

REDACTED FOR PUBLIC RELEASE



FOLLOW-UP AUDIT OF THE TERRORIST SCREENING CENTER

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 07-41
September 2007

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

**FOLLOW-UP AUDIT OF THE
TERRORIST SCREENING CENTER***

EXECUTIVE SUMMARY

The Terrorist Screening Center (TSC) is a multi-agency organization administered by the Federal Bureau of Investigation (FBI) that consolidates terrorist watchlist information and provides 24-hour, 7-day a week operational support for federal, state, local, and foreign governments.¹ The TSC was created by the September 16, 2003, Homeland Security Presidential Directive-6 (HSPD-6), which directed the TSC to integrate all existing U.S. government terrorist watchlists and assist in the screening of individuals who, for example, apply for a visa, attempt to enter the United States through a port-of-entry, attempt to travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation. Prior to the establishment of the TSC, the federal government relied on at least a dozen separate terrorist watchlists maintained by different federal agencies.

In June 2005, the Department of Justice Office of the Inspector General (OIG) issued an audit of the TSC's operations from the time of its inception in 2003.² The OIG reported that although the TSC had made significant strides in becoming the government's single point-of-contact for law enforcement authorities requesting assistance in identifying individuals with possible ties to terrorism and had developed a consolidated terrorist watchlist database, the TSC had not done enough to ensure that the information in that database was complete and accurate. For example, we reported instances where the consolidated database did not contain names that should have been included on the watchlist. Additionally, we found inaccurate or inconsistent information related to persons included in the database. In this prior review, we also found problems with the TSC's management of its information technology, a crucial facet of the terrorist screening process. Our June 2005 report included 40 recommendations to

* The full version of this report includes information that the FBI considered to be law enforcement sensitive and therefore could not be publicly released. To create this public version of the report, the OIG redacted (deleted) the portions of the full report that were considered sensitive by the FBI, and we indicated where those redactions were made.

¹ The participating agencies include the FBI, Central Intelligence Agency (CIA), and the Departments of Homeland Security (DHS) and State (State Department).

² Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center*, Audit Report 05-27, June 2005.

REDACTED FOR PUBLIC RELEASE

the TSC addressing areas, such as database improvements, data accuracy and completeness, and staffing.

The objectives of this follow-up audit were to: (1) determine if accurate and complete records are disseminated to and from the watchlist database in a timely fashion; (2) review the TSC's efforts to ensure the quality of the information in the watchlist database; and (3) assess the TSC's efforts to address complaints raised by individuals who believe they have been incorrectly identified as watchlist subjects.

To accomplish these objectives, we interviewed more than 45 officials and reviewed TSC documents and databases. To evaluate the accuracy and completeness of the consolidated watchlist, we analyzed the consolidated database as a whole, including a review of the number of records in the database, any duplication that existed within those records, and the associated watchlist processes. We also tested individual records within the database for accuracy and completeness, as well as the timeliness of any related quality assurance activities. Finally, we assessed the TSC's activities related to individuals who raised complaints following their involvement in a screening encounter. This included examining the TSC's coordination with other participating agencies and reviewing a sample of such cases to determine if the actions taken were timely and conformed to TSC policy.³

Results in Brief

Overall, this follow-up audit found that the TSC has enhanced its efforts to ensure the quality of watchlist data, has increased staff assigned to data quality management, and has developed a process and a separate office to address complaints filed by persons seeking relief from adverse effects related to terrorist watchlist screening. However, we also determined that the TSC's management of the watchlist continues to have weaknesses. For example, the TSC is relying on two interconnected versions of the watchlist database. As a result of this and other conditions, we identified several known or suspected terrorists who were not watchlisted appropriately. Specifically, we identified 20 watchlist records on suspected or known terrorists that were not made available to the frontline screening agents (such as a border patrol officer, visa application reviewer, or local police officer) for use during watchlist screening encounters (such as at a border crossing, through the visa application process, or during a routine traffic stop). We also found that the number of duplicate records in the database has significantly increased since our last review.

³ Detailed information regarding the audit objectives, scope, and methodology is contained in Appendix I.

REDACTED FOR PUBLIC RELEASE

In addition, because of internal FBI watchlisting processes, we found that the FBI bypasses the normal international terrorist watchlist nomination process and enters these nominations directly into a downstream screening system. This process is cumbersome for the TSC and, as a result, the TSC is unable to ensure that consistent, accurate, and complete terrorist information is disseminated to frontline screening agents in a timely manner.

