Privacy Impact Assessment Update
for the

Watchlist Service

September 7, 2010

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

Reviewing Official
John Kropf
Deputy 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 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 identify two additional authorized DHS recipients of TSDB data via the WLS in the form of a computer readable extract (CRE): the Office of Intelligence and Analysis (I&A) and the U.S. Immigration and Customs Enforcement (ICE).

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 to protect the United States as described above. 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. The two additional authorized recipients, I&A and ICE, will receive TSDB data via the DHS WLS Data Broker in the form of a CRE until such time as a direct connection to the WLS can be made.

DHS Users of WLS

In the initial launch of the WLS, four DHS component systems are scheduled to transition 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 U.S. Customs and Border Protection (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). Since publication of the July 2010 PIA, DHS has determined that two additional components, I&A and ICE, are authorized to receive TSDB data via the WLS in the form of a CRE until such time as these components can make a direct connection to the WLS. Initially, the data sent and maintained in the WLS and then transferred to the I&A and ICE systems through the WLS will be covered by applicable SORNs: (1) I&A Enterprise Records System, DHS/IA-001 May 15, 2008, 73 FR28128, and (2) ICE External Investigations, DHS/ICE-009 January 5, 2010, 75 FR 404.

Privacy Risks Identified with Additional DHS recipients of WLS

Privacy risks associated with implementation of the WLS remain largely unchanged with the addition of I&A and ICE as authorized recipients of TSDB data via the WLS. 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. There are some additional

privacy risks presented by the transmission of TSDB data via the WLS Data Broker in the form of a CRE to I&A and ICE on an ad hoc basis versus a direct connection to WLS Data Broker. Specifically, the currency of the watchlist data will be dependent on the frequency of the ad hoc transmissions to the program. DHS has determined that the currency of the data is not as significant a risk to privacy in these instances because I&A and ICE are using the data for analytical and not screening purposes. This allows I&A and ICE personnel to validate the watchlist information by querying against other DHS systems that contain more current TSDB data, such as TECS, before any actions are taken that would affect an individual. In addition, DHS has determined that ad hoc transmissions to I&A and ICE represent a significant improvement upon previous processes. Furthermore, to mitigate privacy risks associated with CREs, TSDB transmissions to I&A and ICE will be subject to the requirements of *DHS Sensitive Systems Security Policy 4300A* for ad hoc CREs. Among other things, 4300A requires that ad hoc CREs be documented, tracked, and validated every 90 days after their creation to ensure that their continued authorized use is still required or that they have been appropriately destroyed or erased. In addition the policy requires ad hoc CREs to be destroyed or erased within 90 days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data is required to be documented by the Data Owner and audited periodically by the Component Privacy Officer or Privacy Point of Contact (PPOC).

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 update privacy documentation accordingly. DHS is updating the WLS PIA and accompanying SORN to provide transparency into the addition of two authorized recipients, I&A and ICE, of TSDB data via the WLS. Privacy risks associated with implementation of the WLS remain largely unchanged by the addition of these two components.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

The addition of I&A and ICE as authorized recipients of TSDB data via the WLS do 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 I&A and ICE as recipients of TSDB data The uses outlined in the DHS/IA-001 ERS and DHS/ICE-009 External Investigations SORN are consistent with the uses described in the DHS-TSC MOU. While TSDB data is used by the existing four DHS component in support of a screening function, I&A and ICE will use TSDB data for analysis purposes; no immediate action will take place until research has been completed and the component verifies that the individual subject to the analysis is the same individual on the TSDB and confirms the most current information available on the TSDB.

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: (1) DHS/IA-001 ERS (2) DHS/ICE-009 External Investigations. In addition, TSDB data transmitted via the WLS as a CRE will be retained in accordance with DHS Sensitive Systems Security Policy 4300A, which requires ad hoc CREs to be destroyed or erased within 90 days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data is required to be documented by the Data Owner and audited periodically by the Component Privacy Officer or PPOC.

Internal Sharing and Disclosure

DHS has 1) determined that I&A and ICE are authorized and have a need to receive TSDB data; 2) notified TSC consistent with the terms of the DHS-TSC MOU; 3) determined that necessary SORNs are in place to receive TSDB data. Accordingly, with the approval of this PIA, DHS is adding two additional authorized components, I&A and ICE, as recipients of TSDB data via the WLS.

External Sharing and Disclosure

The potential privacy risks of improper external sharing are mitigated by having appropriate systems of records identified for I&A and ICE that identify routine uses by which external sharing may occur. TSDB data incorporated into I&A and ICE systems of records may be shared externally consistent with the routine uses defined in applicable SORNs: DHS/IA-001 ERS and DHS/ICE-009 External Investigations.

Notice

This PIA serves as notice of the new recipients of WLS data as do the DHS/IA-001 ERS and DHS/ICE-009 External Investigations SORNs.

Individual Access, Redress, and Correction

Individual access redress and correction procedures remain unchanged with the addition of I&A and ICE as authorized recipients 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

There are some additional privacy risks presented by the transmission of TSDB data via the WLS Data Broker in the form of a CRE to I&A and ICE on an ad-hoc basis versus a direct connection to the WLS Data Broker. Specifically, the currency of the watchlist data will be dependent on the frequency of the ad hoc transmissions to the program. DHS has determined that the currency of the data is not as significant a risk to privacy in these instances because I&A and ICE are using the data for analytical and not screening purposes. This allows I&A and ICE personnel to validate the watchlist information by querying against other DHS systems that contain more current TSDB data, such as TECS, before any actions are taken that would affect an individual. In addition, DHS has determined that ad hoc transmissions to I&A and ICE represent a significant improvement upon previous processes. While use by the existing four DHS component is in support of a screening function, I&A and ICE use of TSDB data will be for analysis purposes; no immediate action will take place until research has been completed and the component verifies that the individual subject to the analysis is the same individual on the TSDB, and confirms the most current information available on the TSDB. Furthermore, to mitigate privacy risks associated with CREs, TSDB data transmissions to I&A and ICE will be subject to the requirements of *DHS Sensitive Systems Security Policy 4300A*. Among other things, this policy requires that ad hoc CREs must be documented, tracked, and validated every 90 days after their creation to ensure that their continued authorized use is still required or that they have been appropriately destroyed or erased. In addition the policy requires ad hoc CREs to be destroyed or erased within 90 days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the Data Owner and audited periodically by the Component Privacy Officer or PPOC.

Technology

The technology employed by the WLS remains unchanged by the addition of I&A and ICE as authorized recipients. The WLS Data Broker will transmit TSDB data to I&A and ICE on an ad hoc basis in the form of a CRE until such time as a direct connection between the component and the WLS can be achieved.

Responsible Official

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

Approval Signature

Original signed copy on file with the DHS Privacy Office

John Kropf
Deputy Chief Privacy Officer
Department of Homeland Security