Privacy Impact Assessment Update
for the

Watchlist Service

DHS/ALL-027(e)

May 5, 2016

Contact Point
Ted Sobel
Deputy Assistant Secretary (A)
Screening Coordination
Threat Prevention and Security Policy
Office of Policy
Department of Homeland Security

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) receives a copy of the Terrorist Screening Database (TSDB), the U.S. Government's consolidated database maintained by the Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Terrorist Screening Center (TSC), to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities. In July 2010, DHS launched an improved method of transmitting TSDB data from TSC to DHS through a service called the DHS Watchlist Service (WLS). WLS maintains a synchronized copy of the TSDB, which contains personally identifiable information (PII) and disseminates TSDB records it receives to authorized DHS Components. DHS is updating this Privacy Impact Assessment (PIA) to add the United States Citizenship and Immigration Services (USCIS) Fraud Detection and National Security-Data System (FDNS-DS) as an authorized recipient of TSDB data via the WLS.

Overview

Homeland Security Presidential Directive 6 (HSPD-6),[1] issued in September 2003, called for the establishment and use of a single consolidated terrorist watchlist to improve the identification, screening, and tracking of individuals known or suspected to be terrorists or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism ("known or suspected terrorists," defined in HSPD-6) and their supporters. TSC maintains the authoritative terrorist watchlist and distributes current terrorist watchlist information from the TSDB to other government agencies, including DHS and its Components.[2]

Since its establishment in July 2010, WLS has allowed TSC and DHS to move away from a manual and cumbersome process of data transmission and management to a more privacy-protective, automated, and centralized process. WLS replaced multiple data feeds from TSC to DHS Components, and supports DHS's ability to more efficiently facilitate DHS mission-related functions such as counterterrorism, law enforcement, border security, and inspection activities.

WLS ensures that DHS has an authoritative, traceable, and reconcilable feed of the TSDB for use in the Department's mission. The objective of DHS WLS is to simplify and standardize the distribution of TSDB data to supported DHS systems via a centralized interface between TSC and DHS. DHS does not manipulate the data within the TSDB feed received by WLS. WLS sends data

[1] Homeland Security Presidential Directive 6 (HSPD-6) (Sept. 2003), *available at* http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf.
[2] The TSC maintains the TSDB to serve as the U.S. Government's consolidated watchlist for terrorism screening information, and has the final decision authority regarding watchlisting determinations.

updates as received by the TSDB to DHS Components that require bulk updates for internal processing. WLS ensures that each DHS Component receives only the formatted records from the TSDB that it is authorized to receive pursuant to the terms of information sharing agreements with FBI/TSC and as authorized by law and consistent with the Component's legal authorities and privacy compliance documentation. WLS is a system-to-system secure connection with no direct user interface.

Reason for the PIA Update

In the initial launch of the WLS in 2010, four DHS Component systems received bulk data updates from the TSDB through the DHS WLS: (1) Transportation Security Administration (TSA) Office of Transportation Threat Assessment and Credentialing; (2) TSA Secure Flight Program; (3) CBP Passenger Systems Program Office for inclusion in TECS; and (4) the U.S. Visitor and Immigration Status Indicator Technology (US-VISIT) program for inclusion in the DHS Automated Biometric Identification System (IDENT).[3] As documented in the WLS PIA Update dated September 7, 2010, DHS determined that two additional components, the Office of Intelligence and Analysis (I&A) and U.S. Immigration and Customs Enforcement (ICE), were authorized to receive TSDB data via the WLS in the form of a computer readable extract (CRE) until such time as these components could make a direct connection to the WLS.[4] On July 19, 2011, DHS determined that CBP's Automated Targeting System (ATS) was authorized to receive TSDB data through the WLS.[5] On December 1, 2014,[6] DHS issued a WLS PIA Update to document a change in the technological infrastructure of IDENT's receipt of TSDB data. Lastly, DHS expanded the WLS feed to include individuals who may pose a threat to national security, consistent with Executive Order 12333 (or successor order) ("national security threats") and who do not otherwise satisfy the requirements for inclusion in the TSDB, as documented in the March 4, 2016 WLS PIA Update.[7]

Consistent with the requirements of the original July 2010 WLS PIA and the terms of the DHS-TSC MOU, DHS must notify TSC prior to adding additional DHS recipients of TSDB data and conduct a PIA accordingly. DHS is updating this PIA to document the approval of USCIS's FDNS-DS[8] as a new, authorized user of the WLS through a direct connection.

