Privacy Impact Assessment
for the

Watchlist Service

July 14, 2010

Contact Point
Justin Matthes
Director, Transborder Screening Initiatives
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) of 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. DHS and TSC are improving the current method of transmitting TSDB data from TSC to DHS. Through a new service called the "DHS Watchlist Service" (WLS), TSC and DHS will automate and simplify the current manual process. TSC remains the authoritative source of watchlist data and will provide DHS with near real-time synchronization of the TSDB. DHS will ensure that each DHS component system receives only those TSDB records which they are authorized to use under the WLS Memorandum of Understanding and authorized under existing regulations and privacy compliance documentation between TSC and DHS (WLS MOU) and any amendments or modifications thereto. DHS conducted this privacy impact assessment (PIA) because the WLS will maintain a synchronized copy of the TSDB, which contains personally identifiable information (PII), and disseminate it to authorized DHS components.

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

WLS will allow TSC and DHS to move away from a manual and cumbersome process of data transmission and management to an automated and centralized process. WLS will replace 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 will 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.

Implementation of the WLS

During the initial phase of implementation, WLS will include the DHS WLS Data Broker, which will ensure 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 will serve 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 will ensure that each DHS component receives only the formatted records from the TSDB which they are authorized to use under the WLS MOU and as authorized by law and consistent with their legal authorities and privacy compliance documentation.

In the next phase of implementation, WLS will include the DHS WLS Encounters Data Broker which will provide a central mechanism to send and receive designation and encounter information from DHS components back to the TSC. In the current environment, when a DHS component encounters a potential match to the TSDB, a report of that encounter is sent back to the TSDB via system-generated message or manually, by secure phone or secure fax. The major common services of the DHS WLS Encounters Data Broker will include the design, development and implementation of bilateral, standardized information transmission from each DHS system to the TSC of the results from an encounter of a person listed in the TSDB. Once implemented, the WLS will maintain and retain information on encounters.

In its later stages of implementation, the WLS will include the design, development, and implementation of DHS Data Store with Query, which will provide a persistent data store of the TSDB within a DHS server. This phase will allow authorized users to perform queries (individual or bulk) against the persistent data store of the TSDB.

WLS Governance

To support the WLS effort, DHS is employing a stewardship model with the DHS Screening Coordination Office (SCO) serving as the WLS business steward and CBP serving as the technical steward. As business steward, the SCO is responsible for managing the screening mission and DHS component system data requirements/agreements. As the technical steward, CBP is responsible for implementing a streamlined, automated watchlist feed to the DHS components authorized to receive watchlist data. Additionally, the DHS Office of the Chief Information Officer (OCIO) will assist with initial requirements and project management.

DHS Users of WLS

All respective PIAs and System of Records Notices (SORNs) document the authorized set of data elements provided to each component screening programs (see Appendix A) that use the TSDB. There are four anticipated DHS component systems slated for the receipt of the bulk data updates from the TSDB through the DHS WLS Data Broker service. The DHS component systems that will receive data updates from the TSC through the DHS WLS Data Broker are managed by the following program offices: (1) the Transportation Security Administration (TSA)Office of Transportation Threat Assessment and Credentialing at TSA; (2) 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 into the DHS Automated Biometric Identification System (IDENT). If DHS systems are added to receive TSC data, DHS will notify TSC and this PIA and accompanying SORN will be updated accordingly.

TSDB data within the WLS is a near real-time, synchronized mirror of TSC's TSDB. As TSC makes changes to the TSDB, the WLS will echo those changes. When the TSC adds, modifies, or deletes data from the TSDB, the WLS version of TSDB will be automatically synchronized. DHS will not make any changes to the watchlist data in the WLS; these changes will be made automatically when TSC sends updated data. Initially, the data sent and maintained in the WLS and then transferred to the DHS component systems through the WLS will be covered by the SORN for each of those programs: (1) TSA Office of Transportation Threat Assessment and Credentialing, Transportation Security Threat Assessment System DHS/TSA 002, May 19, 2010, 70 FR 28046; (2) TSA Secure Flight Program, Secure Flight Records DHS/TSA 019, November 9, 2007, 72 FR 63711; (3) CBP Passenger Systems Program Office for inclusion in TECS, U.S. Customs and Border Protection TECS DHS/CBP-011 December 19, 2008 73 FR 77778; and (4) US-VISIT program for inclusion into the DHS IDENT DHS/USVISIT-0012, June 5, 2007, 72 FR 31080. In order to provide additional transparency, DHS will also publish a SORN covering DHS's maintenance of the mirror copy of the TSDB for the WLS for publication in the *Federal Register*. This PIA and any applicable

SORNs will be updated if additional systems are given access to the WLS. In addition, DHS will update this PIA and the WLS SORN and file an appropriate records retention schedule for the retention of encounter information before the DHS WLS Encounters Data Broker functionality becomes available.

