Privacy Impact Assessment for
the

Continuous Evaluation (CE) Travel Record Data Service (TRDS)

DHS/ALL/PIA-067

August 15, 2018

Contact Point

David Bottom
Chief Information Officer
Office of Intelligence & Analysis
Department of Homeland Security
(202) 447-3976

Reviewing Official

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Travel Record Data Service (TRDS) is a Department of Homeland Security (DHS) project, whereby U.S. Customs and Border Protection (CBP) travel records are shared with the Office of the Director of National Intelligence (ODNI) National Counterintelligence and Security Center (NCSC) Continuous Evaluation System (CES). NCSC will provide authorized Executive Branch agencies with TRDS information, via the CES, to continuously evaluate the suitability of "covered individuals."[1] NCSC will then share relevant CBP travel information with the covered individual's home agency or authorized Investigative Service Provider to allow that home agency to determine if a security-relevant issue exists. DHS is publishing this Privacy Impact Assessment (PIA) to describe the personally identifiable information (PII) within TRDS and the way in which the data is transferred to the NCSC CES.

Overview

Implementing Continuous Evaluation (CE) is part of overarching personnel security clearance reform efforts. CE is mandated by Executive Order (EO) 12968, as amended, which requires that individuals with eligibility for, or access to, classified information be subject to continuous evaluation under standards determined by the Director of National Intelligence (DNI). CE is further defined in EO 13467, as amended.

CE is a personnel security investigative process used to review the background of individuals who have been determined to be eligible for access to classified information or eligible to hold a sensitive position (hereinafter, this cohort will be referred to as "covered individuals") at any time during their period of eligibility (i.e., for the length of time that an individual is eligible to access classified information or to hold a sensitive position).[2] If an individual is no longer eligible to access classified information, or to hold a sensitive position, the individual's home agency will un-enroll the individual from participation in the CE program.

In accordance with CBP's expectations for the use of its data in TRDS, as memorialized in the information sharing agreement between DHS and NCSC attending the TRDS process, the Office of Intelligence and Analysis (I&A) will correlate the CES data with CBP travel data to determine if any covered individuals traveled, or intended to travel, abroad. Whether a covered individual traveled abroad or not, I&A will transmit that information back to NCSC for use in the CES. CE uses automated records checks of commercial databases, U.S. Government

[1] "Covered Individual" is a person who performs work for or on behalf of the Executive Branch or who seeks to perform work for or on behalf of the Executive Branch, as defined in NCSC Security Executive Agent Directive (SEAD) 6, Continuous Evaluation, January 12, 2018, *available at* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf.
[2] *See* https://www.dni.gov/files/NCSC/documents/products/20180316-CE-FAQs.pdf.

databases and other information lawfully available to security officials to assist with the assessment of an individual's continued eligibility to hold a sensitive position or to access classified materials.[3] Individuals subject to CE include current U.S. Government civilian employees, detailees, contractors, military, and other-sponsored individuals who are determined eligible for access to classified information or eligible to hold a sensitive position. In support of CE, I&A is creating TRDS to share select data elements from CBP travel records for integration into the NCSC CES.

As a service provider, I&A is responsible for ensuring the successful operation and maintenance of TRDS, and for ensuring that TRDS meets NCSC CES technical requirements. CBP, as the data provider, maintains ownership of the travel records in a CBP enclave under CBP authorities. All covered individuals whose travel is vetted through TRDS have previously consented to, inter alia, an ongoing travel history review by signing the Standard Form SF-86 (or equivalent form), which informs signatories that their information will be released for either an initial or periodic background investigation for the purpose of attaining and maintaining a security clearance.

TRDS receives queries from the CES about covered individuals. As a service provider, I&A automatically matches CES queries against CBP's Advance Passenger Information System (APIS)[4] and Border Crossing Information (BCI).[5] I&A subsequently provides the relevant portions of foreign travel records that match the CES query to CES, in accordance with CBP's expectations for the use of its data for the TRDS. Specifically, I&A will send NCSC the APIS and BCI data elements outlined in Section 2.1 below in response to any positive match. While this response is not the entire APIS and BCI record, it represents a substantial part of any relevant APIS or BCI record, which will allow the individual's home agency to manually review and adjudicate the significance of any such match. If the individual's home agency needs the entire APIS or BCI record for its files, the home agency may request those records directly from CBP through the existing Request for Information (RFI) processes.

[3] *See* https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-continuous-evaluation-overview. *See* https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-continuous-evaluation-overview.
[4] *See* DHS/CBP-005 Advance Passenger Information System (APIS), 80 FR 13407 (Mar. 13, 2015).
[5] *See* DHS/CBP-007 Border Crossing Information (BCI), 81 FR 89957 (Dec. 13, 2016).