We also concluded that the TSC needs to further improve its efforts for ensuring the accuracy of the watchlist records. We found that, in general, the TSC's actions to review records as part of a targeted special project successfully ensured the quality of the data. In contrast, our examination of the routine quality assurance reviews revealed continued problems. We examined 105 records subject to the routine quality assurance review and found that 38 percent of the records we tested continued to contain errors or inconsistencies that were not identified through the TSC's quality assurance efforts. Although the TSC had clearly increased its quality assurance efforts since our last review, it continues to lack important safeguards for ensuring data integrity, including a comprehensive protocol outlining the agency's quality assurance procedures and a method for regularly reviewing the work of its staff. Additionally, the TSC needs to work with partner agencies to develop clearly defined areas of responsibility and timeframes for quality assurance matters.

A single omission of a terrorist identity or an inaccuracy in the identifying information contained in a watchlist record can have enormous consequences. Deficiencies in the accuracy of watchlist data increase the possibility that reliable information will not be available to frontline screening agents, which could prevent them from successfully identifying a known or suspected terrorist during an encounter or place their safety at greater risk by providing inappropriate handling instructions for a suspected terrorist. Furthermore, inaccurate, incomplete, and obsolete watchlist information increases the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity.

We are also concerned that the TSC's ongoing review of the watchlist will take longer than projected. At the time of our audit field work in April 2007, the TSC was continuing its efforts to conduct a record-by-record review of the consolidated watchlist and anticipated that all watchlist records would be reviewed by the end of 2007. However, the watchlist database continues to increase by an average of over 20,000 records per month and contained over 700,000 records as of April 2007. Given this growth and the TSC's weak quality assurance process, we believe the TSC is

REDACTED FOR PUBLIC RELEASE

underestimating the time required to sufficiently review all watchlist records for accuracy.

Our audit further determined that the TSC was following its procedures and reaching appropriate resolutions in its review of complaints filed by individuals seeking redress from further adverse experiences that they believed were the result of terrorist watchlist screening. However, we found that the redress reviews were not always completed in a timely manner, and we recommend that the TSC and partner agencies develop timeliness measures for each phase in the redress process.

Additionally, the TSC's redress reviews have identified that the database contains records for individuals that should not be watchlisted and that some watchlist records are inaccurate or incomplete. We believe that these results provide a further indicator that watchlist data needs continuous monitoring and attention. We also believe that the TSC should use information related to terrorist watchlist identities that are frequently the subject of watchlist encounters to proactively initiate redress reviews before complaints are filed.

Our report contains detailed information on the full results of our follow-up review of the TSC and contains recommendations to help the TSC carry out its important role in the terrorist watchlisting process.

Summary of Watchlist Nomination, Screening, and Redress Processes

Agencies that conduct counterintelligence, counterterrorism, and law enforcement activities provide information to the FBI and the National Counterterrorism Center (NCTC) on suspected or known terrorists who are nominated for inclusion on the consolidated terrorist watchlist maintained by the TSC.⁴ The FBI is responsible for submitting to the TSC all domestic terrorist identity nominations, and NCTC is responsible for submitting international terrorist identity nominations.⁵ These two agencies employ analysts who review the information on the known or suspected terrorist identity and forward an unclassified subset of information to TSC analysts, who then review the information to ensure that all required criteria are met

⁴ NCTC was established on May 1, 2003, to develop comprehensive threat assessments through the integration and analysis of terrorist information collected domestically and abroad by the U.S. government. NCTC is a component of the Office of the Director of National Intelligence and was formerly known as the Terrorist Threat Integration Center.

⁵ The FBI is a source agency for domestic and international terrorist information; it forwards relevant information to NCTC on suspected or known international terrorists.

REDACTED FOR PUBLIC RELEASE

to incorporate the identity record in the TSC's consolidated terrorist screening database (TSDB). As additional information is obtained that either enhances the identifying information or indicates that the individual has no nexus to terrorism, source agencies must also submit this information through the nominating process to effect watchlist record modifications and deletions, as appropriate.

The review performed by analysts at NCTC, the FBI, and the TSC includes an analysis of information supporting the watchlist nomination, as well as an examination of the quality, accuracy, and sufficiency of the identity information.⁶ Thus, all identity records undergo a two-stage review before inclusion in the TSDB: (1) at NCTC and then at the TSC for international terrorist identities, or (2) at the FBI and then at the TSC for domestic terrorist identities.

