfers to TWP electronically or is entered manually.
3. ATS UPAX queue receives information from TWP.
4. ATS UPAX vets applicant through the standardized process.
5. CBP staff reviews the Risk Assessment Worksheet (RAW) in ATS UPAX or TWP.
6. CBP staff adjudicates applicants in the ATS UPAX or TWP.
7. RAW with the recommended Pass/Fail is automatically associated with applicant's TWP record; applicant processing is completed in TWP.

Trusted Worker Programs: Recurrent Vetting

ATS UPAX conducts recurrent vetting on individuals with approved applications and granted CBP Seals every 24 hours. Through recurrent vetting, every 24 hours, ATS-UPAX automatically reviews all information found on an approved applicant to determine there is any new derogatory or other information that needs to be manually reviewed by a CBPO. If new derogatory information exists, then CBP may conduct an interview with the applicant to determine whether the information is accurate and whether the applicant should be removed from the program and have his or her access revoked. If necessary, a port director may revoke credentials without conducting an interview. If the applicant's status is revoked, the notification, electronically transmitted from TWP, shall state the grounds for revocation. The decision of the port director will be the final administrative determination in the matter. The notification will inform the individual of how he or she may appeal the decision.

TWP does not conduct recurrent vetting on individuals who have had their application denied or revoked. Once an application is denied or revoked, information about the applicant is removed from ATS-UPAX, unless that information is linked to active law enforcement lookout records, enforcement activities, or investigative cases, in which case the data is maintained by CBP in ATS UPAX consistent with ATS retention schedule as reflected in the ATS SORN (i.e., for the life of the law enforcement matter to support the activity and other enforcement activities that may become related).

eBadge Program: Derogatory Update Notification Service

In addition to ATS UPAX recurrent vetting through CBP holdings, CBP plans to leverage DHS Automated Biometric Identification System (IDENT)[24] services to assist in the recurrent vetting of eBadge program enrollees. CBP will leverage notification services through IDENT, which would provide an electronic notification to ATS UPAX when derogatory information resulting from a recent law enforcement encounter is received on an eBadge program enrolled member. eBadge program applicants initially submit their fingerprints into TSA TVS via the TSA SIDA process. The fingerprints are gathered through TSA TVS and electronically submitted to CBP's TWP via a web service interface. CBP's TWP receives the fingerprint information (i.e., fingerprint binary capture date, fingerprint binary format ID, and fingerprint binary base 64 object), transfers the data into ATS UPAX, and ATS UPAX sends the information to IDENT. IDENT biometrically searches the identity and provides an automated identification response to ATS UPAX that includes all encounters, dates, and locations of encounters (criminal, or non-criminal from state, local or federal law enforcement agencies), along with the following: name, date of birth, citizenship, encounter ID, date, activity (location site of encounter), watchlist status, and Fingerprint Identification Number (FIN). IDENT stores all biometric information on the approved eBadge program applicant.

In the event that the eBadge program applicant and/or member is encountered by law enforcement (e.g., a warrant is issued on the eBadge applicant or member), additional biometrics may be captured from state, local, or federal law enforcement agencies and submitted to IDENT for search against IDENT data holdings through DHS interoperability with the Federal Bureau of Investigations (FBI) Next Generation Identification (NGI) biometric system.[25] IDENT matches the eBadge member previously captured biometrics to the new encounter, linking the event and triggering a derogatory update notification message for submission back to ATS UPAX for the purpose of eBadge CBP Officers reviewing the recurrent vetting eBadge hotlist in ATS UPAX will receive a notification indicating an update to derogatory information has occurred on an individual enrolled in the eBadge program. IDENT then sends CBP a notification message of "new encounter" through ATS UPAX. Officers will subsequently retrieve the identity data from IDENT to review the derogatory information and determine continued program eligibility.