Personnel Security Investigations

Individuals are eligible for access to classified information or to hold a sensitive position only after they have undergone a favorably adjudicated personnel security background investigation.[6] The Director of National Intelligence (DNI), in the role of Security Executive Agent (SecEA), and the Director of the Office of Personnel Management (OPM), in the role of Suitability Executive Agent (SuitEA), are responsible for establishing the Federal Investigative Standards (FIS).[7] Employees eligible for access to classified information or to hold a sensitive position are also subject to periodic reinvestigations and may be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access. A periodic reinvestigation is currently required every five years for an individual's Top Secret clearance or access to sensitive compartmented information, and every 10 years for a Secret clearance. There is a potential that a security-relevant event could occur during the gap between the initial investigation and the periodic investigation, or between periodic investigations, that might indicate to officials the need to re-adjudicate a subject's continued eligibility for classified access or sensitive position. To some extent, the U.S. Government depends on employees to self-report incidents that could trigger a reinvestigation, but absent self-reporting, security officials' awareness of relevant events could be delayed for years during the reinvestigation gap.

Continuous Evaluation

Executive Order (EO) 12968, Access to Classified Information, as amended by EO 13467 (82 FR 8115), requires Executive Branch agencies to conduct CE pursuant to standards determined by the DNI in his role as the U.S. Government's Security Executive Agent (SecEA). The SecEA established the Continuous Evaluation Program (CEP) within ODNI's NCSC to develop Executive Branch standards for CE, and to oversee the conduct and compliance in implementing CE. Correspondingly, an inter-agency working group known as the CE Working Group (CEWG), led by NCSC, was chartered in July 2015, to promote the development and implementation of CE across the Executive Branch in a widely understood, consistent, and efficient manner.

CE is a personnel security investigative process to review the background of individuals who have been determined to be eligible for access to classified information or to hold a sensitive position. CE will leverage technology to perform automated records checks for personnel security on a more frequent basis. Information from CE will supplement traditional initial and periodic background investigations, not replace them. The same privacy protections that apply to personnel security investigations apply to CE.

There are seven data categories of information required for CE automated record checks. The data sources that will be used to conduct CE are the types of data sources already searched in

[6] Executive Order (EO) 12968, Part 3, Section 3.1(b).
[7] See https://nbib.opm.gov/.

personnel security investigations. The significant change in CE is the frequency of searches that are conducted to verify the continued eligibility of all covered individuals across the United States Government. DHS will provide the foreign travel data.

DHS Solution

Individuals subject to CE include current U.S. Government civilian employees, detailees, contractors, military personnel, and other sponsored individuals who are deemed eligible for access to classified information or to hold a sensitive positon. Those covered individuals are identified for CE by their home agency or department (i.e., the federal entity at which the covered individual is employed).

As a technical service provider, I&A will transfer APIS and BCI data, when available, to a CBP cloud environment. All files will be encrypted while in transit and at rest. I&A will verify that all CBP data have been successfully transferred into the cloud.

Data Storage: I&A will move the CBP data required for TRDS into a CBP cloud environment. Access to the TRDS data in the cloud is limited to a small number of cleared, specially trained system administration personnel from I&A, who act as technical service providers on behalf of CBP.

Data Transfer and Conditioning Process: CBP will transfer historic and transactional APIS and BCI data from the CBP source system(s) for APIS and BCI to the cloud. I&A will assist with this effort, as necessary, as a technical service provider. All files will be encrypted while in transit and at rest. I&A will verify that all CBP data have been successfully transferred to the cloud, and ensure the data has not changed during transmission.

Data Correlation Process: TRDS is triggered on a regular basis by an automated prompt to retrieve a list of the covered individuals from the CES. As a service provider, I&A will use a cloud-based tool to match the biographic information of the list of CE enrollees with the CBP APIS and BCI data. Results that match to covered individuals are then sent back to NCSC's CES. At CBP's request, I&A only sends the APIS and BCI data elements listed in Section 2.1 below to NCSC; it does not send the entire record.

As a service provider, I&A correlates the list of enrollees with APIS and BCI records to determine whether a covered individual (a) traveled or intended to travel abroad, or (b) did not travel or intend to travel abroad. Either way, I&A sends notice of that travel/intent to travel, or lack thereof, to NCSC CES. The significance of a match, if any, will be determined by the covered individual's home department or agency through the CES. Sharing of matches with the home agency will not occur until this program is fully operational. Phase 1 testing is only internal DHS testing of TRDS and phase 2 testing is external testing.