The TSC shares the terrorist information contained in the TSDB by sending it "downstream" to other government screening systems where frontline screening agents can use the information to identify individuals against TSDB records.⁷ The following are examples of three databases that contain information from the TSC's consolidated watchlist: (1) an employee of the U.S. Customs and Border Protection (CBP) agency at a U.S. port-of-entry searches the DHS's Interagency Border Inspection System (IBIS) to determine if a person should be granted access to the United States, (2) a state police officer stops a vehicle for a traffic violation and queries the driver's name in the FBI's National Crime Information Center (NCIC) system, and (3) a State Department consular affairs official searches the Consular Lookout and Support System to determine if a foreign national should be granted a visa to visit the United States. The TSC reported that approximately 270 million individuals are screened by frontline screening agents and law enforcement officers each month.⁸

When a name appears to be a match against the terrorist watchlist, frontline screening and law enforcement personnel contact the TSC's

⁶ The TSC's general criterion for including a record in the consolidated watchlist database is that the nominating agency must have provided evidence of a nexus to terrorism. From a data perspective, the minimum criteria for inclusion of a terrorist identity into the TSDB are that the record contains at least a partial name (e.g., given name, surname, or both) and at least one additional piece of identifying information (e.g., date of birth).

⁷ A description of each of the downstream screening systems is contained in Appendix II.

⁸ The TSC provided data on screening agency encounters from February through April 2007. We reported the average of these 3 months.

REDACTED FOR PUBLIC RELEASE

24-hour call center for assistance in confirming the subject's identity. In responding to such a call, the TSC Call Center staff searches the TSDB and other databases to determine if a terrorist watchlist identity match exists. Between the TSC's inception in December 2003 and May 2007, the TSC has documented more than 99,000 encounters for which its call center was contacted. TSC data shows that 53.4 percent of these calls were determined to be a positive match to a terrorist watchlist identity in the TSDB. In those cases, the TSC contacted the FBI, which is responsible for initiating any necessary law enforcement action. In 43.4 percent of these calls, it was determined that the encountered individual did not match the watchlisted identity, and the TSC Call Center staff instructed the frontline screening agent of this resolution. In the remaining 3.2 percent of the encounters, the TSC Call Center staff could not definitively determine if the match was positive or negative and therefore forwarded these calls to the FBI.

The nature of the U.S. government's actions to screen individuals against the consolidated terrorist watchlist can result in individuals being delayed or detained during security screenings. This can range from an individual being subjected to enhanced security screening and slight delays to missing a flight or being detained for a long period of time. Persons stopped may be actual watchlist subjects, individuals misidentified to a terrorist identity, or someone mistakenly included on the watchlist.

In 2005, the TSC created a process for resolving complaints from individuals who were adversely affected by terrorist watchlist-related screenings and who were seeking relief or "redress." Since the creation of a unit dedicated to processing such complaints in 2005, the TSC Redress Office has received 438 terrorist watchlist-related redress complaints.

Known or Suspected Terrorists Missing from Watchlist

Our review revealed continued instances where known or suspected terrorists were not appropriately watchlisted on screening databases that frontline screening agents use to identify terrorists and obtain instruction on how to appropriately handle the subjects. Even a single omission of a suspected or known terrorist from the watchlist is a serious matter. We found at least 20 watchlist records that were not appropriately watchlisted to downstream screening databases. These watchlisting errors are discussed in detail below.

Due to technological differences and capabilities of the various systems used in the watchlist process, the TSC maintains two interconnected versions of the TSDB to allow for the electronic import and export of data. Although the TSC is developing an upgraded TSDB to eliminate the need for the two

REDACTED FOR PUBLIC RELEASE

systems, in the meantime TSC officials informed us that these two databases should be identical in content and therefore should contain the same number of records. However, we discovered during our review that these two systems had differing record counts. Specifically, on one day that we tested the databases the difference was 18 records, and on a subsequent day the difference was 38 records.

On March 26, 2007, the TSC informed us that the differing record counts were due, in part, to five watchlist records that were missing from the TSC database responsible for exporting watchlist records to most downstream screening databases. Therefore, the associated terrorist identities were not included in downstream databases used to screen individuals against the terrorist watchlist. Further, our testing of a sample of 105 watchlist records revealed 7 additional watchlist identities that were not being exported to all appropriate screening databases. As a result of the TSC's failure to export all terrorist watchlist records to screening databases, these 12 watchlisted individuals could be inappropriately handled during an encounter. For instance, a suspected or known terrorist could be erroneously issued a U.S. visa or unknowingly allowed to enter the United States through a port-of-entry. We discussed these records with TSC officials who agreed with our findings and began correcting these omissions.

During the course of our review, we were also informed by TSC officials that in September 2006 they had identified 2,682 records in the TSDB that were not being exported to any screening database. Working with NCTC, the TSC determined that 2,118 of these records should not have been watchlisted in any system and needed to be removed from the TSDB.⁹ TSC officials conducted a manual review of the remaining 564 records and determined that 8 had not been appropriately watchlisted and needed to be renominated to the TSDB.