---

[24] *See* DHS/OBIM/PIA-001 Automated Biometric Identification System, *available at:* www.dhs.gov/privacy.
[25] *See* Federal Bureau of Investigation (FBI) Privacy Impact Assessment (PIA), Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis-ngi-biometric-interoperability and JUSTICE/FBI-009, The Next Generation Identification (NGI) System, Systems of Records Notification (SORN) *available at* https://www.federalregister.gov/documents/2019/10/09/2019-21585/privacy-act-of-1974-system-of-records.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

CBP operates the eBadge program, which provides screening and vetting services for TSA-cleared airport employees seeking access to CBP-controlled Federal Inspection Service (FIS)-restricted areas. eBadge applicants complete Form 3078, and the principal purpose for collecting the information is to enable CBP to conduct a background investigation and thereby determine whether the applicant meets the criteria for issuance of an identification card. The authority to collect information on CBP Form 3078 is pursuant to 5 U.S.C. § 301; 19 U.S.C. §§ 1551, 1565, 1624, 1641; and 19 CFR § 112.42.

CBP operates the Bonded Worker program, which provides warehouse proprietors, Foreign Trade Zone (FTZ) operators, officers, and recordkeeping employees of a corporation that have been granted the right to operate a bonded facility, access to locations where bonded warehouses, facilities, or designated areas operate under CBP supervision. Bonded Worker applicants complete Form 3078, and the principal purpose for collecting the information is to enable CBP to conduct a background investigation and thereby determine whether the applicant meets the criteria for issuance of an identification card. The authority to collect information on CBP Form 3078 is pursuant to 5 U.S.C. 301; 19 U.S.C. §§ 1551, 1565, 1624, 1641; and 19 CFR § 112.42.

CBP operates the Broker's License program, which provides customs brokers (i.e., private individuals, partnerships, associations, or corporations licensed, regulated, and empowered by CBP to assist importers and exporters in meeting federal requirements governing imports and exports) a valid Customs broker license. Custom broker applicants are vetted through TWP and must pass a background investigation in order to be qualified for a broker's license. The authority to collect information on CBP Form 3124 is pursuant to 19 U.S.C. § 1641; 5 U.S.C. 301; Revised, as amended; and 19 CFR § 111.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities[26] provides SORN coverage for individuals applying for access to the FIS, bonded workers, and broker's licenses.

[26] DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, 73 FR 77753 (December 19, 2008).

DHS/CBP-006 Automated Targeting System[27] provides SORN coverage for information retained by ATS UPAX and permits the collection of information from individuals applying for access to the FIS, bonded workers, and broker's licenses.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes, CBP completed a system security plan. The Authority to Operate (ATO) date for e-Business Cloud, of which TWP is a subsystem, was signed on June 14, 2019.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

CBP is working with the U.S. National Archives and Records Administration (NARA) to develop a retention schedule for these records that will be more closely aligned with program requirements. CBP is proposing that all TWP data be retained for six years after an individual's membership is no longer active, whether due to expiration without renewal at the end of the membership validity, abandonment, or CBP termination. Data is retained after membership becomes inactive so that CBP can more easily vet an individual who chooses to reapply, as well as to provide a record for redress purposes. Bonded Worker membership expires after five years; eBadge, and Brokers License have different renewal periods, and each renewal period has been listed below:

For eBadge, each approved CBP Seal will remain valid for 2 years from the date of issuance. Retention of an approved CBP Seal beyond the applicable 2-year period will be subject to the reapplication provisions of paragraph (c)(2) of 19 CFR 122.182.[28]

For Broker's License, each broker must file a written status report with CBP every three years, starting from 1985. The next triennial status report will be due in 2021.[29] The report must be accompanied by the fee prescribed in 19 CFR 111.96(d) and must be addressed to the director of the port through which the license[30] was delivered to the licensee (see 19 CFR 111.15).[31] A report received during the month of February will be considered filed timely. No form or particular format is required.