Privacy Risks Identified with 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. Once DHS has a near real-time mirror of the TSDB, a potential privacy risk could arise in that DHS could use or share TSDB data beyond the scope of TSC's approval. This overall risk is mitigated by the WLS MOU which requires DHS to notify TSC before TSDB data is provided via WLS to additional DHS programs. This risk is also mitigated by the robust audits of actual use of the data which will be performed by TSC and DHS components, as well as through SCO's business stewardship.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

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). The TWPDES messages will provide biographical and biometric data of known or suspected terrorists for the purposes of national security. Information collected includes:

- name,
- date of birth,
- place of birth,
- biometric and photographic data,
- passport and/or driver's license information, and
- other available identifying particulars used to compare the identity of an individual being screened with a known or suspected terrorist.

In addition, WLS will maintain unique identifiers showing the components it has disseminated the information to in order to maintain an audit log.

1.2 What are the sources of the information in the system?

The source of the information for the WLS is the TSC's TSDB. The WLS data will be a mirror of the TSDB, updated in near real time. The WLS will not commingle any other data, including commercial data, with TSDB data and will not add, modify, or delete TSDB data, unless changes to the TSDB are made.

1.3 Why is the information being collected, used, disseminated, or maintained?

Data collected, retained, and disseminated by WLS is intended for use by authorized DHS component systems to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities. TSDB data, which includes personally identifiable information (PII), is necessary for DHS to effectively and efficiently assess the risk and/or threat posed by a person or their related goods and cargo entering or exiting the country.

TSC is providing a near real-time, synchronized version of the TSDB in order to improve the timeliness and governance of watchlist data exchanged between TSC and DHS and within the DHS component systems that use watchlist data.

1.4 How is the information collected?

DHS will receive TSDB data in a single feed from TSC. This feed will consist of TWPDES-formatted watchlist identity-level messages to DHS. The WLS will provide an authoritative, traceable, and reconcilable mirror of the TSDB and ensure that each DHS component receives only the formatted records from the TSDB they are authorized to use under the WLS MOU between TSC and DHS or any amendments thereto.

1.5 How will the information be checked for accuracy?

DHS does not control the accuracy of the information within the watchlist. Nevertheless, DHS has instituted processes within the WLS to ensure the information is a mirror of the information maintained by TSC. When TSC transmits a message, WLS validates the data by checking field lengths and verifying that the data within those fields is in the proper format and that the information originated from TSC, the authoritative source.

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

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

HSPD-6, dated September 16, 2003, requires the Attorney General to establish an organization to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of watchlist information in screening processes. Simultaneously with the issuance of HSPD-6, a Memorandum of Understanding on the "Integration and Use of Screening Information to Protect against Terrorism" (the TSC MOU) was signed establishing the TSC. The TSC created the TSDB in order to meet this goal.[1] The DHS Office of the Chief Information Officer (OCIO) has implemented the Watch List Technical Integration-Integrated Shared Services Project and tasked the project team with establishing the WLS.

The delivery of WLS data across interfaces existing between TSC and DHS is governed by the WLS MOU between TSC and DHS and associated Interface Control Documents and Interconnection Security Agreements. Audits of the use of WLS data by other organizations are performed by CBP Security personnel, in coordination with TSC, during routine certification and accreditation (C&A) activities or at TSC's request. Because TSC manages the authoritative version of the TSDB, WLS will defer to TSC to resolve any discrepancies revealed during regular and intermittent data reconciliation processes.

DHS's authority to maintain WLS and use the TSDB include the following:

- Homeland Security Act of 2002, Pub. L. 107- 296;
- 5 U.S.C. § 301;
- The Tariff Act of 1930, as amended;
- The Immigration and Nationality Act, as amended;
- 49 U.S.C. §§ 114, 5103a, 40113, ch. 49 and 46105;
- Homeland Security Presidential Directive 6, "Integration and Use of Screening Information to Protect Against Terrorism;"
- Homeland Security Presidential Directive 11, "Comprehensive Terrorist-Related Screening Procedures;" and
- Executive Order 12333, "Further Strengthening the Sharing of Terrorism Information to Protect Americans."