However, despite being responsible for removing outdated or obsolete data from the TSDB, the TSC did not have a process for regularly reviewing the contents of the TSDB to ensure that only appropriate records were included on the watchlist. TSC officials told us that they intend to begin performing a monthly review of the database to identify any records that are being stored in the TSDB that are not being exported to any downstream systems. We believe it is essential that the TSC regularly review the TSDB to ensure that all outdated information is removed, as well as to affirm that all records are appropriately watchlisted.

⁹ On April 27, 2007, the TSC implemented an information technology solution to delete these records.

Inconsistent FBI Procedure for Processing Watchlist Data

The FBI's Terrorist Review and Examination Unit (TRES) receives requests from FBI agents to include an individual with known or suspected ties to terrorism on the terrorist watchlist. These requests are provided on nomination forms, which are also used to modify previous submissions or remove records from the watchlist. Analysts at TRES review the nomination information for accuracy and completeness. Once verified, nomination forms for known or suspected *domestic* terrorists are electronically forwarded to the TSC where a TSC analyst manually enters the information into the TSDB. This information is electronically distributed to the downstream screening agency data systems, including the FBI's Violent Gang and Terrorist Organization File (VGTOF), which is part of the NCIC system.

By contrast, once the TRES analyst verifies an FBI-generated *international* terrorist nomination, the analyst enters the information into VGTOF directly and then submits the nomination form to NCTC. Following its review and vetting, the NCTC analyst manually enters the information into its database – the Terrorist Identities Datamart Environment (TIDE) – that in turn feeds the information to the TSDB. Because TRES has already entered the record into VGTOF, it is not necessary for the TSC to export the record it receives from TIDE to VGTOF. Therefore, these records are not exported from the TSDB to VGTOF.¹⁰ Because these VGTOF records will not receive electronic modifications or deletions from the TSDB, the TSC and TRES have agreed that TRES will be responsible for ensuring FBI-originated international watchlist records in VGTOF are accurate, complete, and current.

The FBI's direct entry of international terrorist watchlist nomination data into a downstream screening database bypasses NCTC and the TSC and makes it difficult for the NCTC and the TSC to carry out their responsibilities related to watchlist nominations and records. In our opinion, this process does not comport with the nomination and data flow procedures agreed to by the partner agencies, which requires agencies to provide to NCTC, rather than directly into a downstream database, information related to known or suspected international terrorists. Additionally, we believe the FBI's practice is cumbersome for the TSC and creates unnecessary data errors, anomalies, and inconsistencies as described below.

¹⁰ To alert the TSC of this non-standard entry of records into the TSDB, the TSC implemented a special flag, referred to as "FBI sole source," for FBI-originated international records. This designation precludes all future electronic transactions, including related modifications and deletions, from being exported from the TSDB to VGTOF.

REDACTED FOR PUBLIC RELEASE

To test for data accuracy and consistency, we reviewed a judgmental sample of 50 FBI-originated additions or modifications to the watchlist.¹¹ We found that while the records for the domestic terrorist nominations were generally accurate, the international terrorist nominations were not. We identified 16 records with 28 instances in which the identifying information related to international terrorists was inconsistent between the nomination form, VGTOF, TIDE, TSDB, or other screening systems. According to TSC officials, TREX analysts frequently augment the data on the nomination forms with information they glean from FBI case files and enter this additional information into the VGTOF system. However, this supplemental case information is not forwarded to NCTC and as a result the information is not included in TIDE, not sent to the TSDB, and not made available, if appropriate, to downstream screening systems. Further, because TREX enters the record into VGTOF before the addition of any other existing information from other government databases to which NCTC has access, this additional information is often not included in VGTOF. As a result, vital information on watchlist subjects is not being shared with all appropriate screening agencies.

In addition, we found that the FBI's procedures for processing international terrorist watchlist nominations are cumbersome for the TSC and can inadvertently create an incomplete watchlist. The difference in procedures between the FBI's and other agencies' watchlist nominations requires TSC analysts to review every incoming international terrorist nomination and indicate within the record whether it is an FBI source record. If a terrorist watchlist record is improperly designated as an FBI source record, the subset of terrorist watchlist records in VGTOF will be incomplete because that record will not be exported to or modified within VGTOF. TSC staff told us that they were concerned about this because, when reviewing nominations from NCTC, it is often difficult to distinguish between FBI source records and nominations received from other agencies. In fact, TSC staff stated that there was a period of time (possibly as long as a year) in which many records had been improperly designated as FBI-originated records and vice versa. In March 2007, the TSC and NCTC addressed this problem by developing a method to permit TSC analysts to more easily identify FBI source records.

