Privacy Impact Assessment Update
for the
Watchlist Service

DHS/ALL-027(c)

December 1, 2014

Contact Point
Kelli Ann Burriesci
Deputy Assistant Secretary
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) currently uses 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) for identifying information about those known or reasonably suspected of being involved in terrorist activity, in order 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). The WLS maintains a synchronized copy of the TSDB, which contains personally identifiable information (PII), and disseminates it to authorized DHS components. DHS is issuing this privacy impact assessment update to document a change in the technological infrastructure of the DHS Automated Biometric Identification System's (IDENT) receipt of TSDB biometric information and to notify the public that DHS no longer plans to develop the DHS Data Store with Query, previously described in the July 2010 WLS PIA.[1]

Overview

The Homeland Security Presidential Directive 6 (HSPD-6), 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 appropriately suspected to be 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). The TSC maintains the authoritative watchlist and distributes current watchlist information from the TSDB to other government agencies, including DHS and its components.[2]

WLS allows 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 replaces multiple data feeds from the TSC to DHS components to more efficiently facilitate DHS mission-related functions such as counterterrorism, law enforcement, border security, and inspection activities. DHS does not receive any new data as part of the WLS; the system was created for efficiency purposes only.

WLS includes the DHS WLS Data Broker service, which ensures that DHS has an authoritative,[1] traceable, and reconcilable feed of the TSDB for use in the Department's

[1] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_wls.pdf.
[2] http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf.

mission.[3] 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 updates as received by the TSDB to DHS components that require bulk updates for internal processing. The DHS WLS Data Broker ensures that each DHS component receives only the formatted records from the TSDB that they are authorized to receive under the *Memorandum of Understanding between DHS and TSC regarding the Use of Terrorist Identity Information for the Department of Homeland Security Watchlist Service (WLS MOU)* and as authorized by law and consistent with their legal authorities and privacy compliance documentation.

The following four DHS component systems currently receive bulk data updates from the TSDB through the DHS WLS Data Broker service: (1) the Transportation Security Administration (TSA) Office of Intelligence and Analysis;[4] (2) the TSA Secure Flight Program;[5] (3) the U.S. Customs and Border Protection (CBP) Passenger Systems Program Office for inclusion in TECS;[6] and (4) the CBP Automated Targeting System (ATS).[7]

Reason for the PIA Update

DHS is updating this PIA to provide notice that IDENT will receive biometric TSDB data via a direct interface to the TSDB, under the provisions of the WLS MOU. Through this interface, IDENT will have the same capability to exchange terrorism information as the WLS, but with biometric-based identities. As the DHS enterprise biometric service provider, direct sharing of biometric information from the TSDB to IDENT will result in more consistent, timely, and efficient sharing. The automated return of information from subsequent encounters with these individuals to the TSC will help the exchange of biographic and biometric data captured during the encounter process for the purpose of updating the TSDB record.

DHS is also updating this PIA to notify the public that DHS will not pursue the DHS Data Store with Query. The DHS Data Store with Query, as described in the July 2010 WLS PIA, was intended to allow users to perform queries (bulk or individual) against a current copy of the TSDB managed within a DHS server. DHS will not pursue this functionality and has removed this phase from its future strategy because DHS determined the functions of this capability already exist via other DHS services.

The original WLS PIA also contemplated that IDENT would receive a feed from

[3] 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.
[4] DHS/TSA 002 - Transportation Security Threat Assessment System, 79 FR 46862 (Apr. 11, 2014).
[5] DHS/TSA 019 - Secure Flight Records, 78 FR 55270 (Sept. 10, 2013).
[6] DHS/CBP-011 - U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008).
[7] DHS/CBP-006 - Automated Targeting System, 77 FR 30297 (May 22, 2012).