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

In the current environment, a standard integration mechanism does not exist between the TSDB and DHS systems. As such, TSC and DHS employees must repeat manual steps to produce and deliver the

[1] The Homeland Security Act of 2002, Pub. L. 107-296 (Nov. 25, 2002); the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (Dec. 17, 2004); Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," (Oct. 25, 2005).

data extracts required by the DHS component systems. This lack of automation presents the risk for unintentional errors to be introduced in the processing of data, and increases the risk that the TSDB data used by DHS is not synchronized with the authoritative source, the TSDB. The WLS process will improve the current manual process by automating the transfer and reconciliation checks of the watchlist data, thereby reducing the privacy risks related to data integrity.

In centralizing the receipt of the TSDB, there is a risk that one component could receive more information than it is entitled to under the MOU. This risk is mitigated by the inclusion of administrative access controls and improved oversight of the distribution of the TSDB. Administrative controls include background investigations, secure logins, annual privacy training, security training, etc. for individuals accessing data, and audits. See section 8.1.

WLS will produce and maintain auditing information which will track messages received from the TSC and delivered to DHS components. WLS will provide this information to the TSC to compare and verify data to ensure the accuracy of WLS data. Only administrators have direct access to WLS data. All administrators have successfully completed the DHS Privacy Awareness course and are subject to an annual refresher. All data is transmitted through an encrypted network that is Federal Information Processing Standard (FIPS 140-2) compliant. WLS will further secure the information to DHS component systems using the National Institute of Standards and Technology (NIST) approved transport layer data encryption.

WLS will be built and certified as part of the CBP Enterprise Service Bus (ESB) and will inherit the ESB security controls, as discussed in section 8.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

DHS components will use the TSDB for screening purposes in the same way as currently outlined in their existing privacy documentation. The WLS will not change the uses, but will change the method by which the systems receive watchlist information. When received, DHS components use watchlist information to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities. In particular, DHS uses watchlist information to assess risk and/or threats posed by individuals in the conduct of the components' missions, such as screening individuals flying domestically or into or out of the United States, determining whether an individual meets the criteria for a particular immigration or naturalization benefits, and investigating immigration and customs violations, as outlined in the Homeland Security Act. Additional DHS systems and programs may be added subject to the requirements of the WLS MOU. In addition, this PIA will be updated to reflect such changes if and when they occur.

With respect to policy concerns, the SCO will manage the type of feed the downstream component systems will receive based on the screening needs of the system and the authorized uses as specified in the WLS MOU. WLS, operated by CBP for DHS, will distribute TSDB information obtained from the TSC to DHS components. Based on computer access profiles, downstream DHS components will only access TSDB data as authorized and approved under the WLS MOU.

In addition, WLS will produce and maintain audit information. The audit information will be used to identify and reconcile errors during the transmission of the watchlist as they arise, as well as to perform manual reconciliation efforts between systems.

2.2 What types of tools are used to analyze data and what type of data may be produced?

WLS will consist of three separate services: The DHS WLS Data Broker service will enable TSC to send watchlist data near real time to DHS, the DHS WLS Encounter Data Broker will enable DHS to send encounter data back to TSC and, the DHS WLS Data Store with Query service, will further improve the process and processing of DHS component systems using watchlist data. The DHS WLS Encounter Data Broker and DHS WLS Data Store with Query service will be rolled out in future WLS releases. The DHS WLS Encounters Data Broker will provide a central mechanism to send and receive designation and encounter information from DHS Components and programs back to the TSC. This will enable DHS to transmit encounter data electronically to TSC. The DHS WLS Data Store with Query service will be designed to ensure that queries against the data stores can be executed using minimum Core Biographic Person Data Elements (see Appendix B). It will be developed to ensure the support of controlled access to the queries based on screening requirements for the DHS components and programs as agreed to with the TSC. As DHS develops these future services, this PIA will be updated.

DHS WLS Data Broker

The first set of major common services includes the design and development of the DHS WLS Data Broker to ensure that DHS has an authoritative, traceable and reconcilable version of the TSDB for use by DHS components as part of their respective missions. The mirror of the TSDB received through the DHS WLS Data Broker will be kept intact and unmodified by WLS. DHS will not manipulate the data within the mirror of TSDB received by WLS. The WLS will send the data updates as received by the TSDB to DHS component systems that require bulk updates for internal processing. The DHS WLS Data Broker will ensure that each DHS component system receives only the formatted records from the TSDB for which they are authorized to use.

