



Privacy Impact Assessment

for the

Watchlist Service

DHS Reference No. DHS/ALL/PIA-027(d)

July 10, 2020



Homeland
Security



Abstract

The U.S. Department of Homeland Security (DHS) receives a copy of the Terrorist Screening Database (TSDB), the U.S. Government's consolidated database maintained by the Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Terrorist Screening Center (TSC), to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities. In July 2010, DHS launched an improved method of transmitting TSDB data from TSC to DHS through a service called the DHS Watchlist Service (WLS). Currently, WLS maintains a synchronized copy of the TSDB, which contains personally identifiable information (PII) and disseminates TSDB records it receives to authorized DHS Components. DHS is updating and replacing the DHS/ALL/PIA-027(d) Privacy Impact Assessment (PIA) because the WLS is being expanded to convey additional national security threat actors beyond known or suspected terrorists (KST).

Overview

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

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

The DHS WLS provides DHS with an authoritative, accurate, and reconcilable feed of the TSDB for use in the Department's mission. The DHS WLS simplifies, standardizes, and documents the distribution of TSDB data to supported DHS screening systems via a centralized interface between the TSC and DHS. The DHS WLS ensures that each DHS Component receives only the formatted records from the TSDB that it is authorized to receive pursuant to the terms of information sharing agreements with FBI/TSC and as authorized by law and consistent with the Component's legal authorities and privacy compliance documentation. WLS is a system-to-system secure connection with no direct user interface.

¹ Homeland Security Presidential Directive 6 (HSPD-6) (September 2003) <http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf>.



Reason for the PIA Update

The *Strategy to Combat Transnational Organized Crime* directs the Executive Branch to establish comprehensive information sharing to aid in the identification of Transnational Organization Crime (TOC) members and associates, deny them entry to the United States, and help capture those in the United States or partner countries.² In support of this strategy's implementation, DHS is participating in a TSC-led pilot for a whole of Government approach to watchlisting for TOC actors and which uses WLS as the information sharing mechanism to transmit TOC data from the TSC to DHS.

DHS is updating this PIA because the proposed expansion of the WLS to include certain categories of non-KST records significantly changes the nature of the information received by DHS via WLS. TSC is expanding the WLS to include additional individuals who may pose a threat to national security. Executive Order 13863³ defined TOC actors⁴ and individuals detained during military operations who do not meet the international definition of "prisoner of war" as National Security Threat Actors (NSTAs). Watchlisting these NSTAs is consistent with Executive Order 12333 (or successor order) ("national security threats") for persons who do not otherwise satisfy the requirements for inclusion in the TSDB – KST. TOC actor information will not include U.S. citizens or lawful permanent residents (U.S. Persons). Specifically, DHS will now receive information regarding the following types of individuals via the WLS:

- Individuals who were officially detained during military operations, but not as enemy prisoners of war, and who have been identified as possibly posing a threat to national security, and who do not otherwise satisfy the requirements for inclusion in the TSDB ("military detainees"), consistent with Executive Order 12333 (or successor order) and the Department of Justice Terrorist Screening Records System of Records Notice (SORN) DOJ/FBI-019;⁵ and
- Individuals who may pose a threat to national security because they are known or suspected to be or have been engaged in conduct constituting, in aid of, or related to transnational organized crime, thereby posing a possible threat to national security, and

² See STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME: Addressing Converging Threats to National Security (July 2011), available at <https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf>.

³ Executive Order (E.O.) 13863, "Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Transnational Criminal Organizations," amending E.O. 13581, March 15, 2019, <https://www.govinfo.gov/app/details/DCPD-201900153>.

⁴ A TCO is a group or groups of persons that (a) include one or more foreign persons; (b) threaten the national security, foreign policy, or economy of the United States; and (c) engage in an ongoing pattern of serious criminal activity involving the jurisdictions of at least two foreign states.

⁵ JUSTICE/FBI-019 Terrorist Screening Records System (TSRS), 76 FR 77846 (December. 14, 2011), available at <https://www.gpo.gov/fdsys/pkg/FR-2011-12-14/pdf/2011-32074.pdf>.



do not otherwise satisfy the requirements for inclusion in the TSDB as KSTs (“transnational organized crime actors”), consistent with Executive Order 12333⁶ (or successor order) (“national security threats”) and in support of the White House’s “Strategy to Combat Transnational Organized Crime” (July 19, 2011),⁷ National Security Presidential Directive-59/Homeland Security Presidential Directive-24, “Biometrics for Identification and Screening to Enhance National Security” (June 5, 2008),⁸ and Executive Order 13863 (March 15, 2019).⁹

In support of the implementation of National Security Presidential Memorandum (NSPM)–7,¹⁰ DHS participates in an interagency pilot operated by TSC for a whole of Government approach to watchlisting for TOC actors. It is through the structure of this pilot that DHS uses WLS as the information sharing mechanism to transmit TOC data from TSC to DHS.¹¹

DHS updated and reissued a Department-wide SORN titled “DHS/ALL-030 Use of the Terrorist Screening Database System of Records”¹² on April 6, 2016. One of the reasons for this update was to add the two types of individuals noted above and to clarify one existing category of individuals whose information is currently included in the TSDB: relatives, associates, or others closely connected with a known or suspected terrorist who are excludable from the United States based on these relationships by virtue of Section 212(a)(3)(B) of the Immigration and Nationality Act, as amended.

