FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1272294-0

Total Deleted Page(s) = 1
Page 12 ~ b3; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

Federal Bureau of Investigation

Privacy Impact Assessment
for the
Terrorist Screening Center – Terrorist Screening Database (TSDB)

Issued by:
James J. Landon, FBI Privacy and Civil Liberties Officer

Reviewed by: _____, Chief Information Officer, Department of Justice

Approved by: Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [Component to insert date of PIA approval]

Points of Contact and Signatures

COMPONENT PRIVACY POINT OF CONTACT (POC) Name: [redacted] Office: FBI/OGC/PCLU Phone: [redacted] b6 b7C Bldg./Room Number: JEH 7350 Email: [redacted]	**PIA AUTHOR** (if different from POC) Name: N/A Office: Phone: Bldg./Room Number: Email:
SECURITY REVIEW OFFICIAL (Component CIO/OBD Executive Officer/OCIO Staff Director/JMD Staff Director) Name: Dean E. Hall, Acting Executive Assistant Director-CIO Office: Information Technology Branch Phone: 202-324-6165 Bldg./Room Number: JEH, RM 7125 Email: Signature: [signature] Date signed: 14 May 2012	**SENIOR COMPONENT OFFICIAL FOR PRIVACY** (if designated; otherwise POC) Name: James J. Landon Office: FBI Privacy and Civil Liberties Officer Phone: Bldg./Room Number: Email: Signature: See attached signature page Date signed:
DOJ PIA REVIEWING OFFICIAL Chief Information Officer Department of Justice (202) 514-0507 Signature: Date signed:	**DOJ PIA APPROVING OFFICIAL** Nancy C. Libin Chief Privacy and Civil Liberties Officer, ODAG Department of Justice (202) 307-0697 Signature: Date signed:

THIS PAGE IS FOR INTERNAL ROUTING PURPOSES AND DOCUMENTATION OF APPROVALS. UPON FINAL APPROVAL, COMPONENTS SHOULD REMOVE THIS PAGE PRIOR TO PUBLICATION OF THE PIA

Points of Contact and Signatures

COMPONENT PRIVACY POINT OF CONTACT (POC)	PIA AUTHOR (if different from POC)
Name: [redacted] b6 b7C Office: FBI/OGC/PCLU Phone: [redacted] Bldg./Room Number: FBI HQ JEH 7350 Email: [redacted]	Name: Office: Phone: Bldg./Room Number: Email:
SYSTEM MANAGER/OWNER Name: [redacted] b6 b7C Office: TSC/CIO Phone: [redacted] Bldg./Room Number: TSC/322 Email: [redacted] Signature: [redacted] Date signed: 11/3/12	**SENIOR COMPONENT OFFICIAL FOR PRIVACY** (if designated; otherwise POC) Name: James J. Landon Office: FBI Privacy and Civil Liberties Officer Phone: Bldg./Room Number: Email: Signature: Date signed:
DOJ PIA REVIEWING OFFICIAL Eric R. Olsen Acting Chief Information Officer Department of Justice (202) 514-0507 Signature: Date signed:	**DOJ PIA APPROVING OFFICIAL** Nancy C. Libin Chief Privacy and Civil Liberties Officer, ODAG Department of Justice (202) 307-0697 Signature: Date signed:

THIS PAGE IS FOR INTERNAL ROUTING PURPOSES AND DOCUMENTATION OF APPROVALS. UPON FINAL APPROVAL, COMPONENTS SHOULD REMOVE THIS PAGE PRIOR TO PUBLICATION OF THE PIA