Efficacy of the TRDS Matching Function: As part of the testing and evaluation phases of TRDS, DHS will test the tool used to correlate the DHS and CES data in the cloud and make any necessary configuration changes to ensure it achieves a 90% or higher rate of true matches (i.e., matches that are subsequently validated through human review). DHS has assessed that this rate is appropriate because all potential matches will be subsequently manually evaluated through human review by the investigative entity at the covered individual's home agency. To mitigate the risk that any downstream recipient of TRDS matches will erroneously assume that potential matches have been confirmed - either through technological or manual means - DHS will provide caveat language with all potential matches sent back to the CES indicating that (a) no human validated the match prior to transfer, (b) the absence of a match does not preclude travel, as there may be some border crossings for which CBP does not have information, and (c) that APIS records indicate the mere *intent* to travel, not the fact of travel. Thus, where a TRDS positive match is based solely on an APIS record, the match does not signify a confirmed border crossing.

As technical service providers, I&A personnel will continue to test, quantify, audit, and assess the efficacy of the matching tool throughout the lifecycle of this program. TRDS receives all changes to APIS and BCI data, including corrections and updates. These changes are provided to NCSC's CES system as expeditiously as possible.

Use, Treatment, & Retention of Records: Once the CES receives the response from TRDS, the CES will electronically alert the covered individual's department or agency. On receipt of the electronic prompt, the personnel security function at the sponsoring department or agency follows existing personnel security processes and verifies that the alert or report received pertains to the covered individual. Information obtained through an investigation, if any, is then considered in adjudicating the covered individual's continued eligibility for access to classified information or to hold a sensitive position.

CBP data regarding a covered individual will only be made available to agencies that have an adjudicative interest in the covered individual. I&A personnel, on behalf of CBP, will maintain an accounting of disclosures of CBP records to NCSC through the TRDS process. NCSC CES will maintain a log of all APIS and BCI data disseminated.

The NCSC CES will retain APIS data for one year from origination of the APIS record, which is typically the flight date or record creation date. The NCSC CES will retain BCI data for fifteen years from origination of the BCI record, which is typically the arrival date or record creation date. Departments and agencies may not export CBP data unless such data is determined by the covered individual's sponsoring agency to be relevant to a personnel security investigation or inquiry, to include investigations or inquiries that ultimately lead to a Counterintelligence or Insider Threat investigation or inquiry. In the event CBP data is incorporated into a security, Insider Threat, or Counterintelligence investigation or inquiry case file, the relevant department or agency may retain the CBP data consistent with their records retention legal and policy

requirements, to include any applicable Intelligence Oversight Guidelines. To the extent that a covered individual's home agency requires the full APIS or BCI record associated with a travel event, the home agency will use existing processes to request full the APIS or BCI record from CBP.

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?

Executive Order (EO) 12968, Access to Classified Information, as amended by EO 13467 (82 FR 8115), requires Executive Branch agencies to conduct CE pursuant to standards determined by the Director of National Intelligence (DNI).

Other authorities relating to individuals' qualifications for classified information access or a sensitive position include the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638 (Dec. 17, 2004); the National Security Act of 1947, as amended, 50 U.S.C. 403, et seq.; the Counterintelligence Enhancement Act of 2002, as amended, 50 U.S.C.§ 402b; Executive Order 12333, 46 FR 59941 (1981); Executive Order 13381, 70 FR 37953 (2005); Executive Order 13488, 74 FR 4111 (2009); and Executive Order 13549, 75 FR 51609 (2010).

On July 2, 2016, a Memorandum of Agreement was signed between the ODNI NCSC and DHS that describes the need for DHS to share travel record data with ODNI for CE purposes.

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

The information that TRDS receives from the underlying CBP systems is covered by the SORNs for those source systems, as follows:

- CBP APIS SORN;[8]
- CBP BCI SORN;[9] and
- NCSC Continuous Evaluation System SORN.[10]

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

Yes. TRDS is currently in development and testing. External testing is expected to begin in August 2018. An Interim Authority to Test (IATT) was granted on April 23, 2018, for 150 days.

[8] DHS/CBP-005 Advance Passenger Information System (APIS), March 13, 2015 80 FR 13407.
[9] DHS/CBP-007 Border Crossing Information (BCI), December 13, 2016, 81 FR 89957.
[10] ODNI-13 Security Clearance Reform Research Records, April 2, 2010, 75 FR 16865.

This includes an SSP as well as other required information security documentation. Prior to full deployment, and upon completion of a PIA, TRDS will receive an Authority to Operate (ATO).