DHS is also updating this PIA to provide notice that the analytical project for which U.S. Immigration and Customs Enforcement (ICE) used the computer readable extract of TSDB

⁶ Executive Order No. 12333 – United States Intelligence Activities, 46 FR 59941 (December 8, 1981) (as amended by E.O. 13284, 13344, and 13470) (2008), *available at* <http://www.archives.gov/federal-register/codification/executive-order/12333.html>.

⁷ See STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME: Addressing Converging Threats to National Security (July 2011), *available at* <https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf>.

⁸ Directive on Biometrics for Identification and Screening To Enhance National Security, National Security Presidential Directive/NSPD-59 and Homeland Security Presidential Directive/HSPD-24 (June 5, 2008), *available at* <https://www.gpo.gov/fdsys/pkg/PPP-2008-book1/pdf/PPP-2008-book1-doc-pg757.pdf>.

⁹ Executive Order 13863, “Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Transnational Criminal Organizations,” amending E.O. 13581, March 15, 2019, <https://www.govinfo.gov/app/details/DCPD-201900153>.

¹⁰ See National Security Presidential Memorandum – 7 (October 5, 2017), *available at* <https://www.whitehouse.gov/presidential-actions/national-security-presidential-memorandum-7/>.

¹¹ NSPM-7 identifies transnational criminal actors as individuals, organizations, groups, or networks known or appropriately suspected to be engaged in an ongoing pattern of serious illegal activity involving a foreign jurisdiction and the United States or the jurisdictions of at least two sovereign states that threaten the national security interests of the United States or other global security interests, to include the security of citizens, welfare of communities, economic prosperity and trade, and regional stability.

¹² DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records, 81 FR 19988 (April 6, 2016), *available at* <https://www.dhs.gov/system-records-notice-sorns>.



data has concluded and that data is being archived at ICE. ICE maintained the TSDB data in its LeadTrac system, which was recently modernized.¹³ When the system was modernized, the TSDB data was extracted from the legacy system and not migrated to the new LeadTrac environment due to the fact that the analytical project was completed. The current retention period approved by the National Archives and Records Administration (NARA) for data in the LeadTrac system is 75 years; however, ICE intends to request that NARA lower the retention period for this TSDB extract to 25 years.

Privacy Impact Analysis

Authorities and Other Requirements

The President's *Strategy to Combat Transnational Organized Crime* directs the Executive Branch to establish comprehensive information sharing to aid in the identification of TOC members and associates, deny them entry to the United States, and help capture those in the United States or partner countries.¹⁴ In support of this memorandum and to fully implement National Security Presidential Directive-59/Homeland Security Presidential Directive-24, "Biometrics for Identification and Screening to Enhance National Security" (June 5, 2008), Attorney General Order (AGO) No. 3548-2015 (August 6, 2015), Executive Order 13773 (February 9, 2017)¹⁵, and Executive Order 13863 (March 15, 2019)¹⁶, the WLS is being expanded to include individuals who may pose a threat to national security, consistent with Executive Order 12333 ("national security threats").

National Security Presidential Memorandum (NSPM)-7 directs the Executive Branch to lawfully identify, integrate and make available through, accurate and timely national security threat actor information, effectively manage information and when appropriate and consistent with applicable law, deliberately use information to support national security activities.¹⁷ NSPM-7 provides the Department with the authority to watchlist and to share certain categories of non-KST information.

¹³ See DHS/ICE/PIA-044 LeadTrac System, available at <https://www.dhs.gov/privacy-documents-ice>.

¹⁴ See STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME: Addressing Converging Threats to National Security (July 2011), available at <https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf>.

¹⁵ Executive Order 13773, "Executive Order on Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking," February 9, 2017
<https://www.govinfo.gov/app/details/DCPD-201700106>.

¹⁶ Executive Order 13863, "Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Transnational Criminal Organizations," amending E.O. 13581, March 15, 2019
<https://www.govinfo.gov/app/details/DCPD-201900153>.

¹⁷ See National Security Presidential Memorandum -7 (October 5, 2017), available at <https://www.whitehouse.gov/presidential-actions/national-security-presidential-memorandum-7/>.



DHS has updated the Use of the TSDB SORN¹⁸ to include both of these additional populations.