#11-523

FEDERAL BUREAU OF INVESTIGATION
TERRORIST SCREENING CENTER
TERRORIST SCREENING DATABASE

Points of Contact and Signatures

COMPONENT PRIVACY POINT OF CONTACT (POC) Name: Office: Phone: Bldg./Room Number: Email:	**PIA AUTHOR** (if different from POC) Name: Office: Phone: Bldg./Room Number: Email:
SECURITY REVIEW OFFICIAL (Component CIO/OBD Executive Officer/OCIO Staff Director/JMD Staff Director) Name: Office: Phone: Bldg./Room Number: Email: Signature: _____ Date signed:	**SENIOR COMPONENT OFFICIAL FOR PRIVACY** (if designated; otherwise POC) Name: Office: Phone: Bldg./Room Number: Email: Signature: _____ Date signed:
DOJ PIA REVIEWING OFFICIAL Luke McCormack Chief Information Officer Department of Justice (202) 514-0507 Signature: [signature] Date signed: 6/20/12	**DOJ PIA APPROVING OFFICIAL** Nancy C. Libin Chief Privacy and Civil Liberties Officer, ODAG Department of Justice (202) 307-0697 Signature: [signature] Date signed: 7/16/12

Section 1: Description of the Information System

Introduction

The mission of the Terrorist Screening Center (TSC), created by Homeland Security Presidential Directive 6 (HSPD-6), is to consolidate and coordinate the United States Government's approach to terrorism screening and to facilitate the sharing of terrorism information[1] while safeguarding privacy and civil liberties. To carry out its mission, the TSC maintains the U.S. Government's consolidated database of names and other identifying information for all known or suspected terrorists (KSTs) and others deemed appropriate for watchlisting. This database is known as the Terrorist Screening Database (TSDB). TSC supports domestic and foreign partners' terrorism screening efforts by providing access to the TSDB according to written agreements with levels of access appropriate to the needs of each recipient and the U.S. Government.

Process

On an ongoing basis, the National Counterterrorism Center (NCTC) provides to TSC international terrorist information related to individuals to be included in the TSDB in accordance with the *Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism* (TSC MOU). NCTC provides this information either in the form of an official nomination for inclusion in the TSDB or as a request for the modification or deletion of an existing TSDB record. NCTC's terrorist identities database, known as TIDE, contains information beyond the information that meets the minimum substantive derogatory and identifying criteria for nominations to the TSDB. Therefore, prior to NCTC's submission to the TSC, NCTC and the nominating agency must both ensure that the nomination contains information that demonstrates that the minimum standard for inclusion in the TSDB is met. Included in NCTC's submission to the TSC are biometric information or "terrorist identifiers," such as names, aliases, dates of birth, passport numbers and derogatory information on the individual to support both the nomination to TSDB (i.e., meets the minimum substantive derogatory criteria) and the individual's watchlisting status (i.e., placement on the No Fly and Selectee Lists). In a process that is parallel to the NCTC international terrorist nominations process, the FBI Terrorist Review and Examination Unit (TREX) sends domestic terrorist nominations to the TSC nominations unit via internal FBI secure email.

Once the international or domestic terrorist nomination records are sent to the TSC by either automated transactional or manual means, a TSC analyst completes a nomination review to determine whether the information submitted meets the standard for watchlisting (or one of the approved

---

[1] "Terrorism information" as defined in IRTPA, Section 1016(a)(4): (A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to--(i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and (B) includes weapons of mass destruction information.

exceptions to the general standard) in the TSDB.[2] Although derogatory information is used by the TSC to evaluate the nomination, only biographic information is actually ingested into TSDB. TSC's Single Review Queue (SRQ) enables the TSC's Nominations and Data Integrity Unit (NDIU) to review each screening nomination to ensure it meets the watchlisting standard prior to the record's inclusion in TSDB, thereby greatly improving the accuracy of the data in TSDB. During the SRQ process, every request to add, modify, or delete a TSDB record is reviewed by a TSC analyst to ensure the accuracy of watchlisting records and the removal of inaccurate records from TSDB.