FBI officials responded to our concerns by stating that they had implemented their nomination procedures to ensure that FBI international terrorist information was entered into VGTOF in a more efficient manner. Yet, our review of 70 FBI record transactions (50 nominations previously

¹¹ The total sample of 50 records consisted of 25 each for domestic and internationally known or suspected terrorists. These 50 records were part of our 156 watchlist record sample that we selected for testing.

mentioned and 20 deletions) revealed that although the transactions were entered into VGTOF in a timely manner, the transactions were not incorporated into the TSDB in a timely fashion.¹² Specifically, 18 of the 70 transactions took more than 5 days for TREX to process, with one transaction taking 35 days. In addition, we identified 2 instances in which TREX erroneously delivered nomination forms for domestic terrorists to NCTC that resulted in delays of 6 and 16 days, respectively.

Delays in including terrorist information in the consolidated database present a significant vulnerability to the integrity of the consolidated watchlist. Further, the FBI's current practice of bypassing NCTC and the TSC and entering international terrorist-related data directly into VGTOF increases the likelihood that watchlist information within the TSDB, TIDE, VGTOF, and other downstream databases is inaccurate and incomplete. As a result, we recommend that the FBI, NCTC, and TSC work together to design a more consistent and reliable process by which FBI-originated international terrorist information is provided to NCTC for inclusion in TIDE and disseminated to the TSDB and downstream screening systems, including VGTOF.

Duplicate Terrorist Watchlist Records

Multiple records containing the same unique combination of basic identifying information can needlessly increase the number of records that a call screener must review when researching a specific individual. In addition, when multiple records for a single identity exist, it is essential that the identifying information and handling instructions for contact with the individual be consistent in each record. Otherwise, the screener may mistakenly rely on one record while a second, more complete record may be ignored. This can result in important information being missed. Further, inconsistent handling instructions contained in duplicate records may pose a significant safety risk for law enforcement officers or screeners.

In reviewing the TSDB for duplicate records, we defined duplicate records as those records that contain the same identifying information for five primary identifying fields – [SENSITIVE INFORMATION REDACTED].¹³ In our June 2005 TSC report, we identified 31 such instances of duplicate records in the TSDB and recommended that the TSC implement corrective

¹² Officials from NCTC, the TSC, and TREX stated that each agency attempts to process nominations to the watchlist within 1 day.

¹³ For each terrorist watchlist record in the consolidated database, only these five fields are exported to downstream systems for use in identifying suspected or known terrorists during the watchlist screening phase.

REDACTED FOR PUBLIC RELEASE

action. For our current audit, we again determined that duplicate records existed within the TSDB and that the occurrence of duplicates had increased significantly. In March 2007, we found that the TSDB contained 2,533 repeated combinations in the 5 core fields involving 6,262 watchlist records. For example, one unique combination of the 5 core fields had 19 associated records. Further, our analysis of the 6,262 duplicate TSDB records indicated that at least 20 percent had some discrepancy in handling instruction, identifying information, or watchlist export designation. For example, we identified one individual with duplicate identity records in the consolidated watchlist. Because both records pertained to the same individual, the instructions for handling the subject should be consistent. However, we identified significant differences between the records regarding handling instructions and additional warnings related to the individual. Specifically, one record noted that the individual was "armed and dangerous with violent tendencies" and also had a valid arrest warrant. The other record did not contain this important information. These types of inconsistencies place screeners and law enforcement officers at undue risk and could potentially result in the admittance of a dangerous individual into the United States.

According to the TSC Chief Information Officer (CIO), the TSC does not have an ongoing process to review the TSDB for duplicate records. Based on our findings, however, the TSC CIO stated that the TSC plans to implement a procedure to conduct weekly reviews of the TSDB for duplicate records and forward any issues to the TSC's internal quality assurance unit for review.

The TSC's Watchlist Quality Efforts

Our June 2005 audit report identified weaknesses in the completeness and accuracy of the consolidated watchlist. At that time, TSC management acknowledged that it needed to focus more attention on ensuring the quality of the watchlist. We recommended that the TSC regularly review and test the information contained in the consolidated watchlist database to ensure the data is complete, accurate, and non-duplicative. We also recommended that the TSC coordinate with participating agencies and establish procedures to identify and resolve missing and conflicting record information.

In response to our recommendations, the TSC increased its quality assurance efforts and implemented a data quality improvement plan. Additionally, in November 2006, the TSC's consolidated terrorist watchlist database was upgraded to incorporate a tracking feature for quality assurance activities. As a result of this upgrade, individual watchlist records in the database now contain a record (referred to as a QA ticket) in which

REDACTED FOR PUBLIC RELEASE

TSC staff can record all quality assurance work that has been performed on that record.