Additionally, fingerprints are retained in IDENT. NARA approved records retention schedule for the IDENT system requires OBIM to maintain IDENT records in custody for 75 years or when no longer needed for legal or business purposes, whichever is later (DAA-0563-2013-

[27] DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[28] 19 CFR § 122.182, Customs Duties; Part 122. Air Commerce Regulations, Subpart S. Access to Customs Security Areas.
[29] 19 CFR § 111.30 (d)(1), Customs Brokers; Subpart C. Duties and Responsibilities of Customs Brokers.
[30] 19 CFR § 111.96 (b)(1), Customs Brokers; Subpart E. Monetary Penalty and Payment of Fees.
[31] 19 CFR § 111.15, Customs Brokers; Issuance of License.

0001-0006). CBP is re-evaluating the current retention period to determine whether a new retention period or combination of retention periods is appropriate. CBP will publish a PIA update for any change in the retention period.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Some of the information collected in this system is covered by the PRA with OMB Control Numbers 1651-0008 (CBP Form 3078) and 1651-0034 (CBP Form 3124).

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The following data elements are captured by TSA via the SIDA application process and transmitted to CBP TWP:

- **Application Data:** application ID; airport code; airport category; SIDA badge access level; SIDA badge status; SIDA badge issue date; SIDA badge document identification number; SIDA badge expiration date; SIDA badge document file name (conditional); SIDA badge document format (conditional).
- **Applicant Biographic Data:** first name; last name; gender; birth date; place of birth (country); present address type (main residence and mailing address); address street; address city; address state; address country; organization name; organizational postal code (conditional); country of citizenship; passport number (conditional); passport country (conditional).
- **Applicant Biometric data:** fingerprint binary capture date; fingerprint binary format ID; and fingerprint binary base 64 object.

The applicant's employer must submit a letter of intent to CBP. The letter of intent does not have a standard format and varies from port to port. The below information is a sample of what is provided from the employer of the eBadge applicant in the letter of intent.[32]

[32] 19 CFR 122.182, Customs Duties; Part 122. Air Commerce Regulations, Subpart S. Access to Customs Security Areas, *available at*: https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=17a4277dd9c6449feb252c542701bd87&ty=HTML&h=L&mc=true&r=PART&n=pt19.1.122.

- Name of applicant requiring access to CBP security area (first, last);
- Proof of applicant citizenship, if interviewed (i.e., a passport or other form of photo ID);
- Applicant email address;
- Applicant job title;
- Position description;
- First time applicant, and new SIDA badge number (if applicable);
- Renewal applicant, current SIDA badge number, and SIDA badge expiration date (if applicable);
- Access level requested (zone 1 or zone 2);
- Bond number;
- Employer printed name and signature; and
- Employer contact information (email address, phone number);

Information collected from the eBadge applicant on the CBP Form 3078 and entered into TWP:

- Type of Activity Requiring an ID Card;
- Date of this application;
- Name (last, first, middle);
- Social Security number (SSN);
- Other names the individual has been known by (nicknames, aliases, etc.);
- Date of birth;
- Home address (number, street, city, state, and zip code);
- Name and address of present employer;
- Phone number (applicant);
- Business phone number (applicant);
- Place of birth (city, county, state, country);
- Height;
- Weight;

- Color hair;
- Color eyes;
- Visible scars or marks;
- Photograph of applicant (voluntary, and attached to form);[33]
- Whether the individual has ever applied for a U.S. Coast Guard or Merchant Marine card (Y/N);
- Has application for a U.S Coast Guard or Merchant Marine card been denied (Y/N);
- Explanation of application denial (if applicable);
- U.S. Coast Guard or U.S. Merchant Marine Card Number (if applicable);
- List all residences during the last 5 years (dates, number and street, city, state);
- Previous U.S. Military Service (if applicable);
- Branch of Service (if applicable);
- Military Service Serial Number (if applicable);
- Type of Military Discharge (if applicable);
    - If discharge was other than honorable, explain in full detail (if applicable);
- Whether the individual has ever applied for an identification card with U.S. Customs and Border Protection;
- Previous employment, list over last 10 years (dates, employer name and address, occupation);
- Whether the individual has ever been convicted of any crime or offense (Y/N);
- If yes, explain all convictions (date, place, charge, court, final disposition); and
- Whether the individual uses or has ever used narcotic drugs (Y/N).