In the majority of cases, nominations to the TSDB are accepted based on reasonable suspicion that the individual is a known or suspected terrorist. First Amendment protected activity alone must not be the basis of a nomination.

b3
b7E

b3
b7E

TSC shares TSDB information pursuant to law, policy, and formal agreements with TSC's customers via electronic export[3] and transactional feed[4]. TSC's customers include the Department of Homeland Security (transportation and border screening), Department of

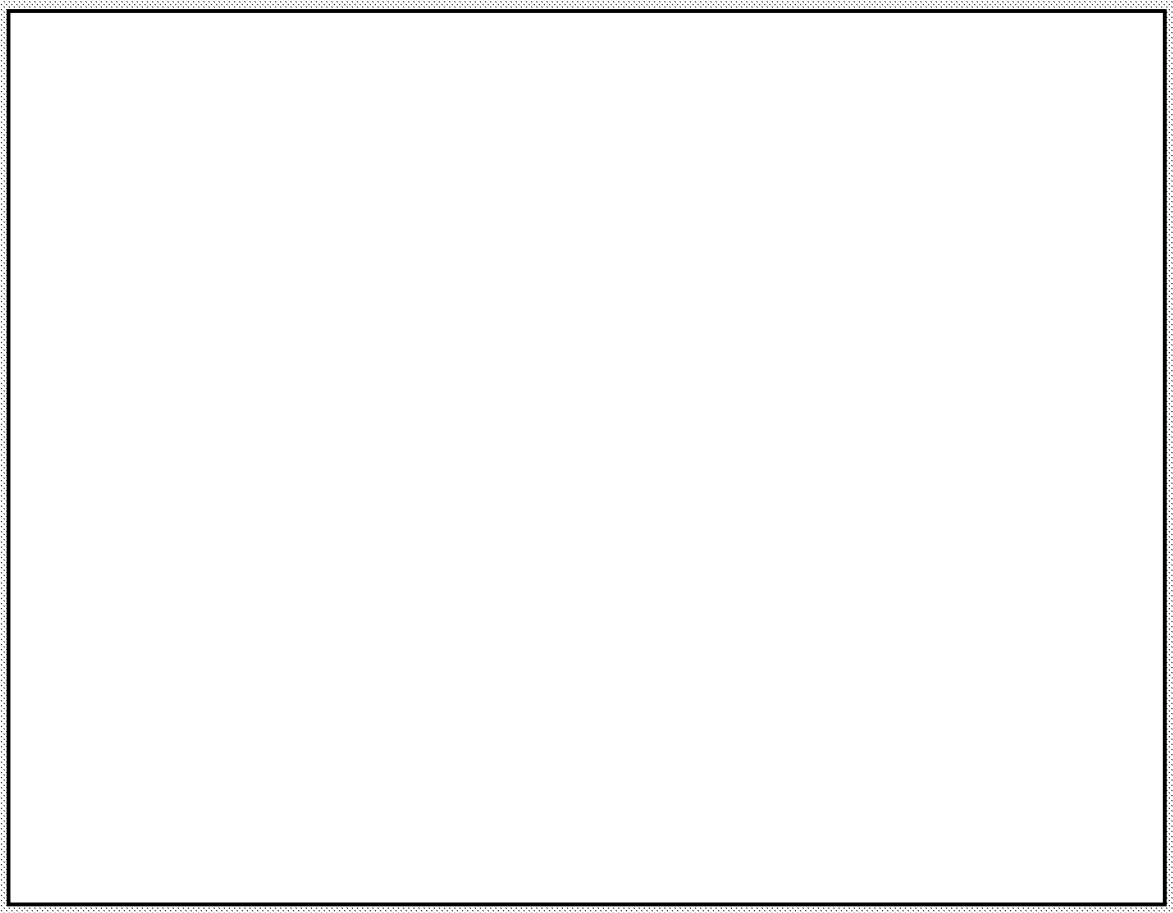
[2] The standards for watchlisting are outlined in the July 2010 Watchlisting Guidance, which has been developed to help standardize the watchlisting community's nomination and screening decisions.

[3] "Electronic Export" is a means for transporting data from one place to another on a periodic, as opposed to a continuous, basis.

[4] "Transactional Feed" is a processing method in which transactions are executed immediately when they are received by the system, rather than at some later time as in batch-processing systems, which may utilize an electronic export.