the TSC[8] from the TSDB through the Data Broker service because IDENT is the DHS recipient component system for biometric bulk data updates. However, the technological considerations for establishing a direct connection to share biometric information are considerably different from biographic information. Due to technological complexities (further described below), DHS determined that the most efficient mechanism for IDENT to receive TSDB biometric information is via a direct interface to the TSDB, rather than through an interface to the WLS system. Through the direct interface with the TSDB, IDENT will have the same capability to exchange terrorism information as the WLS, but with biometric-based identities. Receiving data directly from the authoritative source in a near real-time manner will improve IDENT's ability to provide accurate, timely, and authoritative information on known or suspected terrorists to its users. IDENT will continue to adhere to the provisions in the WLS MOU. This direct connection also enables TSC to leverage the full biometric services capabilities in IDENT, as described in the IDENT PIA.[9]

This direct exchange improves upon the existing, semi-manual third-party exchange of biometric terrorist identity information from the TSDB through the FBI Criminal Justice Information System (CJIS) Division's Next Generation Identification (NGI). In practice, this is a cumbersome activity. The direct interface to the TSC eliminates the need for IDENT to receive information from a third party (FBI CJIS NGI.)[10]

DHS has identified a new privacy risk with the direct interface between IDENT and the TSDB. While the direct feed promotes data integrity by allowing DHS to receive the biometric terrorist identifying information directly from the authoritative source, DHS has not identified a robust reconciliation process for the biometric direct feed. The biometric records in the direct feed include very limited biographic information, and DHS is thus limited to comparing only the biometric itself to align with the current reconciliation process[11] for biographic records. To mitigate this new risk, the DHS

[8] DHS/ALL/PIA-027 Watchlist Service PIA (July 14, 2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_wls.pdf.
[9] DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.
[10] Please refer to the original WLS PIA for an explanation of the privacy risks associated with this information sharing effort overall.
[11] *See* DHS/ALL/PIA-027 Watchlist Service PIA (July 14, 2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_wls.pdf. In particular, Section 1.5 states "WLS includes an automated reconciliation process that will provide assurance to the TSC that the WLS has applied the near real-time updates of the TSDB properly, and also that DHS component users of WLS have applied the near real-time updates of the TSDB properly when passed through DHS WLS. During data reconciliation, WLS will look for discrepancies or errors in critical data fields. If there are discrepancies between DHS's WLS and TSC's TSDB, DHS will notify TSC of each discrepancy between the two datasets. Discrepancies will be resolved by the TSC, which will result in the TSC sending updated

Office of Biometric Identity Management (OBIM) and the TSC will generate and share reports at least weekly to compare biometric records and identify inconsistencies. OBIM and TSC will explore the possibility to automate this functionality.

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

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

The Use of the Terrorist Screening Database (TSDB) System of Records[12] and the IDENT[13] SORNs continue to provide SORN coverage for this connection.

Characterization of the Information

As described in the original WLS PIA, Terrorist Watchlist information is sent to DHS using the Terrorist Watchlist Person Data Exchange Standard (TWPDES) terrorist information sharing extensible markup language (XML) standard that conforms to the National Information Exchange Model (NIEM). Because of unique formatting issues of the structure of the biometric model within IDENT, IDENT is unable to receive or process messages in TWPDES format; IDENT instead uses IDENT Exchange Messages (IXM) format. This difference in format contributed to the technological differences for establishing a connection to share biometric information compared with a biographic information feed.

As part of the direct interface between TSDB and IDENT, messages will be sent from TSC in IXM format. DHS will now receive two feeds of data from the TSC: the TWPDES-formatted biographic feed to the WLS system, and the IXM-formatted biometric feed to OBIM for inclusion in IDENT. Both feeds will provide authoritative, traceable, and reconcilable TSDB information, and will have protections in place to ensure that each user system receives only the formatted records from the TSDB it is authorized to use under the WLS MOU.

---

transactions to the WLS. The data reconciliation process will take place periodically and no less than annually, to ensure that data quality is maintained."

[12] DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records, 76 FR 39408 (July 6, 2011).