Information collected from candidates for Bonded Worker and entered into TWP:

- Employment location;
- The applicant must complete the CBP Form 3078 (entered manually into TWP by CBP). The CBP Form 3078 data elements listed in the eBadge section also apply to the bonded worker program.

[33] The photo is not electronically entered into TWP; the form itself is scanned and uploaded into TWP.

Additionally, the port director may require an individual applicant to submit fingerprints on form FD 258 or electronically at the time of filing the application, or in the case of applications from a business entity, the port director may require the fingerprints on form FD 258 or electronically of all employees of the business entity.

Information collected from candidates for a Broker's License:

The applicant must complete the CBP Form 3124 (entered manually into TWP by CBP). The CBP Form 3124 data elements are listed below:

- Name (and other names used);
- Date of birth;
- SSN;
- Type of license applied for;
- CBP Port;
- Whether the individual has ever applied for a customs broker's license;
- License suspension/revocation information (if applicable);
- Whether the applicant is an officer or employee of the United States;
- Place of birth;
- U.S. Citizenship status (i.e., natural-born or naturalized);
- Date and place of naturalization (if applicable);
- Home phone number;
- Business phone number;
- Home address;
- List of criminal convictions or offenses;
- Bankruptcy, tax lien, debt legal judgement status;
- Name, addresses, and phone number of references (applicant must list 6); and
- Name, addresses, dates of birth, place of birth of all Corporate Officers or Principals (if applicable).

2.2 What are the sources of the information and how is the information collected for the project?

Individuals applying to the eBadge and Bonded Worker programs complete the CBP Form 3078 and submit it to CBP. The applicant's employer can also complete the form on behalf of the applicant.

Individuals applying to the Broker's License program complete the CBP Form 3214 and submit the form to CBP. The applicant, or employer of the applicant, can be complete the CBP Form 3214. The applicant's employer can potentially complete the form on behalf of the applicant.

Additionally, applicants applying to the eBadge program must first apply to the TSA SIDA badge process and submit the following fingerprint information to TSA: fingerprint binary capture date; fingerprint binary format ID; and fingerprint binary base 64 object. The TSA Transportation Vetting System (TVS) transmits the fingerprint data to CBP's TWP via a web-service interface. The fingerprint information is received by TWP and transmitted to ATS.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

This system does not use commercial sources or publicly available information.

2.4 Discuss how accuracy of the data is ensured.

CBP uses the ATS UPAX system to vet Trusted Worker program applicants and determine if applicants match to any derogatory information. If there is a discrepancy or if CBP has reason to believe an application is incomplete or inaccurate, CBP may require the Trusted Worker program applicant to participate in a personal interview where a CBP Officer can verify the information provided and the applicant can clarify any inaccuracies.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that, due to the need to manually enter information from CBP Form 3078 and CBP Form 3124, inaccurate data could be entered into TWP by the CBPO, which may result in an erroneous decision to approve or disapprove enrollment in a particular program.

Mitigation: There is always a risk of a typographical error when an individual manually enters information into a system. If there are any doubts concerning whether the individual applying for the Trusted Worker program is the same individual of record in a law enforcement database, or if that database record raised accuracy concerns, CBP may conduct a personal interview and use the application data to verify the information. CBP offers the applicant an

opportunity to reapply and clarify potential inaccuracy. In addition to reapplying, eBadge applicants can appeal CBP's denial or revocation and may note that they believe CBP is using incorrect information.

Privacy Risk: There is a risk that the letter of interest submitted from the employer, on behalf of the employee, may contain inaccurate information about the employee requesting access to a trusted worker program (eBadge, Bonded Worker, and Brokers License). The inaccurate information may result in an erroneous decision to approve or disapprove enrollment of the applicant in a particular program.