State (passport and visa screening), approved Foreign Partners, and the Federal Bureau of Investigation Criminal Justice Information Services Division (CJIS) for law enforcement screening through the National Crime Information Center (NCIC).

b3
b7E



b3
b7E

Quality Control

HSPD-6 requires the TSC to maintain "current, accurate, and thorough" information concerning known or suspected terrorists. It is the responsibility of NCTC, the TSC, and the nominating agency to ensure that this standard is maintained. Both NCTC and the TSC have a multilayered review process to ensure that each nomination meets the necessary standard for inclusion in the TSDB and that each request for modification or deletion of a record in TSDB is proper. To ensure that the processes in place are effective, both NCTC and TSC continuously audit and review them. In addition to providing as much derogatory information as possible when nominating an individual to the TSDB, nominating agencies also have a responsibility to provide guidance on the watchlisting nomination process on a periodic basis. This periodic review must include a specific review of U.S. person nominations.

[redacted]

b3
b7E

[redacted]

b3
b7E

Redress

The goal of the watchlist redress process is to provide for timely and fair review of individuals' complaints and to identify and correct any errors in the TSDB. Redress complaints are funneled through the DHS Traveler Redress Inquiry Program (DHS TRIP), which is the single point of contact for all traveler screening issues, and those that concern the TSDB are directed to the TSC thereafter. TSC's Redress Office is responsible for receiving, tracking, and researching watchlist-related complaints. Each redress complaint receives an in-depth analysis to determine if the person's complaint is related to a TSDB record, including determining whether the complainant is the watchlisted individual and whether that individual still meets all the watchlisting criteria. Each complaint is coordinated with the nominator to ensure the Redress Office has the most current, accurate, and thorough information available for its review. Where appropriate and warranted by the current information and applicable criteria, a person's watchlist status may be adjusted (e.g., downgraded from No Fly to Selectee) or the person's identity may be removed from the TSDB.

Legal or Use Restrictions

[redacted] b3 b7E

The general policy of the U.S. Government is to neither confirm nor deny an individual's watchlist status. In addition to the provisions in the TSC MOU, which require nominator approval before TSDB information can be used in any process that might result in public disclosure, the Redress MOU requires each screening agency to contact TSC if it receives a request for information or records that might reveal an individual's watchlist status.

All sharing of information from the TSDB must be consistent with TSC authorities and the authorities of the recipient agency, which includes ensuring compliance with the Privacy Act.

[redacted] b3 b7E

Users access TSDB [redacted] Encounter Management Application (EMA)[8].

[redacted] b3 b7E

[5] Nominations are requests for data inclusion or modification in the TSDB.
[6] A Privacy Threshold Analysis (PTA) for [redacted] is currently pending review. b3 b7E
[7] A PTA for [redacted] is currently pending review.
[8] A PIA for EMA is currently pending review.

- EMA is the system that assists the TSC in the evaluation and management of information related to encounters of possible KSTs and others deemed appropriate for watchlisting.

[redacted]

b3
b7E

[redacted]

[redacted]

b3
b7E

The Quality Assurance (QA) review process allows tracking of potential and actual problems in the data and for correction of errors.

When records are removed from the TSDB, for whatever reason, they are retained in the limited access TSDB Archive for audit, quality assurance, litigation, and other purposes. The archived record search feature allows users to search and view archived TSDB records in accordance with TSC privacy and auditing guidelines. Each search must be justified by one of six reason codes[9] in accordance with

[9] The 6 reason codes are: (1) To research and resolve a TSC redress matter (including a matter that has reached litigation) to determine the nature of the complaint or problem; (2) Where archived TSDB data is relevant in litigation in which the

TSC policies. All of the data from archive searches is extensively audited and protected to ensure that it has been marked as archived and is not accessed by users without proper authorization and purpose. Before an individual is granted access to TSDB Archives, the TSC Privacy Officer determines whether the individual has a need to access the data in accordance with TSC guidelines and if so, provides specific TSDB Archives Privacy Training to the user.