[13] DHS/NPPD-004 DHS Automated Biometric Identification System (IDENT) System of Records, 72 FR 31080 (June 5, 2007).

The direct connection between IDENT and TSDB does not change the amount and type of PII collected by DHS. Information included as part of the direct feed include:

Biometric data:

- Digital facial image;
- Fingerprints; and
- Iris image.

Biographic data:

- Known or Suspected Terrorist Identifiers;
- Fingerprint Identification Number (FIN);
- Encounter Identification Number (EID);
- National Unique Identification Number (NUIN);
- Organization, Unit, Sub-unit;
- Activity Reason; and
- Activity Type.

Privacy Risk: There is a risk that the information in WLS and IDENT may be untimely or inconsistent with each other because there are two separate feeds of TSDB information coming to DHS.

Mitigation: This risk is partially mitigated because the data is sent from TSDB to WLS and IDENT concurrently and in a near real time environment. DHS will conduct a manual reconciliation at least weekly until OBIM and the TSC can develop an automated process to further mitigate this risk.

Uses of the Information

There are no new privacy risks. IDENT currently uses the existing DHS-DOJ Interoperability[14] to receive biometric terrorism identity information in a semi-manual fashion by way of FBI CJIS NGI. In practice, this is a cumbersome and frequently manual activity. Establishing a direct connection between IDENT and TSDB greatly improves biometric operations because it automates the information exchange and ensures that the biometric information used by DHS is current and accurate.

This direct exchange does not establish any new users of IDENT or TSDB information, but is rather a change in the mechanism in which DHS receives TSDB information. Existing users of IDENT will remain consistent with current protocols and authorities.

[14] *See* DHS/NPPD/PIA-007(b) Biometric Interoperability Between DHS and DOJ Biometric Interoperability Between the U.S. Department of Homeland Security and the U.S. Department of Justice PIA (October 13, 2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_visit_update-b.pdf.

Notice

There are no new privacy risks. This PIA update and the newly published Appendix X to the IDENT PIA[15] provide notice that IDENT will receive TSDB information directly from the TSC. DHS also provides notice through the DHS-wide system of records notice for WLS.[16]

Data Retention by the project

There are no new privacy risks. Although TSDB information will now be provided to IDENT via a direct interface and will maintain messages it receives, IDENT will not retain historical copies of the TSDB. When the TSC adds, modifies, or deletes data from a record in the TSDB, IDENT will receive an accompanying add/modify/delete message in a near real time environment.

If IDENT identifies a possible match to the TSDB data, IDENT will retain the data in accordance with the DHS Automated Biometric Identification System (IDENT) SORN[17] for seventy-five years.

Information Sharing

There are no new privacy risks. DHS will share encounter and auditing information with the TSC pursuant to the WLS MOU. TSC will share terrorism information received from encounters pursuant to the TSC MOU, the Intelligence Reform and Terrorism Prevention Act of 2004, and applicable legal authorities pursuant to current business processes and security measures. The direct connection between IDENT and TSDB does not change the type of information provided from OBIM to the TSC upon match and further defined in the IDENT PIA.

DHS shares information from IDENT on subsequent encounters of TSDB-identified individuals with the TSC under routine use A of the IDENT SORN. Routine use A permits DHS to share information with appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

---

[15] DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA, *available at* www.dhs.gov/privacy.
[16] DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records, 76 FR 39408 (July 6, 2011).
[17] DHS/USVISIT-004 - DHS Automated Biometric Identification System (IDENT), 72 FR 31080 (June 5, 2007).

In instances in which TSDB information is incorporated into a DHS system, DHS shares the information in accordance with the routine uses for DHS source system's SORN.

Redress

There are no new privacy risks. Redress procedures have not changed.

Auditing and Accountability

There are no new privacy risks. Auditing and accountability measures have not changed.

Responsible Official

Kelli Ann Burriesci
Deputy Assistant Secretary
Screening Coordination
Threat Prevention and Security Policy
Office of Policy
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security