The DHS WLS Data Broker services will include automation of the processes and procedures needed to ensure the optimization of data reconciliation between the TSC and DHS. Automated reconciliation will provide assurance to the TSC that the WLS has properly applied the near real-time updates of the TSDB at DHS, and also that the DHS component systems properly applied the near real-time updates of the TSDB when passed through DHS WLS Data Broker.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

WLS does not utilize commercial or publicly available data and will not comingle TSC data with commercial or publicly available data for any purpose.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

In order for the WLS to be successful, DHS must be able to control access to the data to those approved in accordance with the WLS MOU between TSC and DHS. The receipt of TSDB information by additional DHS systems will be authorized subject to the requirements of the WLS MOU. Implementation of WLS and the layers of the centralized administrative controls will provide greater privacy controls than the current manual process. DHS/SCO will oversee all access to the TSDB data through the WLS. There is a possible risk that once DHS has a mirror of the TSDB, DHS could use or share that data beyond the scope of TSC's approval. This overall risk is mitigated by agreements stated in the WLS MOU, which references and governs individual component systems, and is supported by the ability to audit actual use of the data, as well as through SCO's business stewardship of the WLS.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

WLS retains all information defined in Section 1.1 of this Privacy Impact Assessment (PIA) in accordance with the applicable DHS SORN, based on the needs of the program. When the TSC adds, modifies, or deletes data from the TSDB, WLS will exactly mirror those updates.

3.2 How long is information retained?

WLS will maintain a near real-time mirror of the TSDB, and will not retain historical copies of the TSDB. WLS will be synchronized with the TSDB. When the TSC adds, modifies, or deletes data from the TSDB, WLS will perform these functions almost simultaneously. The DHS component that is screening individuals 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) TSA Office of Transportation Threat Assessment and Credentialing, Transportation Security Threat Assessment System DHS/TSA 002, May 19, 2010, 75 FR 28046 identifies seven years for possible matches and ninety nine for confirmed matches;

(2) TSA Secure Flight Program, Secure Flight Records DHS/TSA 019, November 9, 2007, 72 FR 63711 proposed to NARA the following retention schedule seven years for possible matches and ninety nine years for matches;

(3) in the CBP Passenger Systems Program Office for inclusion in TECS, U.S. Customs and Border Protection TECS DHS/CBP-011 December 19, 2008 73 FR 77778 for seventy five years or the life of the law enforcement matter; and

(4) the US-VISIT program for inclusion into the DHS Automated Biometric Identification System (IDENT) DHS/USVISIT-0012, June 5, 2007, 72 FR 31080 for seventy five years.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention schedule has been approved for CBP,US-VISIT, and TSA.

3.4 Privacy Impact Analysis: Given the purpose for retaining the information, explain why the information is needed for the indicated period.

There is a privacy risk that results if DHS retains TSDB data longer than TSC would retain that same data. This risk is mitigated by WLS's mirroring of the TSDB itself. When TSC adds, modifies, or deletes a record, WLS will synchronize with these TSDB actions. Because TSC manages the authoritative source of terrorist watchlist data, WLS will defer to TSC to resolve any discrepancies revealed during regular and intermittent data reconciliation processes. WLS will engage in periodic, automated data reconciliation with TSC to ensure the accuracy and consistency of WLS data and repeat this process with each downstream component.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Terrorist watchlist data will be shared with all DHS systems that have a legacy arrangement with TSC for access to TSDB data. The DHS WLS Data Broker will not transmit TSC data to additional DHS systems without prior notification to the TSC. Component systems that currently receive data directly from TSC will receive the same data via WLS.

The four DHS component systems to receive TSDB data via the WLS will be: (1) TSA Office of Transportation Threat Assessment and Credentialing; (2) TSA's Secure Flight Program; (3) the CBP Passenger Systems Program Office for inclusion in TECS; and (4) the US-VISIT program for inclusion into the IDENT.

4.2 How is the information transmitted or disclosed?

WLS will receive TWPDES messages from the TSC and distribute parsed subsets of that data to subscribed DHS component systems within DHS, as approved by DHS SCO, consistent with the WLS MOU, and the component's DHS mission-related functions. All electronically transmitted data will be exchanged via a secure message interface with message traffic exchanged over routed and point-to-point network facilities. WLS will further secure the information to DHS component systems using National Institute of Standards and Technology (NIST) approved transport layer data encryption.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

One privacy risk is that DHS components will receive data through WLS they are not authorized to receive. This risk is mitigated through SCO's policy oversight and CBP's technical stewardship of the access process. In the initial phase, only DHS systems that currently receive this data would receive it through WLS. As additional DHS systems are identified, the WLS MOU will be amended. Only authorized DHS systems will receive feeds through WLS.