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

TRDS will not require a NARA approved record retention schedule. The sources of the travel records (APIS and BCI) remain under CBP control and are covered by the existing NARA retention schedules and SORNs associated with the underlying source systems, APIS and BCI.

Retention Schedule

NCSC CES will retain APIS data for one year from origination of the APIS record, which is typically the flight date or record creation date. NCSC CES will retain BCI data for fifteen years from origination of the BCI record, which is typically the arrival date or record creation date. If there is no match (i.e., the covered individual is not associated with an APIS or BCI record), the CES will store that negative response in accordance with its SORN, NARA schedule, and AG Guidelines. In the event CBP data is incorporated into a security, Insider Threat, or Counterintelligence investigation or inquiry case file, the relevant department or agency may retain the CBP data consistent with its records retention legal and policy requirements, to include any applicable Intelligence Oversight Guidelines. To the extent that a covered individual's home agency requires the full APIS or BCI record associated with a travel event, the home agency will use existing processes to request full the APIS or BCI record from CBP.

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.

While the Paperwork Reduction Act does not apply to the exchange of information using TRDS, it does apply to certain aspects of CBP's original collection of travel records and is covered under the following control numbers:

- OMB 1651-0088 – Passenger and Crew Manifest for Passenger Flights
- OMB 1651-0103 – Passenger List/Crew List
- OMB 1651-0107 – Application for Waiver of Passport or Visa
- OMB 1651-0111 – Arrival and Departure Record

The PRA also applies to certain information collected from individuals for personnel security purposes and includes the following collections:

- OMB 3206-0005 – Standard Form 86, Questionnaire for National Security Positions
- OMB 3206-0191 – Standard Form 85P, Questionnaire for Public Trust Positions

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

TRDS itself does not collect any information. Rather, it uses CBP APIS and BCI records, as well as NCSC CES's list of enrollees, to determine whether an individual is associated with an APIS or BCI record. When such an association exists, I&A as a service provider, discloses relevant portions of the associated APIS or BCI records to the NCSC CES. DHS does not collect any CE enrollee data for this effort; all CE enrollee data is immediately purged from the CBP cloud environment after each correlation between the NCSC and DHS data sets is complete.

The following fields from the covered individual list will be used to conduct the SEARCH of the APIS and BCI data:

APIS biographical fields queried:

- Name (i.e., Last Name, Middle Name, First Name);
- Gender;
- Date of Birth;
- Country of Citizenship;
- Document Type (e.g., passport);
- Document Number (e.g., passport number); and
- Document's Issuance Country (e.g., country that issued the passport).

BCI biographical fields queried:

- Name (i.e., Last Name, First Name, Middle Name);
- Date of Birth;
- Gender;
- Country of Citizenship;

- Document Type (e.g., passport);
- Document's Issuance Country (e.g., country that issued the passport); and
- Document Number (e.g., passport number).

The following fields will be used to create a RESPONSE in the event of a positive match.

APIS:

- Date Of Export;
- Source Country;
- Data Source;
- Passenger;
    - TECS ID: Source system record ID number;
    - Name (i.e., First Name, Middle Name, Last Name);
    - Passenger type;
    - Gender;
    - Date of Birth;
    - Citizenship Country;
    - Embarkation;
    - Debarkation;
    - First arrival airport;
    - CBP embarkation airport;
    - CBP debarkation airport;
    - CBP First Arrival;
    - Airline record locator;
    - Document List;
        - Document;
            - Document type;
            - Number;

- Expiration date;
- Issuance date; and
- Issuance Country.

- Address List;
  - Address;
    - Address type;
    - Building number;
    - Street name;
    - Apartment number;
    - City name;
    - Country name;
    - State code;
    - Postal code; and
    - Residence country.

- Flight;
  - TECS ID: Source system record ID number;
  - Vessel name;
  - Vessel identifier type;
  - Vessel identifier;
  - Vessel registration country;
  - Vessel voyage number;
  - Carrier;
  - Flight Number;
  - Origin airport code;
  - Origin country;
  - Destination airport code;
  - Destination Country;

- Site code;
- Flight Type;
- Flight Date;
- Flight Estimated Time of Departure; and
- Flight Estimated Time of Arrival.