TSDB uses the Microsoft Active Directory (AD) product to perform user authentication and authorization. Data in TSDB is only accessible by users with appropriate roles and need for the information. Role-based groups are assigned by job function, as determined by appropriate TSC management, and re-evaluated on an as needed basis. TSC maintains a detailed audit capability and will impose discipline and/or revoke access based on improper usage of any part of the TSDB.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

[redacted] b3 b7E

[redacted] The collected information must support the minimum biographic and/or the minimum substantive derogatory information necessary for nomination.

[redacted] b3 b7E

United States is a party or has significant interest; (3) To identify or resolve matters that require a quality assurance review and/or possible correction to TSC or third-agency records; (4) To respond to requests from congressional oversight committees and government auditors or oversight bodies, and to perform internal audits; (5) To evaluate the adequacy of TSC's data and procedures in the aftermath of a terrorist attack, and to support any investigation into such an attack; (6) To test new software by the Information Technology Department, or for general user training.

b3
b7E

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected.

b3
b7E

Potential privacy risks associated with this system are data breaches[10], data overcollection, and maintenance of inaccurate data. TSC has mitigated these risks as follows.

b3
b7E

[10] Data breach includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether physical or electronic.

[redacted] b3 b7E

The risk of the TSDB maintaining inaccurate and/or untimely data is addressed in several ways. All nominations are reviewed by NCTC or FBI TREX analysts, as appropriate, before they are sent to the TSC. In addition, as part of the QA process described above, once submitted, the nominations are reviewed by at least two TSC nominations unit analysts for accuracy and timeliness. TSC also works with the Departments of State and Homeland Security using two automated data reconciliation techniques to ensure that these agencies have accurate information in the exports they are receiving from the TSDB. As a final mitigation, individuals may also seek redress through the DHS TRIP process (see redress discussion in response to 5.4) if they believe TSDB data is inaccurate.

The potential risk of data overcollection stems from the need to have sufficient information to make a determination about a watchlist nomination. Biographic information helps identify an individual and the more information available, the greater likelihood that a positive identification of the correct individual can be made. Because the TSC cannot anticipate how an individual may be encountered, information that appears to be unnecessary, such as an [redacted] or a tattoo marking, actually may be needed to evaluate whether an encounter with an individual in the TSDB has occurred. The risk of overcollection of derogatory information is easily mitigated because it is not stored in the TSDB; the TSDB contains only biographic information and an individual's watchlisting status. b3 b7E

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
X	For intelligence activities		For administrative matters
	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		

[1] TSDB is a [redacted] see Section 6, *infra*. b3 b7E

X	Other (specify): HSPD 6 directs TSC to use TSDB information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign government, and private-sector screening processes; and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

Under HSPD-6, TSC has the dual mission of maintaining the TSDB and disseminating information from it, to the extent permitted by law, to support (a) Federal, State, local, territorial, tribal, foreign government, and private-sector screening processes; and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes. Therefore, TSC's maintenance of the TSDB supports screening processes at U.S. ports of entry, U.S. embassies, international postal and cargo facilities, for special events, for HAZMAT licenses, for firearms purchases, during police stops, for citizenship and immigration processes, and for foreign screening operations abroad. Use of TSDB information for these purposes helps protect the American people from terrorist attacks by alerting appropriate officials when a KST or other person deemed appropriate for watchlisting attempts to gain access to any of the facilities, people, systems, or benefits for which screening has been authorized.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	- Section 1021 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, 118 Stat. 3638. - Section 212(a)(3)(B) of the Immigration and Nationality Act of 1952.
X	Executive Order	-Homeland Security Presidential Directive 6 (HSPD-6) -Homeland Security Presidential Directive 11 (HSPD-11) -Homeland Security Presidential Directive 24 (HSPD-24)