Mitigation: There is always a risk of error when employers create the letter of interest. If there are any doubts concerning whether the individual in the letter of interest is the same individual of record in a law enforcement database, or if that database record raised accuracy concerns, CBP may conduct a personal interview and use the application data to verify the information. CBP offers the applicant an opportunity to reapply and clarify potential inaccuracy.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP collects voluntary information from applicants in order to assess their eligibility for enrollment in the eBadge, Bonded Worker, or Broker's License programs supported by TWP. CBP vets these individuals to ensure they either meet or remain eligible for program participation. CBP conducts recurrent vetting on program applicants and enrollees to ensure that they do not pose threats to law enforcement or national security. The recurrent vetting in TWP determines the applicant's eligibility and grants them continued access to CBP-controlled areas.

For Broker's License, Form 3124, the principal purpose for collecting the information is to enable CBP to conduct a background investigation on the applicant and thereby determine whether the applicant meets the criteria established for the issuance of a Customs broker's license. A broker's license is necessary for an individual to engage in "customs business." CBP uses the SSN as an identifier when conducting a background investigation, and as an identifier throughout the career of the Customs broker.

For eBadge and Bonded Worker, Form 3078, the principal purpose for collecting the information is to enable CBP to conduct a background investigation and thereby determine whether the applicant meets the criteria for issuance of an identification card allowing him or her access to work in an FIS.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The TWP system does not conduct data mining. However, CBP may conduct data mining on information CBP submits to ATS UPAX as explained in the ATS PIA.[34]

3.3 Are there other components with assigned roles and responsibilities within the system?

CBP is creating a link between TSA's Transportation Vetting System and TWP that allows TSA to transfer eBadge applications to CBP. TSA will not have any access to TWP other than to push eligible applications into TWP from TVS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information used to enroll individuals in trusted worker programs will be used for a purpose inconsistent with the original collection.

Mitigation: All system users are trained to use information strictly for determining program eligibility. Access to TWP is granted to users by a limited number of system administrators and access level varies based on a need to know and the user's role. Users are also required to take annual privacy training to ensure that they know and understand the importance of managing sensitive PII.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CBP is providing notice of a new privacy sensitive system by publishing this PIA. In addition, DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities[35] and DHS/CBP-006 Automated Targeting System[36] discuss the information collected as part of the Trusted Worker program and provide notice.

---

[34] *See* DHS/CBP/PIA-006 Automated Targeting System, *available at:* www.dhs.gov/privacy.
[35] DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities System of Records Notice, 73 FR 77753 (December 19, 2008).
[36] DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).

Additionally, CBP provides a Privacy Act Statement on the CBP Form 3078 and CBP Form 3124.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

CBP does not require anyone to participate in the programs. Consent is implied when an applicant applies to a Trusted Worker program. Applicants must certify that they understand any information they provide, including any supporting documentation, biometric data, and statements made during interviews, may be shared among law enforcement and other government agencies as necessary to conduct a background investigation. TWP uses data collected only for the purpose defined, including border and immigration management, national security, and law enforcement. Once enrolled, individuals have no opportunity to "opt out" of the use of their data for any of these stated purposes.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that applicants and enrollees may not know how CBP may use the information they submitted to TWP.

Mitigation: CBP mitigates this risk by providing Privacy Act Statements stating the purpose for the data collection on the CBP Form 3078 and CBP Form 3124, provided to applicants for the Bonded Worker and Broker's License programs. CBP also mitigates the risk by publishing this PIA, the DHS/CBP-010 SORN, and the DHS/CBP-006 SORN.

Privacy Risk: There is a risk that an employer, submitting an application on behalf of an applicant, may not provide the applicant notice of how CBP intends to use the information submitted into TWP.

Mitigation: This risk is partially mitigated through publishing this PIA, the DHS/CBP-010 SORN, and the DHS/CBP-006 SORN. Additionally, because CBP access is needed to do their job employees have constructive notice that CBP has approved of their access by reviewing information about them.

Privacy Risk: There is a risk that the references whose names, addresses, and telephone numbers are submitted on CBP Form 3124 by the applicant may not be provided notice of collection and use of their information.