BCI:

- Export Date Time;
- TECS ID: Source system record ID number;
- Name (i.e., Last Name, First Name, Middle Name);
- Date Of Birth;
- Gender;
- Country Of Citizenship;
- Location Code;
- Crossing Date Time;
- Mode of transportation code;
- Travel Direction Code;
- Secondary Examination Status;
- Terminal;
- Lane Number;
- Visa Admission Class Code;
- Visa Admit Until Date;
- Document;
  - Document Number;
  - Document Type Code; and
  - Document Issuing Country Code.
- RFID: Only available if a radio frequency identification (RFID) card is used at

either land or sea. Once CBP systems are modernized, the RFID field will be populated;

- APIS entry;
  - Carrier; and
  - Carrier Route Number.
- Vessel Official Number;
  - Arrival Port Code; and
  - Departure Port Code.
- Vehicle;
  - License Plate Number;
  - License Plate State Code; and
  - Foreign Country Indicator Code.
- Package Result Code;
- Status;
  - API Code;[11]
  - API Onboard Status Code;[12]
  - API Confirmation Status Code;[13] and
  - Process Result Code.[14]
- Package Result Code.[15]

The information in these queries is not maintained or stored in the cloud beyond that temporarily required to perform the matching operations. Once positive results are identified, the response is returned to NCSC and the query results are deleted from TRDS. TRDS will track the positive and negative results shared with NCSC.

[11] Code confirming if the data is APIS.
[12] Whether the individual is crew or non-crew.
[13] CBP generated status code if the API was confirmed. (e.g., "confirmed" or "referred").
[14] The result of processing a person at the land border (e.g., "admit" or "refer").
[15] A code used in the land environment to provide the status of vehicle or person packages.

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

The sources of the information are the CBP APIS and BCI systems, as well as the CES enrollee list, which is produced by NCSC. The CBP APIS and BCI data is not collected solely for use in TRDS, but once collected the data is moved up to a secure cloud environment for processing. While not specifically collected for just TRDS, the CES enrollee data is collected to conduct all CE checks. The CES enrollee data is delivered temporarily to the CBP Cloud environment for correlation with APIS and BCI data. No CES data is retained by DHS.

The information is not collected, but the data is delivered through secure means to an approved enclave. This is being done to verify the self-reporting of covered individuals for CE purposes. These individuals have previously provided consent to access the data.

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

No. TRDS does not use publicly available data.

2.4 Discuss how accuracy of the data is ensured.

TRDS verifies the accuracy of the CBP data throughout the TRDS process through data management services that are available in the cloud environment. These services help I&A ensure that no data is dropped or corrupted during the file extraction, transfer, and loading processes. For example, one such service counts the number of data files in both the APIS and BCI datasets prior to and immediately following transfer to the cloud to ensure that the correct number of files is actually transferred from DHS's network to the cloud environment. Additionally, TRDS will receive updates approximately every four hours from the APIS and BCI source systems. The accuracy of the search algorithm was tested in Phase 1 and will be tested in Phase 2. I&A will validate results through manual review.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of over-collection of PII.

Mitigation: The APIS and BCI data fields have been reviewed to identify the minimum amount necessary to fulfill the NCSC CE technical requirements. In addition, NCSC CES will abide by a relatively short retention period for maintaining the CBP information – one year for APIS and fifteen years for BCI.

Privacy Risk: The data correlation tool may return incorrect travel records to NCSC CES,

providing more information than is required for NCSC's CE mission or inaccurate, nonresponsive information.

Mitigation: Prior to launch of the pilot, the data correlation tool has been rigorously tested and tuned to minimize false positives, initially against synthetic (fake) data. During final system testing, and before approval to operate, the algorithms will be tested and tuned using a control set of known travel events of covered personnel. These travel events will be matched against live data to ensure the same high confidence results (i.e., results at the 90% or higher rate of accuracy) as the development testing against synthetic data. Periodically, privileged users will retest these algorithms and tune them as needed to ensure a continued high level of confidence in the results and to further minimize the number of false positive records provided to NCSC. Finally, in all circumstances, positive matches are subject human review.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

TRDS provides travel record data to the NCSC CES to verify the reported travel of covered individuals. Discrepancies between their reported foreign travel and their actual foreign travel may be indicators requiring further investigation. By consolidating and automating DHS travel record data for external query by the NCSC CES, DHS enables the Personnel Security Offices at each Executive Branch department or agency to perform this discrepancy identification.

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.

No.

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

TRDS will not be accessible by other DHS Components, and they have no roles or responsibilities regarding TRDS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that NCSC CES business rules or the subject's sponsoring agency will misinterpret CBP information due to the complexities in travel data. For example, APIS is only an indication of the intent to travel.

Mitigation: Any NCSC personnel who handle CE information will be required to complete training prior to accessing CE information. This training, the same taken by personnel security professionals, will include significant instruction on how to protect civil liberties and privacy in accordance with the Privacy Act of 1974 and with the Office of Management and Budget directives on protecting Personally Identifiable Information.[16] APIS data will be provided to NCSC with the disclosure that it is only intent to travel.