The Nominations and Data Integrity Unit (NDIU) is responsible for performing the TSC's activities related to ensuring the quality and accuracy of the watchlist. The NDIU's activities for ensuring the quality of watchlist information can be categorized into three areas: (1) reviewing incoming watchlist data (referred to as the single review queue); (2) performing reviews of historical records following an encounter where the TSC identifies a potential discrepancy in watchlist records; and (3) conducting special quality assurance projects, such as performing a targeted review of the Transportation Security Administration (TSA) No Fly list.¹⁴ As of March 2007, the TSC had assigned 34 staff to this unit. In comparison, as of September 2004 the TSC had 12 staff assigned responsibility for nominations and data integrity tasks, including 1 staff member that was dedicated solely to quality assurance matters.

To examine the TSC's efforts to ensure the quality of the information in the TSDB, we examined 156 TSDB records that had been subjected to the TSC's quality assurance procedures. Of these 156 records, 36 involved record deletions and we found that each had been handled appropriately. Using the remaining sample of 120 records, we performed tests to determine if the watchlist records were accurate. We found that, in general, the TSC's actions to review records as part of a targeted special project successfully ensured the quality of the data, and we identified virtually no errors in the 15 records we tested in connection with special project reviews. In contrast, our examination of 105 records subjected to the single review queue or post-encounter quality assurance reviews revealed that 38 percent of these tested records continued to contain errors or inconsistencies that were not identified through the TSC's quality assurance efforts.

In general, we believe the actions the TSC has taken to improve quality assurance since our last audit are positive steps. We also recognize that it is impossible to completely eliminate the potential for errors. However, the inaccuracies that we identified in TSDB records that had undergone the TSC's quality assurance processes underscore the need for additional actions to ensure that the TSDB is a reliable source of information about known or suspected terrorists. The results of our testing and analysis of the TSC's quality assurance efforts are summarized below.

¹⁴ [SENSITIVE INFORMATION REDACTED]

REDACTED FOR PUBLIC RELEASE

The TSC's Review of the No Fly List

In July 2006, the Homeland Security Council Deputies Committee issued guidance on how to correctly apply its criteria for including individuals on the No Fly list. Subsequently, the TSC submitted all TSDB records associated with individuals who were on the No Fly list to a comprehensive quality assurance review using this guidance. When the TSC began its review in July 2006, the No Fly list contained 71,872 records. The TSC completed its special review of the No Fly list on January 31, 2007, determining that the No Fly list should be reduced to 34,230 records.¹⁵ The TSC recommended 22,412 records for removal from the No Fly list and placement on the TSA's Selectee list.¹⁶ For another 5,086 records, the TSC determined that the individual did not require inclusion on either the No Fly or Selectee list.

We selected and reviewed 15 records that were part of the TSC's review of the No Fly list. We did not find any data inaccuracies or inconsistencies in these records. Each record's basic identifiers [SENSITIVE INFORMATION REDACTED] were shown consistently in all of the affected databases and each record remained the same or was downgraded from the No Fly list in accordance with the final recommendation of the TSC.

Data Inaccuracies and Inconsistencies Exist After Quality Assurance Review

Unlike our review of the No Fly list special project, however, our examination of records passed through the TSC's single review queue or encounter-driven quality assurance processes revealed that records were still likely to contain errors or inconsistencies. We examined 105 records to determine if basic information [SENSITIVE INFORMATION REDACTED] was shown consistently in all of the affected databases. We also verified that correct handling codes were included on watchlist records. In short, our testing revealed that records the TSC reviewed through its routine quality assurance processes frequently continued to contain errors, which indicates weaknesses in the TSC's practices for verifying the integrity of the original watchlist data.

As previously reported, we found that 7 of the 105 records we tested were not exported to appropriate downstream databases. In addition, our

¹⁵ During its review of the No Fly list, the TSC continued to receive routine No Fly list additions, modifications, and deletions through the watchlist nomination process. As a result, it is not possible to subtract the special project-driven No Fly list changes from the starting point of 71,872 records and obtain the correct number of No Fly records as of January 31, 2007.

¹⁶ [SENSITIVE INFORMATION REDACTED]

REDACTED FOR PUBLIC RELEASE

review of the 105 watchlist records that had been subjected to the TSC's single review queue or encounter-driven quality assurance processes revealed that 35 records had inconsistent identifying information when comparing one or more fields in the TSC's consolidated watchlist records with the source or screening agencies' database records. Identifying information related to terrorist watchlist identities must be accurate and consistent across all systems involved in the watchlisting process, namely the TSDB, the downstream systems, and the nominating agencies' systems. Inconsistent data can confuse or delay TSC Call Center operators in their efforts to determine whether an encountered individual is a positive match to a known or suspected terrorist. Further, inconsistent information among databases involved in terrorism screening indicates that at least one record may be incorrect. Incorrect records can also misinform frontline screening agents and contribute to the misidentification of a person not on the watchlist or the inappropriate release or admittance of a dangerous individual. Finally, our testing of the 105 sample watchlist records also revealed that 5 records contained incorrect handling instructions.