USCIS is integrating WLS into its existing screening (i.e., background, identity, and security check) processes used to ensure the integrity of the U.S. immigration system, as required

[3] *See* DHS/ALL/PIA-027 Watchlist Service, *available at* www.dhs.gov/privacy.
[4] *See* DHS/ALL/PIA-027(a) Watchlist Service, *available at* www.dhs.gov/privacy.
[5] *See* DHS/ALL/PIA-027(b) Watchlist Service, *available at* www.dhs.gov/privacy.
[6] *See* DHS/ALL/PIA-027(c) Watchlist Service, *available at* www.dhs.gov/privacy.
[7] *See* DHS/ALL/PIA-027(d) Watchlist Service, *available at* www.dhs.gov/privacy.
[8] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS), *available at* www.dhs.gov/privacy.

by Title 8 U.S.C. § 1101 *et seq*. USCIS developed FDNS-DS[9] to record, track, and manage the screening process, as well as to increase the effectiveness of the U.S. immigration system in combating benefit fraud, protecting the public safety, identifying potential threats to national security, and identifying vulnerabilities that may compromise the integrity of the legal immigration system. As a recipient of TSDB data, FDNS-DS compares TSDB entries to biographic information contained within immigration requests or form submissions in order to identify possible national security concerns. When information in a benefit request or form matches information from the TSDB, FDNS-DS generates a notification that is elevated within FDNS-DS for manual review. An FDNS-DS user conducts a review to determine if further action is necessary as part of the FDNS-DS case management process.

With the addition of FDNS-DS as authorized recipient of TSDB data via the WLS, the privacy risks associated with implementation of WLS remain largely unchanged, as described in the original PIA dated July 14, 2010. WLS improved on the previous manual process by automating the process TSC and DHS use to ensure DHS has the most current watchlist data. This same automated process includes a reconciliation process that ensures that the watchlist data DHS uses in its screening programs is an accurate, timely copy of the TSDB.

Concurrent with this Watchlist Service PIA update, DHS is publishing an update to the FDNS-DS PIA[10] that identifies the privacy risks and mitigation strategies built in the FDNS-DS screening processes, to include screening against the WLS.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

The addition of FDNS-DS as an authorized recipient of TSDB data via the WLS alters the requirements outlined in the original DHS/ALL/PIA-027, dated July 14, 2010, as follows:

Authorities

DHS will continue to receive the same information currently received from TSC, through the FDNS-DS technical connection. Therefore, there are no changes or impacts to the authorities permitting the collection of the TSDB data.

SORN

[9] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS), *available at* www.dhs.gov/privacy.
[10] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS), *available at* www.dhs.gov/privacy.

This use of information is covered under the Use of the Terrorist Screening Database SORN,[11] which was republished in April 2016 to include USCIS FDNS as a recipient of the TSDB via the WLS. USCIS use of the TSDB records is covered by the USCIS Fraud Detection and National Security SORN.[12]

System Security Plan

FDNS-DS was approved for entrance into the DHS Ongoing Authorization Program on August 26, 2014.

Paperwork Reduction Act

The WLS program is not covered by the PRA because there are no forms associated with this collection.

Characterization of the Information

The addition of FDNS-DS as an authorized recipient of TSDB data via the WLS does not change the amount and type of PII collected by the WLS.

Uses of the Information

USCIS uses WLS for screening as part of the background, identity, and security check process described in the FDNS-DS PIA.[13] As a recipient of TSDB data, FDNS-DS compares TSDB entries to biographic information contained within immigration requests or form submissions in order to identify possible national security concerns. When information in a benefit request or form matches information from the TSDB, FDNS-DS generates a notification that is elevated within FDNS-DS for manual review. An FDNS-DS user conducts a review to determine if an administrative investigation should be performed. FDNS-DS also uses the TSDB data to perform entity resolution and to reveal non-obvious relationships among identities.