Privacy Risk: NCSC CES may exceed the data retention period specified by the source system.

Mitigation: Once the NCSC CES acquires travel record data, it will provide the results to the covered individual's sponsoring agency. CES will automatically purge records in accordance with the records retention schedule information – one year for APIS and fifteen years for BCI. The Annex to the MOA between DHS and NCSC provides additional levels of specificity to the July 2016 MOA, specifically regarding retention responsibilities and third party dissemination responsibilities.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

TRDS information is derived from the CBP APIS and BCI data sets. All U.S. Government employees give consent and receive notice on the Standard Form (SF-86, OMB No. 3206 0005) that the foreign travel information provided on the SF-86 form, or equivalent form, will be verified. TRDS is the automated means for verification of foreign travel.

The APIS SORN[17] allows CBP to collect and maintain records on certain biographical information on all passengers and crew members who arrive in, depart from, or transit through (and crew that fly over) the United States on a covered air or vessel carrier, and, in the case of crew members, those who continue domestically on a foreign air or vessel carrier, to additionally encompass private aircraft, rail, and bus travel. Routine Use O of the APIS SORN allows for the sharing of information to a federal agency if the information is relevant and necessary to either the

[16] NCSC Continuous Evaluation Top 15 Frequently Asked Question (FAQ), 3 April 2017, *available at* https://www.dni.gov/files/NCSC/documents/products/20180316-CE-FAQs.pdf.
[17] DHS/CBP-005 Advance Passenger Information System (APIS), March 13, 2015 80 FR 13407.

requesting agency's decision or a DHS decision concerning the issuance of a security clearance.

The BCI SORN[18] describes CBP's collection and maintain records on border crossing information for all individuals who enter, are admitted or paroled into, and (when available) exit from the United States, regardless of method or conveyance. Routine Use Q of the BCI SORN allows for the sharing of information to a federal agency if the information is relevant and necessary to either the requesting agency's decision or a DHS decision concerning the issuance of a security clearance. In addition, once published, this PIA will provide additional notice of the intended use of data prior to collection.

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

Individuals subject to CE include current U.S. Government employees, detailees, contractors, and other sponsored individuals who are deemed eligible for access to classified information or to hold a sensitive positon. Those covered individuals are identified for CE by completion of the OPM Standard Form 86, "Questionnaire for National Security Positions," last revised November 2016. In signing the Standard Form 86 (or equivalent form) for release of information and submission to either an initial or periodic background investigation for the purpose of attaining a security clearance, covered individuals and those applying to become one authorized the U.S. Government to conduct background investigations, reinvestigations, and continuous evaluation.

Individuals have the right to decline to provide data to DHS components, Department of State (DoS), Department of Justice (DOJ), and Department of Defense (DOD), unless they are part of a law enforcement action. However, in doing so, they may become ineligible for any benefits for which they are applying or may become ineligible to hold their current position. The SF-86 informs all U.S. Government employees that providing the information is voluntary. The SF-86 also informs them that if they do not provide each item of requested information, the U.S. Government will not be able to complete the investigation, which will adversely affect their eligibility for a national security position, eligibility for access to classified information, or logical or physical access. Once they have provided the information, individuals have no opportunity to consent to, or refuse, the use of this data for national security, law enforcement, immigration, intelligence, and other homeland security mission-related purposes. The CEP falls within these mission purposes. TRDS automates a system of travel review that is currently done manually by authorized security individuals. TRDS receives queries from the NCSC about persons with security clearances or in sensitive positions that have provided consent for these queries, and automatically matches these queries against DHS travel records.

[18] DHS/CBP-007 Border Crossing Information (BCI), December 13, 2016, 81 FR 89957.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that a covered individual may not be aware that foreign travel information collected directly from the individual on the SF-86, or equivalent form, will be verified (e.g., provided during an application for a benefit or credential) via personnel security officers using the NCSC CES.

Mitigation: The DHS and other U.S. Government agencies mitigate this risk by the public notice through this PIA and the associated SORNs. Signature on the SF-86, or equivalent form, informs the applicant that release of information and submission to either an initial or periodic background investigation for the purpose of attaining a security clearance. Covered individuals, and those applying to become one, authorize the U.S. Government to conduct background investigations, reinvestigations, and CE. The collecting agency provides notice at the point of collection that the information that the applicant provides may be shared with other federal, state, local, and foreign government agencies and authorized organizations following approved routine uses described in the associated published SORNs. The SF-86, or equivalent form, informs the applicant that the information that the individual provides on the form may be confirmed during the investigation, and the investigation may extend beyond the time covered by this form, when necessary to resolve issues.