A second privacy risk is DHS components that do receive the WLS feed may receive data that exceeds their authorized levels in the WLS MOU. This risk is also mitigated by policy guidance from SCO and CBP control over the internal feeds to DHS systems and the WLS MOU with TSC. Only authorized data elements will pass through WLS to DHS components.

WLS will distribute parsed subsets of the mirrored 'master' data to authorized DHS component systems within DHS, as approved by DHS SCO in coordination with TSC as determined by the needs of the component's DHS mission-related functions. All electronically transmitted data will be exchanged via a secure message interface with message traffic exchanged over routed and point-to-point network facilities. WLS will further secure the information to DHS component systems using NIST approved transport layer data encryption.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

WLS data is shared with TSC, which is a federal government organization external to DHS. TSC receives confirmation messages to ensure the messages sent to DHS have been received. TSC also receives error messages and requests for data as part of the reconciliation process, which ensures that all organizations maintain exact replicas of the data authorized for dissemination to the authorized DHS systems.

All other sharing of the WLS data will be conducted pursuant to the programmatic system of records notices that have been published for the particular systems and are outlined in the WLS system of records notice. TSC receives encounter information from the various DHS components that may interact with individuals that may match against a TSDB record.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

WLS data will be a near real-time mirror of the TSC's TSDB which will be automatically updated. Initially, the following Privacy Act systems of records will cover the four programs that will be leveraging WLS: (1) the TSA Office of Transportation Threat Assessment and Credentialing, Transportation Security Threat Assessment System DHS/TSA 002, May 19, 2010, 75 FR 28046; (2) the TSA Secure Flight Program, Secure Flight Records DHS/TSA 019, November 9, 2007, 72 FR 63711; (3) the CBP Passenger Systems Program Office for inclusion in TECS, U.S. Customs and Border Protection TECS DHS/CBP-011 December 19, 2008 73 FR 77778; and (4) the US-VISIT program for inclusion into the DHS IDENT DHS/USVISIT-0012, June 5, 2007, 72 FR 31080. In order to provide additional transparency, DHS will also submit a SORN covering DHS's maintenance of a mirror copy of the TSDB for the WLS for publication in the *Federal Register*. This PIA and any applicable SORNs will be updated if additional systems are given access to the WLS. In addition, DHS will update this PIA and WLS SORN and file an appropriate records retention schedule for the retention of encounter information before the DHS WLS Encounters Data Broker functionality becomes available.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The WLS reconciliation data will be shared directly with the TSC in order to ensure DHS has an accurate mirror copy of the TSDB. In instances where the information in the WLS data has been incorporated into a DHS system, the information will be shared in accordance with the PIA and SORN describing the system and with the security protocols in place. DHS will continue to share the same encounter information with TSC as well as auditing and reconciliation information. 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.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

WLS will not transmit data from the WLS directly outside of DHS. Data are transmitted to TSC as part of the reconciliation process. TSC receives confirmation messages to ensure the messages sent to DHS have been received. TSC also receives error messages and requests for data as part of the reconciliation process, ensuring all organizations maintain exact replicas of the data. All data are transmitted over an encrypted network that is Federal Information Processing Standard (FIPS) 140-2 compliant. WLS will further secure the information to DHS component systems using NIST-approved transport layer data encryption.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Notice of the overall nature and use of terrorist watchlist data is provided via the TSC's SORN for the TSDB. Notice of specific DHS uses of the data is provided via the PIAs and SORNs for DHS component systems listed in Appendix A, below and via this PIA.

Initially, the following Privacy Act system of records will cover the four systems that will be using the WLS: (1) the TSA Office of Transportation Threat Assessment and Credentialing, Transportation Security Threat Assessment System DHS/TSA 002, May 19, 2010, 75 FR 28046; (2) the TSA Secure Flight Program, Secure Flight Records DHS/TSA 019, November 9, 2007, 72 FR 63711; (3) the CBP Passenger Systems Program Office for inclusion in TECS, U.S. Customs and Border Protection TECS DHS/CBP-011 December 19, 2008 73 FR 77778; and (4) the US-VISIT program for inclusion into the DHS IDENT DHS/USVISIT-012, June 5, 2007, 72 FR 31080.