During our review, it became apparent that both the TSC's quality assurance efforts and our reviews of watchlist records identified errors and inconsistencies in incoming records from the source agencies – NCTC and the FBI. We discussed the watchlist nomination process with NCTC and FBI officials, and both agency representatives stated that records are reviewed for accuracy, completeness, and consistency before the records are forwarded to the TSC. However, these efforts are failing to identify a significant number of deficiencies in the nominated records. The TSC's quality assurance efforts, therefore, are hampered by the inaccurate and incomplete source material.

Untimely Resolution of Quality Assurance Issues

Delays in the closure of quality assurance matters directly affects the accuracy of the consolidated watchlist database because records can contain inaccurate and incomplete information for extended periods of time while the matter is being resolved. We examined a sample of 51 quality assurance matters opened between February 2006 and February 2007. We found that these matters were open from 0 days (matter was closed the same day as it was opened) to 329 days. On average, the quality assurance matters examined in our sample were open for 80 days.

The TSC has not established a performance measure identifying what it believes to be an acceptable duration for its analysts to complete a quality assurance review. According to TSC personnel, NDIU analysts were supposed to follow up on all quality assurance matters every 30 days.

REDACTED FOR PUBLIC RELEASE

However, the TSC does not have a mechanism such as a standardized report or digital dashboard that catalogs all outstanding quality assurance matters.¹⁷ In concert with the development of timeframes for resolving quality assurance matters, we believe the TSC should develop a system, including an aging schedule, to track its quality assurance work.

Weaknesses in TSC Quality Assurance Policy and Oversight

We also found that the TSC has implemented necessary enhancements in its quality assurance resources and processes since our last audit. Our examination of records submitted to the TSC's No Fly list special project showed that the TSC's review was generally successful in ensuring the quality of watchlist records. However, the inaccuracies we found in our review of watchlist records that were subjected to the TSC's single review queue and post-encounter quality assurance reviews – examinations that are less comprehensive than the No Fly list review – indicate a need for further enhancements to these quality assurance processes.

During our audit, we performed a physical observation of TSC analysts conducting quality assurance reviews of watchlist records. We noted that the analysts' method of performing their reviews was not always consistent. For example, some analysts inspected all of the documents supporting a TSDB record while other analysts relied solely upon summary information. We also found that the analysts were not consistently documenting their quality assurance work.

We believe that this situation was caused by inadequate standard operating procedures (SOP) detailing the TSC's quality assurance processes and by insufficient training. The TSC has an SOP for its quality assurance efforts, but the document was last revised on August 16, 2005. Moreover, the document provides incomplete guidance to analysts on the processing of quality assurance matters and did not mention the existence of special quality assurance projects and encounter-based quality assurance reviews. Further, while the SOP informs the analysts performing standard quality assurance reviews how to examine watchlist records, it fails to detail what fields, supporting information, and other aspects of the records the analysts should be verifying and comparing. In addition, these procedures do not instruct the analysts on the necessary actions to take when inaccurate or incomplete information is identified.

¹⁷ A digital dashboard is a business management tool that visually displays the status of a business project. The dashboard can provide warnings, next steps, action notices, and summaries of a project.

REDACTED FOR PUBLIC RELEASE

Additionally, the TSC provides its quality assurance analysts only a few days of training before allowing them to work independently, and no supplemental training is required. Moreover, the TSC does not have a mechanism for regularly evaluating the work of its quality assurance analysts to help ensure that the analysts are performing appropriate reviews and keeping abreast of any process changes. We believe that the TSC should develop a more detailed and comprehensive quality assurance SOP to better guide NDIU analysts through their work. In addition, the TSC should develop a mechanism to routinely review its analysts' work to identify processing deficiencies and areas requiring additional training.

Insufficient Process to Comprehensively Review Watchlist Data Quality

In response to our previous TSC audit that identified errors and inconsistencies in the watchlist records, the TSC stated that it intended to conduct a record-by-record review of the approximately 400,000 records in the TSDB. The TSC later estimated that this review would not be complete until 2012. In February 2007, TSC officials stated that the review was being performed through its three-pronged quality assurance strategy – the single review queue, encounter-driven quality assurance reviews, and special projects. TSC officials told us that they plan to examine the TSDB following the completion of the ongoing special projects and determine how many TSDB records have not yet been reviewed. The TSC then plans to review any previously unexamined TSDB records.