Mitigation: This risk is partially mitigated through publishing this PIA. Additionally, some applicant references are contacted by CBP, and upon contact, are notified that their information was provided by the applicant on CBP Form 3124 and entered into TWP and will only be used to perform a character check on the applicant. Other references may never be

contacted, but reference information will not be put into any other system and being a reference will have no impact on CBP vetting of the reference if they travel or apply for a benefit.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

CBP is proposing that all TWP data be retained for six years after an individual's membership is no longer active, whether due to expiration without renewal at the end of five years, abandonment, or CBP termination. Data is not deleted immediately after membership becomes inactive so that CBP can more easily vet an individual who chooses to reapply, as well as to provide a record for redress purposes. The historical record can also be useful for other vetting purposes when an individual has been found ineligible for a TW program.

For eBadge, each approved CBP Seal will remain valid for 2 years from January 1, 2002, in the case of a CBP Seal issued prior to the date, and for 2 years from the date of issuance in all other cases. Retention of an approved CBP Seal beyond the applicable 2-year period will be subject to the reapplication provisions of paragraph (c)(2) of 19 CFR 122.182.[37]

For Broker's License, each broker must file a written status report with CBP every three years, starting from 1985. The next triennial status report will be due in 2021.[38] The report must be accompanied by the fee prescribed in 19 CFR 111.96(d) and must be addressed to the director of the port through which the license was delivered to the licensee (see 19 CFR 111.15).[39] A report received during the month of February will be considered filed timely. No form or particular format is required.

Additionally, fingerprints captured for the eBadge, Bonded Worker, and Brokers License programs are retained in IDENT. NARA approved records retention schedule for the IDENT system requires OBIM to maintain IDENT records in custody for 75 years or when no longer needed for legal or business purposes, whichever is later (N1-563-08-34). DHS is re-evaluating the current retention period to determine whether a new retention period or combination of retention periods is appropriate. DHS will publish a PIA update for any change in the retention period.

[37] 19 CFR 122.182, Customs Duties; Part 122. Air Commerce Regulations, Subpart S. Access to Customs Security Areas.
[38] 19 CFR 111.30 (d)(1), Customs Brokers; Subpart C. Duties and Responsibilities of Customs Brokers.
[39] 19 CFR 111.96 (b)(1), Customs Brokers; Subpart E. Monetary Penalty and Payment of Fees.
19 CFR 111.15, Customs Brokers; Issuance of License.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk CBP will retain information about trusted worker program applicants for longer than necessary.

Mitigation: This risk is mitigated. Approved applications are stored for the duration of the individual's membership in the program and then for six additional years. Bonded Worker membership expires after five years. For eBadge, approved CBP Seals remain valid for 2 years. For Broker's License, each broker must file a written status report with CBP every three years. CBP stores information for longer than expiration dates in order to more easily vet individuals who reapply. A denied application is stored for 6 years. If CBP revokes a credential prior to expiration then the records are stored for 6 years after revocation. The same is true for credentials that are abandoned before membership expires, in which case TWP retains the information for 6 years after abandonment date. If information provided by applicants is linked to a law enforcement record CBP will maintain that information in ATS UPAX for 75 years.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CBP may share information related to an eBadge applicant with the applicant's employer. CBP may share eBadge information for airport workers with airport authorities through commercial service providers as part of the background checks process. CBP does not share bonded worker or broker's license program information outside of DHS. CBP does not share TWP information with any non-DHS agencies.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Sharing of information with employers and airport authorities is done pursuant to Routine Use J of DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, which permits the sharing of information to third parties during the course of a background check in order to obtain pertinent information about the applicant.

CBP does not share bonded worker or broker's license program information outside of DHS.

6.3 Does the project place limitations on re-dissemination?

CBP does not permit re-dissemination of information shared out of TWP.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

CBP employees are required to complete DHS Form 191 for all information disclosures out of TWP.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information shared with employers and the airport authority will be disseminated further.