Additionally, in order to provide more transparency DHS will be publishing a SORN for the WLS in the *Federal Register*.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Regarding the TSDB, which the WLS receives from TSC, individuals do not have an opportunity to decline to provide information. WLS obtains information directly from the TSC and not from the individuals. Programs that will receive TSDB data via the WLS may provide individuals with opportunities to decline to provide their information specific to that program. These opportunities are enumerated in the program-specific PIAs.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. WLS data exists as a near real-time mirror of TSC's TSDB, which is governed by TSC. DHS uses data from the TSC according to legacy arrangements with DHS components that currently have access to TSDB data, the WLS MOU and the operations of the DHS component systems as described in the PIAs and SORNs for those systems – see Appendix A.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

There is a risk that notice is not provided regarding the manner in which DHS will receive and manage data from the TSDB. This PIA serves that notice as well as explaining the improvements made to the way DHS receives and manages TSDB data. Notice of TSDB data is already provided through the SORN for the TSDB as well as notice of DHS's existing uses of that data through the privacy compliance documentation for the DHS component systems. TSC collects information for counterterrorism, intelligence, and law enforcement purposes and aggregates data in the TSDB. WLS collects data from the TSC/TSDB in support of DHS mission related functions.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

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, or US-VISIT, 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, such as watchlist matching results or analyses that were not supplied by that individual. Information collected from individuals by DHS components are addressed in program specific PIAs. Additionally, DHS has established a voluntary redress process to assist individuals seeking to ensure that DHS has access to the most accurate information on the individual for the purposes of determining an individual's match to a name on the watchlist. An individual who believes he or she may have been unfairly or incorrectly delayed, denied boarding or identified for additional screening by DHS may initiate the redress process by completing and submitting a Traveler Inquiry Form (TIF) to the DHS Traveler Redress Inquiry Program (DHS TRIP).

Based on the information provided by the individual seeking redress, DHS TRIP will appropriately coordinate to address the request. PIAs for DHS TRIP, CBP Passenger Screening, WHTI, TWIC and TSA

Office of Transportation Security Redress (OTSR) are available at www.dhs.gov/privacy. Redress requests should be addressed to: Program Manager, DHS TRIP, U.S. Department of Homeland Security Washington, DC 20528. Additionally, requests for access to the information submitted during the redress process may be made by submitting a request to the DHS TRIP email link TRIP@dhs.gov posted on the DHS TRIP website www.dhs.gov/trip.

7.2 What are the procedures for correcting inaccurate or erroneous information?

The individual may obtain the forms and information necessary to initiate the redress process on the DHS TRIP website at www.dhs.gov/trip or by contacting the DHS TRIP office by mail. Written requests may be sent to the DHS TRIP office, and must include the individual's name and current address. DHS will provide the necessary documents and information to individuals through its website or by mail.

The individual must send to the DHS TRIP office the personal information and copies of the specified identification documents. If DHS needs additional information in order to continue the redress process, DHS will notify the individual in writing and request that additional information. An individual's redress application will be suspended if documentation is not received on or before the established deadlines.

DHS, in coordination with appropriate federal law enforcement or intelligence agencies, if necessary, will review all the documentation and information requested from the individual, correct any erroneous information, and provide the individual with a timely written response.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are notified of redress procedures through this PIA and the DHS website.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Individuals should seek formal redress through DHS TRIP, as described in Section 7.1.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

DHS TRIP provides a redress process that furthers the privacy interest of the individual by making available an easy-to-use website that facilitates the submission and processing of redress requests. Because DHS TRIP collects PII directly from the individual, the risk of collecting inaccurate information should be minimized. A PIA for DHS TRIP was published by DHS on January 18, 2007. It is available at the DHS website (www.DHS.gov). Moreover, individuals may request access and correction to their PII pursuant of the Privacy Act.

With the implementation of the WLS, DHS will consolidate and streamline data feeds between the TSC and DHS components for use in approved DHS screening programs.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

Authorized personnel and contractors with a "need-to-know" relevant to DHS's mission, and as described in the WLS MOU and legacy arrangements with TSC, may access WLS data through the applicable DHS component or program office. DHS supervisors must submit system access requests for eligible users to the appropriate program office. To become eligible, a user must successfully pass a background investigation and complete annual privacy training. The program office will verify the user's background check status and completion of the annual privacy training before issuing a user account. In addition, the user must sign a statement certifying that he has received training regarding system security. After an account has been established, additional safeguards exist to protect WLS data. Specifically, the program office conducts annual reviews of internal user accounts in addition to periodic assessments of technical, administrative, and managerial controls which enhance data integrity and accountability. Each DHS program office is in full compliance with the DHS IT Security Program Handbook, which established a comprehensive information security program to include management policies, operational policies, application rules, and directives on roles and responsibilities. Specific security and access privilege procedures are documented in the information sharing agreements between TSC and each DHS component system.