The uses of the data are outlined in the DHS/USCIS-006 FDNS SORN and are consistent with the uses described in the DHS-TSC MOU. The WLS data transfer will improve the current, manual process by automating the transfer and reconciliation checks of TSDB data, ensuring USCIS screening programs use accurate and timely data, and decreasing the chance of human error, thereby reducing the privacy risks related to data integrity.

[11] *See* DHS /ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records, 81 FR 19988 (Apr. 6, 2016).
[12] *See* DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (Aug. 8, 2012).
[13] *See* DHS/USCIS/PIA-013-02, Fraud Detection and National Security Data System (FDNS-DS), *available at* www.dhs.gov/privacy.

Notice

There are no new privacy risks. This PIA update serves as notice of the new recipient of WLS data. DHS also provides notice through the FDNS SORN and Use of the Terrorist Screening Database SORN, published on April 6, 2016 (81 FR 19988).

Data Retention by the project

There are no new privacy risks. USCIS maintains, separate from WLS, information on a match or possible match with the TSDB and will retain this information in FDNS-DS in accordance with the NARA approved retention schedule [N1-566-08-18] outlined in the FDNS SORN. The FDNS SORN states FDNS records have a retention period of 15 years from the date of the last interaction between FDNS personnel and the individual after which time the record will be deleted from FDNS. The 15-year retention schedule provides FDNS with access to information that is critical to the investigation of suspected or confirmed fraud, criminal activity, egregious public safety, or national security concerns. Upon closure of a case, any information that is needed to make an adjudicative decision (such as a statement of findings report), whether there was or was not an indication of fraud, criminal activity, egregious public safety, or national security concerns, will be transferred to the Alien File (A-File) and maintained in the A-File.

Information Sharing

DHS will share encounter and auditing information consistent with the mechanisms established with the TSC pursuant to the WLS MOU. With this update, TSDB information is incorporated into a FDNS-DS, and USCIS may share the information in accordance with the routine uses for FDNS-DS.

Privacy Risk: There is a risk that USCIS will inappropriately disseminate TSDB information.

Mitigation: DHS has determined that FDNS-DS is authorized and has a need to receive TSDB data. Internal sharing of data is strictly limited to those who have a need to know in order to ensure the integrity of the U.S. immigration system, as required by required by Title 8 U.S.C. § 1101 *et seq*. USCIS governance ensures that users are only granted the privileges and access necessary to perform their job. Any external sharing of data is compatible with the purpose of collection and consistent with the routine uses in the FDNS SORN. There are formal agreements in place that fully outline responsibilities of the parties, security standards, and limits to the use of information, including re-dissemination.

Redress

There are no new privacy risks. Redress procedures have not changed. The DHS Traveler Redress Inquiry Program (TRIP) provides redress for individuals who encounter screening-related travel difficulties.

Auditing and Accountability

Privacy Risk: There is a risk that USCIS will not account for the disclosure of TSDB information from FDNS-DS.

Mitigation: This risk is mitigated because FDNS-DS is the primary case management system used to track all actions related to potential fraud, public safety, or national security concerns and intelligence threats. A record of each disclosure is kept on file, and system audit trail logs are maintained to identify transactions performed by both internal and external users of the system. Further, at the request of DHS, Requests for Information for national security purposes from external entities are coordinated and tracked through the DHS Office of Intelligence and Analysis (I&A) Single Point of Service (SPS).[14]

Responsible Official

Ted Sobel
Deputy Assistant Secretary (A)
Screening Coordination
Threat Prevention and Security Policy
Office of Policy
Department of Homeland Security

Approval Signature

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

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

[14] *See* DHS/ALL/PIA-044 DHS Single Point of Service Request for Information Management Tool, *available at* www.dhs.gov/privacy, for more information.