Privacy Risk: There is a risk that covered individuals, when booking foreign travel, may be unaware that DHS will be sharing that information for CE purposes.

Mitigation: This risk is partially mitigated. DHS is providing general notice through this PIA. Agencies may also choose to provide notice to their employees. Covered individuals are already required to provide most of the information collected to their home agency under SEAD 3. However, there is no direct notice to covered individuals that when booking travel some of the information they provide and notice of that travel will be shared with their home agency.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection

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

TRDS and CES will retain APIS data for one year from origination of the APIS record, which is typically the flight date or record creation date. TRDS and CES will retain BCI data for fifteen years from origination of the BCI record, which is typically the arrival date or record creation date. Departments and agencies may not export CBP data unless such data is determined by the covered individual's home agency to be relevant to a personnel security investigation or inquiry, to include security investigations or inquiries that lead to a Counterintelligence or Insider

Threat[19] investigation or inquiry. In the event CBP data is incorporated into a personnel security, Insider Threat, or Counterintelligence investigation or inquiry case file, the relevant department or agency may retain the CBP data consistent with its records retention legal and policy requirements, to include any applicable Intelligence Oversight Guidelines.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk data may be retained beyond the period specified in the source system.

Mitigation: TRDS will automatically delete records based upon source system retention policies. Specifically, TRDS contains code that automatically deletes APIS records one year from the date in the Flight Date field and BCI records 15 years from the date in the Crossing Date field. These policies will be based on the creation date of the record and TRDS will automatically delete the records. Privileged users will periodically review the system logs to ensure these deletions are occurring accurately and in the appropriate timeframe.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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.

Yes. TRDS will share CBP data with the NCSC CES for the purpose of conducting CE. Once NCSC CES receives a positive match from TRDS, NCSC CES will electronically alert the responsible department or agency. On receipt of a match, the personnel security function at the sponsoring department or agency verifies that the alert or report received pertains to the enrolled individual. When the match is confirmed, appropriate personnel security officials review the nature of the alert to determine the need for further investigation, as dictated by the National Security Adjudicative Guidelines (Security Executive Agent Directive 4)[20] and 2012 Federal Investigative Standards Expandable Focused Investigation requirements. Information obtained though that investigation, if any, is then considered in adjudicating the covered individual's continued eligibility for access to classified information or to hold a sensitive position.

[19] *See* DHS/ALL/PIA-052 DHS Insider Threat Program, *available at* www.dhs.gov/privacy.
[20] *See* http://ogc.osd.mil/doha/SEAD4_20170608.pdf.

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

The external sharing described above is compatible with the original purpose for collection, as permitted by the Privacy Act of 1974 (5. U.S.C. sec. 552a) and pursuant to routine uses published in the APIS[21] and BCI[22] SORNs. This information is shared primarily for the specific purpose of adjudicating personnel security actions. TRDS limits the sharing of source system data, minimizing what is passed to ODNI to only those fields relevant to personnel security activities.

6.3 Does the project place limitations on re-dissemination?

Federal agencies that receive APIS and BCI information are subject to the Privacy Act and may not re-disclose information without clear authority to do so when the information disclosed by DHS is subject to the Privacy Act's protections. TRDS results, which include all the data fields listed in section 2.1, are intended to provide U.S. Government department/agency Personnel Security Offices (PSO) with a holistic view of the individual in question. Results are only shared with the PSO for those individuals who are of interest to their organization for personnel security adjudication actions. DHS has an approved Memorandum of Agreement Annex that provides additional specificity to the re-dissemination of TRDS data by NCSC.

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

DHS I&A maintains audit logs of information shared including information shared with NCSC CES via TRDS, and will conduct periodic audits to ensure source datasets and related PII are being handled and retained in accordance with data policies and protection criteria. The TRDS capability will provide a dashboard capability to assist specifically nominated system administrators to monitor correct operations and ensure no inappropriate or inadvertent access by unauthorized personnel.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that the information shared by DHS is not properly handled and protected, or is misused by the receiving agency.

Mitigation: NCSC is responsible for management and oversight of the CES, and has agreed within the provisions of its MOA with DHS to ensure proper handling and use of the information it receives from DHS, in accordance with its authorities including the subsequent sharing of the information with third parties (i.e., home agencies).