Mitigation: This risk is partially mitigated. CBP uses a disclosure letter to inform employers and airport authorities that the information they receive may not be further disseminated.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

To gain access to TWP information, an enrollee may request information about his or her records contained in TWP through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)) by writing to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002
Fax Number: (202) 325-0230

When seeking records from TWP or any other CBP system of records, the request must conform to Part 5, Title 6 of the Code of Federal Regulations. An individual must provide his or her full name, current address, and date and place of birth. He or she must also provide:

- An explanation of why the individual believes DHS would have information on him or her;
- Details outlining when her or she believes the records would have been created;

- And if the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

The request must include a notarized signature or be submitted pursuant to 28 U.S.C. § 1746, which permits statements to be made under penalty of perjury as a substitute for notarization. Without this information, CBP may not be able to conduct and effective search and the request may be denied due to lack of specificity or lack of compliance with applicable regulations. Although CBP does not require a specific form, guidance for filing a request for information is available on the DHS website at http://www.dhs.gov/file-privacy-act-request and at http://www.dhs.gov/file-foia-overview.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals wishing to correct inaccurate information may submit a Privacy Act Amendment request through the same access process explained above.

7.3 How does the project notify individuals about the procedures for correcting their information?

CBP sends a denial letter to denied applicants that explains the redress process and how applicants can request a record change. CBP provides notice to the individual on how to correct his or her information in this PIA, the DHS/CBP-010 SORN, and the DHS/CBP-006 SORN.

eBadge and Bonded Worker applicants submitting the CBP Form 3078, or Broker's License applicants submitting the CBP Form 3124, must certify the information is accurate and provide a signature and date. On the CBP Form 3078, a signature and date of either the individual (applicant) or association, corporation, or partnership are required in question 35. On the CBP Form 3124, a signature and date are required in section 3.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not know that their denial was based upon erroneous information.

Mitigation: The risk is mitigated by the denial letter that lists the name and address of the applicant and a clear and concise statement of why the application was denied. For example, if the denial is due to criminal conviction or arrest, the type of offense, year, and state in which the incident occurred will be revealed.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

TWP is protected through a multi-layer security approach. The protective strategies are physical, technical, administrative, and environmental in nature and provide access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication of sending parties, and personnel screening to ensure all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

All TWP access and activities are monitored by security and application logs, and regular audits are conducted according to the CBP audit and accountability policy and procedures as stated in the CBP Information Systems Security Policy and Procedures Handbook to ensure compliance. CBP employees found to have engaged in unauthorized access to CBP systems are subject to disciplinary action that could result in criminal penalties or dismissal.

The user base for TWP is CBPOs trained in the input of biographic information from travelers, the correct capture and storage of their biometric information, and in traveler vetting processes. They will access the system through CBP-standard workstations, with appropriate peripheral equipment, and the operation of the system will take place solely within CBP controlled space at designated Ports of Entry and the CBP Risk Assessment Center.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All CBP personnel with access to TWP must complete the DHS Security Awareness Training Course, which includes privacy training. Additionally, all CBP users must keep their TECS access up to date, which requires completion of the TECS Privacy Awareness (TPA) course every two years.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

All users are assigned a role in TWP. There are basic user roles (e.g., CBPO, Technician), supervisory user roles (e.g., supervisor and risk assessor supervisor) and support roles for Office of Field Operations HQ, such as for running reports. The privileged user roles are the supervisory roles. These roles have the ability to create the basic user roles for CBPOs at the POE.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All business requirements, Memoranda of Understanding, and Information Sharing Agreements are reviewed by the respective CBP program manager within the CBP Office of Field Operations, in consultation with the Office of Information Technology. Agreements involving PII are also generally approved by the CBP Privacy Officer, the Office of Chief Counsel, and DHS in accordance with procedures developed by the DHS Information Sharing Governance Board.

Responsible Officials

John A. Maulella
Director
Traveler Entry Programs
Admissibility and Passenger Programs
Office of Field Operations
U.S. Customs and Border Protection
Department of Homeland Security
(202) 344-2605

Debra L. Danisek
CBP Privacy Officer
Office of Privacy and Diversity
U.S. Customs and Border Protection
Department of Homeland Security
(202) 344-1610

Approval Signature

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

_____

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