PIAs are in place for each DHS component that will receive information from the WLS; user access procedures are fully described therein – see Appendix A.

8.2 Will Department contractors have access to the system?

Contractors to DHS will have an essential role in designing, developing, implementing, and managing the system due to their specialized expertise. Contractors must complete the same process as Federal employees seeking WLS system access as described above, to include a full field background investigation and security and privacy training before they are allowed to access any WLS data.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All users of the WLS system are required to complete and pass a bi-annual General Privacy Act Awareness Course (GPAAC) to maintain their access to the system. The GPAAC presents Privacy Act responsibilities and DHS policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the user's understanding of appropriate controls put in place to protect privacy as they are presented. A user must pass the test scenarios to retain access to WLS. This training is regularly updated.

DHS employees are also required to sign statements acknowledging that they have been trained and understand the security aspects of their systems and comply with the following requirements:

- Access records containing personal information only when the information is needed to carry out their official duties.
- Disclose personal information only for legitimate business purposes and in accordance with applicable laws, regulations, and WLS policies and procedures.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

WLS and the CBP Enterprise Service Bus (ESB) Certification and Accreditation (C&A) will be completed by CBP as the executive agent for DHS prior to WLS implementation. WLS will follow the Department-wide C&A process, which is documented in DHS Management Directive 4300.1. The Designated Approving Authority (DAA) reviews and approves or disapproves the system's C&A materials and approves corrective actions necessary to mitigate risks. Successful Certification and Accreditation results in an Authority to Operate (ATO), which is generated by the DAA. If the DAA finds issues or concerns, he will develop a Plan of Action & Milestones (POAM) to address the system's shortcomings. The CBP Core Enterprise Network, which WLS uses as a backbone, has already been certified and accredited.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

WLS allows for oversight and audit capabilities to ensure that the data are being handled consistent with all applicable laws and regulations regarding privacy and data integrity. WLS maintains audit trails or logs for the purpose of reviewing internal and external user activity. WLS actively prevents access to information for which a user lacks authorization as defined by the user's role in the system. Multiple attempts to access internal information without proper authorization will cause WLS to suspend access automatically. Misuse of WLS data can subject a user to discipline in accordance with the DHS Code of Conduct, which can include being removed from a position. CBP Security will also use the logs during C&A activities to audit their completeness prior to issuing a certificate to operate.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Identifiable privacy risks of WLS include unauthorized access to data, accidental disclosure of PII, and improper modification of data. These risks have been mitigated by defense-in-depth strategy, access controls, auditing, and appropriate oversight. WLS will operate through CBP's Enterprise Service Bus and thus will adhere to the following security controls that are part of that environment: These controls, as described below, ensure that only authorized individuals access the information.

Certificate Authorities.

DIMC is the root certificate authority for DHS, which is issued under Federal Bridge certificate authority. All messages are signed with a private key by the sender using a certificate issued by DIMC or another certificate authority under the Federal Bridge. The CBP ESB will not accept messages signed by a Certificate Authority (CA) that is not under the Federal Bridge. If an external entity is unable to obtain a certificate signed by a CA under the Federal Bridge, an external PSPO service possessing a certificate signed by DIMC must be leveraged to fulfill the message signature requirements.

Digital Signatures.

The process for attaching digital signatures to XML messages and verifying/validating them will be leveraged through the use of Web Services Security (WS Security) communications protocol. WS Security protocol contains specifications on how integrity and confidentiality can be enforced.

Attaching Digital Signature.

The WS Security section of a message, as defined by the WS Security specification, is contained within the SOAP header, designated by the wsse: Security element. The signing entity is responsible for attaching the following within the WS Security section.

- Timestamp – Used to indicate when the digital signature was created and when it expires
- Binary Security Token – Base64 encoded X509 public key certificate associated to the private key used to sign the message
- Signature – Contains a description of the signed content of the message, including a reference to the specific elements that were signed, the digest values created from the reference elements, the digitally encrypted signature created using each digest value, and key information referencing the public key certificate to be used to verify the signature

Signature Validation.

Signature Validation ensures that the data being transmitted was not tampered with (Signature Verification) and allows the receiver to determine from whom the message was coming and verifies that the sender was who the sender claimed to be (Certificate Validation).

Signature Verification Process.

Using the imbedded public key certificate, the receiver decrypts the digital signature contained within the signature value element. The decryption reveals the digest value used to create the digital signature. This digest value is compared to a digest value created by the receiver from the signed info reference elements. The signature is verified if the two digest values match.