[21] DHS/CBP-005 Advance Passenger Information System (APIS), March 13, 2015 80 FR 13407.
[22] DHS/CBP-007 Border Crossing Information (BCI), December 13, 2016, 81 FR 89957.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to obtain redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals seeking notification of and access to APIS and/or BCI records contained in the underlying source systems of records may submit a request in writing to the CBP Freedom of Information Act (FOIA) officer by mail:

FOIA Officer
U.S. Customs and Border Protection
90 K Street, NW
9th Floor, Mail Stop 1181
Washington, DC 20229

Some of the requested information may be exempt from access pursuant to the Privacy Act or the Freedom of Information of Act (for those individuals who are not U.S. citizens or lawful permanent residents and whose records are not covered by the Judicial Redress Act) in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in TRDS could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension.

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

The opportunity to explain, refute, or clarify may be accomplished via standard home agency processes such as interviews with the home agency investigator.

Additionally, if an individual is concerned the underlying travel record is incorrect, individuals, regardless of citizenship, may submit redress requests online through the DHS Traveler Redress Inquiry Program[23] (TRIP) website, www.dhs.gov/trip, or mail the completed form and documents to DHS TRIP, 601 South 12th Street, TSA-901, Arlington, VA 20598-6901. Completing the form online saves processing time and helps prevent data entry errors. After an individual submits a redress form, the individual will receive notification of receipt from DHS

[23] See the DHS Traveler Redress Inquiry Program Privacy Impact Assessment at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhstrip.pdf.

TRIP. DHS TRIP will review the redress form and will determine which component/agency will be able to respond most effectively to the submission. When a redress request is related to TRDS processing, DHS TRIP will coordinate with TRDS. TRDS will then review the individual's records and correct the information, if appropriate. DHS TRIP will notify the individual of the resolution of that request. Additionally, an individual may submit redress requests directly to the CBP Privacy Officer (See section 7.3). If an individual is dissatisfied with the response to his or her redress inquiry, then he or she can appeal to the DHS Chief Privacy Officer, who reviews the appeal and provides final adjudication concerning the matter. The DHS Chief Privacy Officer can be contacted at Chief Privacy Officer, Attn: DHS Privacy Office, Department of Homeland Security, Mailstop 0655, 245 Murray Lane, SW, Washington, DC 20528, USA; or by fax: 1-202-343-4010.

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

The procedure for submitting a request to correct information is outlined in this PIA and the associated SORNs. As stated above, individuals may submit requests for information and correction as permitted by the Privacy Act and agency policy, which will be reviewed and corrected on a case-by-case basis.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There are risks of a lack of access to information and inability to seek redress and correction.

Mitigation: Redress is available through requests as described above including contacting the CBP FOIA Officer; however, providing individual access or correction of the records may be limited for reasons as expressly permitted by the Privacy Act. The existing redress procedures are adequate to address the individual's right to access and correct their records. However, as stated above, individuals may submit requests for information and correction as permitted by the Privacy Act and agency policy, which will be reviewed and corrected on a case-by-case basis.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

TRDS auditing will occur at the system level. As the only human interaction with the system will be for administrative purposes, privileged user access to TRDS data will be logged and aggregated for independent review. Periodically, privileged users independent of those normally responsible for TRDS systems maintenance will review the audit logs to ensure

compliance with the conditions specified in this PIA and other project relevant security documentation. Any discrepancies will be noted and notification provided to the relevant authorities for follow-up and disposition.

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

TRDS requires no human interaction with the data. However, all technical professionals are required to complete Privacy Act training. The privileged users with access to the TRDS hosting system (system administrators) are all trained to DHS privacy standards for privileged user system access additionally, users will be made aware that APIS data is merely an *intent to travel*. TRDS will depend upon the I&A Chief Information Officer (CIO) controls and monitoring to ensure privileged users are adequately trained and retain currency in their privacy training.

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

TRDS does not provide for user access to the data. Only privileged users (system administrators, etc.) will interact with the system. TRDS will adhere to the broader I&A CIO policies and procedures for privileged user access.

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 proposed modifications to TRDS information sharing will come through DHS I&A CIO Top Secret Program Management Office (TSPMO) for processing. The TSPMO Project Manager will coordinate proposed changes with Office of the Chief Information Officer (OCIO), I&A Privacy, the Oversight & Intelligence Law Division, and the DHS Privacy Office. Because the source information is extracted from CBP systems, the appropriate persons at CBP, such as the CBP Privacy Office and CBP Office of Chief Counsel, will be included in this coordination. Changes to TRDS will occur only after all of these offices achieve consensus and agreement.

Final decisions will be documented and recorded by the DHS I&A CIO TSPMO, on behalf of CBP, and maintained in the appropriate repositories.

Responsible Officials

David Bottom
Chief Information Officer
Office of Intelligence & Analysis
Department of Homeland Security

Approval Signature

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

_____
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security