X	Federal Regulation	-TSC System of Records Notice, 72 Fed. Reg. 47073 (Aug 22, 2007), as amended by 76 Fed. Reg. 77846 (Dec. 14, 2011) -Privacy Act Exemptions Final Rule, 28 CFR 16.96 (Dec. 2, 2005)
X	Memorandum of Understanding/agreement	-Memorandum of Understanding on the Integration and Use of Screening Information (Sep. 16, 2003) ("TSC MOU") -Terrorist Screening Center MOU, Addendum A -Terrorist Screening Center MOU, Addendum B -Memorandum of Understanding on Terrorist Watchlist Redress Procedures
X	Other (summarize and provide copy of relevant portion)	-Watchlisting Guidance (approved by National Security Council (NSC)/Homeland Security Council (HSC) Deputies Committee July 2010)

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Various types of TSDB information have different retention periods under the TSC's NARA-approved retention schedule, Job Number: N1-065-06-2. Active individual records in the TSDB master file will be deleted or destroyed 99 years after date of entry. The TSDB system has an archive module that maintains records that are no longer considered appropriate for watchlisting. These records can be accessed only by a strictly limited set of TSC personnel who must provide specific justification for accessing archived records each time they do so. This justification, along with user and other information, is maintained in a detailed audit log. According to the TSC NARA retention schedule, TSC must delete or destroy individual TSDB records 50 years after the records status changes to inactive (50 years after going into the Archive).

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The primary threats to privacy as a result of the use of TSDB information are improper access and improper use of the information. The TSC mitigates these threats first, through comprehensive privacy training. Upon their entry on duty at TSC, all personnel are trained on their privacy-related rights and responsibilities by the TSC Privacy Officer or designate. All TSC personnel are also

required to complete annual FBINet-Virtual Academy Privacy training, as well as Federal Information Systems Security Awareness training.

The TSC also mitigates these privacy threats through access controls on the TSDB. Section 2.3 explains TSC's role-based access protocol. General access controls to the data are also employed: the TSDB resides in a secure FBI facility and users need physical access to the FBI secure area to access the TSDB. Once a TSC employee no longer has an official need for TSDB information, access to TSDB is terminated. Users are also forced to change their password after initial login and then every 90 days or more frequently if the user believes the password may have been compromised

Additionally, TSC strives to ensure thorough, accurate, and current data. While NCTC's TIDE database and the TSC's TSDB are managed separately, effort is made to keep the two databases synchronized—with non-conflicting information about the same identities—to the greatest extent possible. TSC has developed a method to continuously update TSDB by adding functionality that improves the accuracy (and therefore the quality) of the data. This process works by allowing errors in the TSDB to be edited and corrected at TSC, provided appropriate documentation is available to support the change, rather than waiting for NCTC first to complete its entire—sometimes time consuming—process of checking and confirming TSC's data correction work.

As noted previously, TSC has also established a strictly controlled archive for records that are no longer appropriate for watchlisting that can be accessed only by a limited group of TSC personnel for specifically defined purposes. The TSDB system requires that the user accessing archived records provide justification for each access. This justification information is maintained as part of the audit trail.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component				
DOJ components				
Federal entities				
State, local, tribal gov't entities				
Public				

b3
b7E

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

b3
b7E

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

The TSC shares information externally with screening partners via TSDB exports and transactional feeds. The exports and transactional feeds are listed on the diagram in section 1 of this document. Transfers to other U.S. federal agencies are based on memoranda of understanding (MOUs) and Interface Control Documents (ICDs). The MOUs include privacy provisions that are reviewed and approved by the TSC Privacy Officer and FBI Office of the General Counsel. The ICDs specify how and to whom TSDB data will be transferred based on official need.

b3
b7E

b3
b7E

Depending on the particular identity fields used in the search, and the number of identities in TSDB that are sufficiently similar to the search query, a particular query may return many close matches (exact matches are not required), or none.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: TSC is usually not the initial collector of information from individuals; instead, information in TSDB is generally extracted from law enforcement or intelligence case information, which individuals do not have the opportunity to decline to provide. Also, it is the policy of the US Government not to confirm or deny terrorist watchlist status.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: See previous response.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

In order to protect national security, there is no consent form crafted or distributed to the individuals whose records are maintained in the TSDB. In fact, it is the policy of US government to neither confirm nor deny TSDB status. Moreover, practically speaking, the TSC is usually not the original collector of information in TSDB from individuals. However, the Terrorist Screening Records System of Records Notice, last updated at 76 Fed. Reg. 77,846 (Dec. 14, 2011), provides the public with general notice about the information that is collected, as well as the routine uses of that information.

