Privacy Impact Assessment Update
for the
Watchlist Service

DHS/ALL-027(b)

July 19, 2011

Contact Point
Justin Matthes
Director, Information Screening Policy
Screening Coordination Office
Office of Policy
Department of Homeland Security

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) currently uses the Terrorist Screening Database (TSDB), a consolidated database maintained by the Department of Justice Federal Bureau of Investigation Terrorist Screening Center (TSC) that contains 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 new service called the "DHS Watchlist Service" (WLS). At that time, DHS published a privacy impact assessment (PIA) to describe and analyze privacy risks associated with this new service. 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 add the U.S. Customs and Border Protection (CBP) Automated Targeting System (ATS) as an authorized recipient of TSDB data via the WLS.

Introduction

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). Currently, the TSC distributes the watchlist information from the TSDB to other government agencies, including DHS and DHS's internal components.

WLS allows TSC and DHS to move away from a manual and cumbersome process of data transmission and management to an 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. At this time, WLS is a system-to-system secure connection with no direct user interface.

WLS is currently in its initial phase of implementation and includes the DHS WLS Data Broker, which ensures that DHS has an authoritative, traceable, and reconcilable mirror of the TSDB for use in the Department's mission. WLS serves as a main repository, feeding data to downstream DHS components. DHS will not manipulate the data within the TSDB mirror received by WLS. The WLS will send 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 which they are authorized to use under the DHS-TSC Memorandum of Understanding (MOU) and as authorized by law and consistent with their legal authorities and privacy compliance documentation. ATS will receive TSDB data via the DHS WLS Data Broker through a direct connection to the WLS.

DHS Users of WLS

In the initial launch of the WLS, four DHS component systems transitioned to receiving bulk data updates from the TSDB through the DHS WLS Data Broker service (1) the Transportation Security Administration (TSA) Office of Transportation Threat Assessment and Credentialing; (2) the TSA Secure Flight Program; (3) the 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). 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 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. Since that time, DHS has determined that CBP's ATS is now authorized to receive TSDB data through the WLS; ATS is described further in DHS/CBP-006 – Automated Targeting System, August 6, 2007, 72 FR 43567.

Privacy Risks Identified with Additional DHS recipients of WLS

With the addition of ATS as authorized recipients of TSDB data via the WLS, the privacy risks associated with implementation of the WLS remain unchanged as described in the original PIA dated July 14, 2010. WLS improves on the current 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.

Reason for the PIA Update

Consistent with the requirements of the 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 privacy impact assessment accordingly. DHS is updating the WLS PIA and accompanying SORN to provide transparency into the addition of ATS as an authorized recipient of TSDB data via the WLS. Privacy risks associated with implementation of the WLS remain unchanged by the addition of this CBP recipient system.

Additionally, DHS has published a DHS-wide system of records notice for the WLS, DHS/All-030 Use of the Terrorist Screening Database, published on July 6, 2011 (76 FR 39408) in order to provide additional transparency to the uses of TSDB.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

The addition of ATS 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 System and the Information

Uses of the WLS remain unchanged by the addition of ATS as a recipient of TSDB data. The uses outlined in the DHS/CBP-006 ATS SORN are consistent with the uses described in the DHS-TSC MOU.

Retention

Retention plans for the WLS remain unchanged from the July 2010 PIA. The DHS component that is using the TSDB data will maintain, separate from the WLS, information on a match or possible match with the TSDB and will retain this information in accordance with the appropriate DHS SORN: DHS/CBP-006 ATS.

Internal Sharing and Disclosure

DHS has 1) determined that ATS is authorized and has a need to receive TSDB data; 2) notified TSC consistent with the terms of the DHS-TSC MOU; 3) determined that the necessary SORN is in place to receive TSDB data. Accordingly, with the approval of this PIA, DHS is adding ATS as an authorized recipient of TSDB data via the WLS.

External Sharing and Disclosure

The potential privacy risks of improper external sharing are mitigated by having an appropriate SORN in place for ATS that identifies routine uses by which external sharing may occur. TSDB data incorporated into the ATS system of records may be shared externally consistent with the routine uses defined in applicable DHS/CBP-006 ATS.

Notice

This PIA serves as notice of the new recipient of WLS data as well as the DHS/CBP-006 ATS SORN. Additionally, DHS has published a DHS-wide system of records notice for the WLS, DHS/All-030 Use of the Terrorist Screening Database, published on July 6, 2011 (76 FR 39408). During the routine biennial review process, DHS will update this SORN with new users, including ATS.

Individual Access, Redress, and Correction

Individual access redress and correction procedures remain unchanged with the addition of ATS as an authorized recipient of TSDB data via the WLS. Pursuant to a Privacy Act request, individuals can access information they have provided to DHS. Privacy Act requests for access to an individual's record must be in writing and may be addressed to the DHS FOIA/PA, The Privacy Office, U.S. Department of Homeland Security, 245 Murray Drive SW, STOP-0550, Washington, DC 20528-0550 or to TSA, CBP, US-VISIT, I&A, or ICE, if the individual knows which component holds the record. Requests should conform to the requirements of 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS. The request should include a description of the records sought, the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received. After conferring with the appropriate component or agency, the agency may waive applicable exemptions in appropriate circumstances where it

would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained. WLS will not make available information on the individual that were not supplied by that individual, such as watchlist matching results or analyses.

Technical Access and Security

Technical access and security risks remain unchanged with the addition of ATS as an authorized recipient of TSDB data via the watchlist.

Technology

The technology employed by the WLS remains unchanged by the addition of ATS as an authorized recipient.

Responsible Official

Justin Matthes
Director, Transborder Screening Initiatives
Screening Coordination Office
Office of Policy
Department of Homeland Security

Approval Signature

Final signed version on file with the Privacy Office.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security