Certificate Validation Process.

The receiver accesses what it knows to be the sender's public key certificate and compares it to the public key certificate imbedded in the message. The certificate is validated if the two are in sync and the certificate is not listed in the CA's list of certificates that have been revoked or are no longer valid, called a Certificate Revocation List (CRL). The receiver's copy of the sender's public key certificate is verified in advance that it is signed by a known CA. DHS will have access to the CA’s CRL to ensure the sender’s public key certificate is valid.

WLS is designed to limit the use of PII only to approved uses by authorized parties and protect against inadvertent and unnecessary disclosure. Access to the system and data will be strictly controlled. Only individuals with proper authorization, credentials, training and need to know will be granted access to the system in performance of their duties. Access and audit log reviews, along with other security precautions are in place to further secure system and data access. Processes and policies are in place to further provide that the system use in limited to its intended design while limiting as much as possible the use of PII.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

WLS is composed of commercial off-the-shelf (COTS) and government off-the shelf products (GOTS), which are integrated through government custom code. System components include COTS hardware and operating systems along with custom applications running on aforementioned systems.

9.2 What stage of development is the system in and what project development lifecycle was used?

WLS is currently in the Development phase. WLS will be following the CBP System Life Cycle as well as the DHS System Engineering Life Cycle.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No. WLS does not employ technology that raises novel privacy concerns. As previously discussed, WLS simply 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 will replace multiple data feeds from the TSC to DHS components to facilitate DHS-mission related functions, such as counterterrorism, law enforcement, border security, and inspection activities. DHS will not receive any new data as part of the WLS; the system was created for efficiency purposes only.

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan

Chief Privacy Officer
Department of Homeland Security

Appendix A

WLS Downstream DHS Components with Privacy Impact Assessments and System of Record Notices

1. **Secure Flight**
   - DHS/TSA – 019 Secure Flight System of Records Notice November 9, 2007, 72 FR 63711
   - Transportation Security Administration's Secure Flight Program, PIA, October 21, 2008, (*PDF, 27 pages - 284 KB*)
2. **TSA Office of Transportation Threat Assessment & Credentialing (TTAC) Programs**
   - DHS/TSA – 002 Transportation Security Threat Assessment System SORN, May 19, 2010, 75 FR 28046
   - Transportation Security Administration's Security Threat Assessment for Airport Badge and Credential Holders PIA, December 20, 2006
   - Hazardous Materials Endorsement PIA, June 1, 2004
   - Transportation Worker Identification Credential (TWIC) Program, PIA, November 5, 2004
   - Alien Flight Student Program, PIA, December 4, 2009
   - Maryland Three (MD-3) Airports, PIA, February 20, 2009
   - Air Cargo Security Requirements, PIA, November 12, 2008
   - Large Aircraft Security Program, PIA, October 2, 2008
   - Airmen Certificate Vetting Program, PIA October 22, 2007
3. **TECS Interagency Border Inspection System (TECS)**
   - DHS/CBP – 011 TECS System of Records Notice, December 19, 2008 73 FR 77778
4. **Automated Biometric Identification System (IDENT)**
   - DHS/USVISIT – 0012 Automated Biometric Identification System (IDENT) SORN, DHS/USVISIT-0012, June 5, 2007, 72 FR 31080
   - Enumeration Services of the Automated Biometric Identification System (IDENT) PIA, May 25, 2007.

Appendix B

Core Biographic Person Data Elements (CBPDE)

As communicated in the Core Biographic IEPD, the CBPDE is a core set of biographic data elements (and their formats) that are to be included in any biographic identity-related information exchange. These elements represent the minimum elements used for establishing unique biographic identities for information exchange throughout DHS.

Element	NIEM	NIEM Definition
First Name	nc:PersonGivenName	The first name of a person.
Last Name	nc:PersonSurName	The last name or family name of a person.
Middle Name	nc:PersonMiddleName	The middle name of a person.
Name Translation	nc:PersonPrimaryLanguage	Data type for the language capability of an individual
Date of Birth	nc:PersonBirthDate	The date a person was born.
Country of Birth	nc:PersonBirthLocation/ nc:LocationCountry (Selected ISO and FIPS country code lists)	The location where a person was born.
Gender	nc:PersonSexCode (Selected code list)	The gender or sex of a person.
Country of Citizenship	nc:PersonCitizenship abstract (Selected ISO and FIPS country code lists)	A county that assigns rights, duties, and privileges to a person because of the birth or naturalization of the person in that country.