Because this system contains information related to the government's counterterrorism, law enforcement and intelligence programs, records in this system are exempt from notification, access, and amendment to the extent permitted by subsections (j) and (k) of the Privacy Act. If individuals are experiencing repeated delays or difficulties during a government screening process and believe that this might be related to terrorist watch list information, however, they may contact the Federal agency that is conducting the screening (''screening agency'') or the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP). DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs—such as airports and train stations—or crossing U.S. borders. By contacting DHS TRIP with a complaint, individuals will be able to take advantage of the procedures available to help misidentified persons and others experiencing screening problems.

The TSC assists the screening agencies and DHS TRIP in resolving any screening complaints that may relate to terrorist watch list information, but does not receive or respond to individual complaints directly. However, if TSC receives any such complaints, TSC will forward them to the appropriate screening agency.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: TSDB is accredited by FBI Security Division [redacted] b3 b7E

X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: [redacted] Monitoring tools are in place to manage the health and maintenance of TSDB. The TSC IT Security Team performs security tests and evaluations on iterations of TSDB prior to deployment. Only those individuals with a clear need to know are permitted access to TSDB in order to complete their duties.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: March 02, 2010
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: The following NIST 800-53 Audit Family controls apply to TSDB: AU-1, AU-2 (3) (4), AU-3 (1) (2), AU-4, AU-5 (1) (2), AU-6 (1), AU-7 (1), AU-8 (1), AU-9, AU-10, AU-11, AU-12 (1).
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.
	The following training is required for authorized users to access or receive information in the system:
X	General information security and privacy training
X	Training specific to the system for authorized users within the Department.
X	Training specific to the system for authorized users outside of the component.
X	Other (specify): Indoctrination and Orientation training for all new TSC employees and contractors.

b3
b7E

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

Per the current Approval to Operate TSDB implements access and security controls commensurate with its Levels of Concern and those controls are appropriately monitored, maintained, and upgraded per FBI C&A and FISMA requirements. More specifically, access to the TSDB is role-based, so that the appropriate TSC management personnel have the ability to limit the types of information any particular user can see and the types of data changes any individual user can implement. Role based accesses are evaluated on an as needed basis by TSC management personnel.

The system resides in a secure FBI facility; users need physical access to the FBI/TSC

controlled facility to access the TSDB.[12] Upon entry on duty at TSC, and annually thereafter, TSDB users are trained in the appropriate use and access of data. The TSC Security Unit, however, led by the TSC Chief Security Officer, is responsible for ensuring compliance with the Rules of Behavior for FBI Information Systems under the control of TSC. All queries conducted on information contained in the general TSDB are recorded so that effective auditing may be accomplished; for the TSDB Archives, specific written justification is required and recorded for each individual query.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: 76 Fed. Reg. 77,846 (Dec. 14, 2011).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Records relating to United States citizens and/or lawfully admitted permanent resident aliens (together, U.S. persons) are retrieved in generally the same manner as records relating to non-U.S. persons in the TSDB. Within each identity, however, there is an indicator of whether the individual to whom the information pertains is a U.S. person. Users can search for a record using several methods, including controlling for U.S. persons or non-U.S. persons. The user can search for a record by entering biographic information, using analysis tool filtering, or by way of system identifiers unique to the record.

Biographic identifiers in TSDB include:

- Name
- DOB

[redacted]

b3
b7E

- Citizenship
- Passport Number

b3
b7E

Analysis Tool:

- TSDB analysis tool allows you to narrow searches by grouping records with similar attributes.

The content of TSDB exports vary.

b3
b7E

All general TSDB users can access all active records in the TSDB. As described previously, records in the TSDB archive require special approval to be accessed. Access to all TSDB records is audited.