Characterization of the Information

There is a privacy risk that the addition of the military detainees and TOC actors is an expansion of the WLS beyond its original stated purpose of conveying information related to terrorism – the TSDB.

Individuals falling within these additional categories have been determined to be threats to the national security of the United States, through NSPM-7. This determination makes it possible to manage and share these individuals' information in similar fashion to how previously categorized NSTAs' (KSTs') information is managed and shared.

These new categories of records undergo a similar review process to the existing terrorist watchlist nomination review processes before being included in the WLS. For example, nominators are departments or agencies that have information to indicate that an individual is reasonably suspected of being involved with transnational organized crime and nominates that individual to TSC based upon information that originated with that department or agency, a third department or agency, and/or foreign governments. TSC rigorously reviews the information before it is included in its TOC Actor Detection Program (TADP) as a TOC record and transferred to DHS via the WLS. All records submitted by federal, state, and local departments and agencies must meet the reasonable suspicion standard before being accepted into the TADB. As a result, all TADB records exported through DHS systems have previously met this standard.¹⁹ For NSTA data submitted by foreign governments, per HSPD-6 agreements, the data is presumed to meet the reasonable suspicion standard.

If a record does not meet minimum substantive derogatory or identifying criteria for watchlisting, the record will not be included in the TADP. If new information nullifies the derogatory information, the record will be removed immediately from the TADP.

Uses of the Information

This expansion introduces changes to how data is used within WLS. The information will be used by DHS to assist in efforts to stop transnational organized crime including human trafficking and drug smuggling. Additionally, WLS continues as the mechanism to convey

¹⁸ DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records, 81 FR 19988 (April 6, 2016), available at <https://www.dhs.gov/system-records-notices-sorns>.

¹⁹ Reasonable suspicion requires articulable facts which, taken together with rational inferences, reasonably warrant the determination that an individual is known or suspected to be or has been engaged in conduct constituting, in preparation for, in aid of or related to terrorism and terrorist activities (for inclusion into the TSDB) or transnational organization crime (for inclusion into TADP). The reasonable suspicion standard is based on the totality of the circumstances in order to account for the sometimes fragmentary nature of terrorist information. These criteria are spelled out in interagency standards and watchlisting guidance.



information maintained in the TSDB to authorized DHS systems. Information added to the TSDB on individuals known or suspected to be a threat to national security will be distinguished from individuals known or 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) and their supporters.

Information about individuals who are known or suspected to be or have been engaged in conduct constituting, in aid of, or related to transnational organized crime is shared with the TSC for inclusion in TSC’s existing watchlisting and vetting infrastructure for national security threats. Eligibility for inclusion as a TOC member is limited in scope to non-U.S. Persons associated with transnational criminal organizations. Prior to any change to this scope, TOC watchlisting will be evaluated by the Deputy Attorney General and assessed in coordination with participating federal agencies.

Notice

There are no new privacy risks. DHS has provided notice through the DHS-wide system of records notice for WLS²⁰ and through the publication of this PIA update.

Data Retention by the project

There are no new privacy risks. Although the information from the TSC will now include additional categories of individuals, the data will be retained per the same rules as existing categories.

Information Sharing

TOC actor information will be shared more widely than KST information because the number of officials with need-to-know access is greater for TOC. DHS will share encounter and auditing information consistent with the mechanisms established with the TSC pursuant to the WLS Memorandum of Understanding. 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, as fully described in previous WLS PIA updates.

Redress

There are no new privacy risks. Redress procedures have not changed with the expansion of information collected. The DHS Traveler Redress Inquiry Program (TRIP) provides redress for individuals who encounter screening-related travel difficulties to include the additional individuals in the WLS who may pose a threat to national security.

Additionally, all individuals, regardless of citizenship, may obtain access to records consistent with the Freedom of Information Act (FOIA) unless disclosure is prohibited by law

²⁰ DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records, 81 FR 19988 (April 6, 2016), available at <https://www.dhs.gov/system-records-notice-sorns>.



or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. The DHS FOIA contact address is: Chief Privacy Officer/Chief Freedom of Information Act Officer, Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, DC 20528-0628. Requests for information are evaluated to ensure that any release of information is lawful and does not disclose information that would cause a clearly unwarranted invasion of personal privacy or that would disclose techniques and/or procedures for law enforcement investigations or prosecutions.

Auditing and Accountability

There are no new privacy risks. Auditing and accountability measures have not changed. As part of the transnational organized crime operational pilot, the pilot is evaluated by participating agencies and the TSC. Interagency pilot participants use this analysis to evaluate the pilot and determine appropriate future actions.

Responsible Official

Alex Zemek
Deputy Assistant Secretary
Screening and Vetting Office (SVO)
Counterterrorism and Threat Prevention Policy (CTTP)
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security
(202) 891-2120

Approval Signature

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

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717