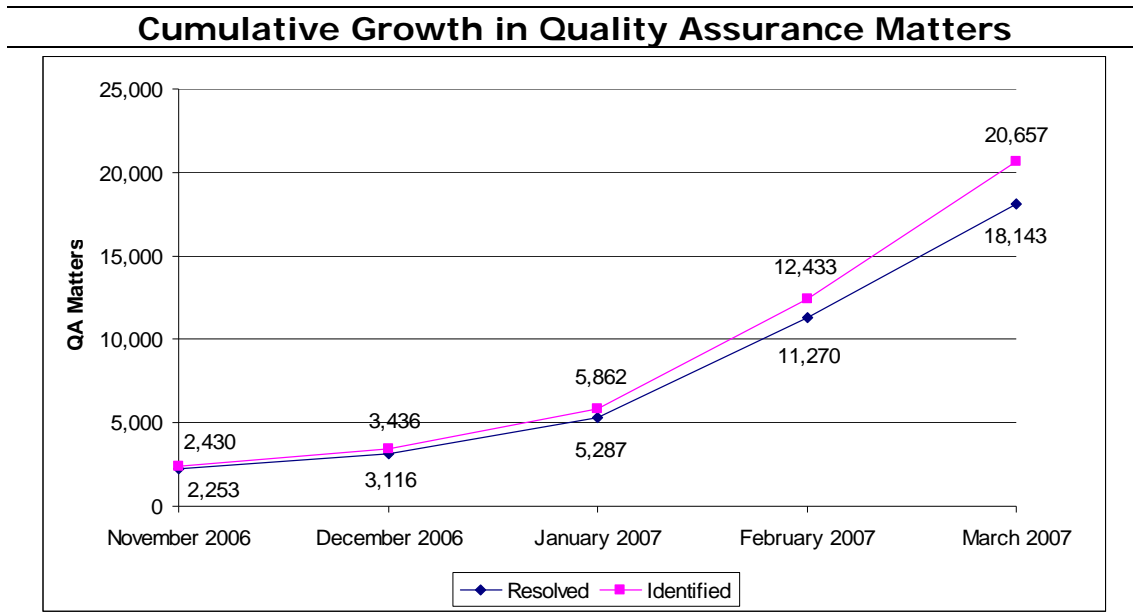
In February 2007, TSC officials told us that since the inception of the single review queue in March 2006 over 670,000 TSDB records had been reviewed and the agency had revised its estimated completion date. TSC officials now project that the record-by-record review will be complete by the end of 2007. However, we believe that the TSC may have overstated the number of records reviewed and is underestimating the amount of time and effort that it will take to complete its review of the entire TSDB. We base these conclusions on the following factors:

- As previously discussed, the TSC's single review queue and encounter-driven quality assurance processes do not sufficiently ensure the quality of the watchlist records. Therefore, the TSC should reconsider records examined in these processes in its count of records reviewed.
- The number of records reviewed is not limited to the review of unique records. Rather, the TSC's quality assurance process allows for one record to be reviewed multiple times: through the single review queue, following each request to modify or delete

the record, in accordance with one or more special projects, and subsequent to each encounter. Therefore, we believe that the TSC's cumulative tally of records reviewed can include records counted multiple times.

- Between September 2006 and April 2007, the TSDB grew at an average rate of over 20,000 records per month. This growth adds to the analysts' workload. Since April 2004, the TSDB has more than quadrupled in size, growing from 150,000 to 724,442 records in April 2007.
- As of February 2007, there were about 3,000 open quality assurance matters that required follow-up.

As part of this review, we obtained TSC data for the number of quality assurance matters identified and resolved between November 2006 and March 2007.¹⁸ These data show that the TSC is identifying incomplete or inaccurate information in TSDB records faster than the matters are being resolved by source agencies. As the following graph shows, cumulative differences between identified quality assurance matters and addressed quality assurance matters increased from 177 in November 2006 to 2,514 in March 2007. This differential also shows that the TSC is regularly identifying errors or concerns with known or suspected terrorist records.



Source: OIG analysis of Terrorist Screening Center data

¹⁸ The TSC only could provide historical data on quality assurance matters since November 2006 when the latest version of the TSDB was deployed.

REDACTED FOR PUBLIC RELEASE

We believe that if the number of watchlist records and the associated quality assurance matters in the TSDB continue to grow, the TSC will not complete the record-by-record review of the TSDB by the end of 2007 as anticipated. The TSC needs to accurately determine the magnitude of the unexamined portion of the TSDB so that the TSC can implement a sound plan for examining those records and develop a realistic completion date for the project. Further, the TSC should establish benchmarks against which it can measure its progress.

Watchlist Redress

We found that the TSC's efforts to resolve terrorist watchlist redress matters since our previous audit have improved. For example, in 2005 the TSC created a dedicated unit for redress matters. The TSC also helped to spearhead the creation of a multi-agency Memorandum of Understanding (MOU) focusing on watchlist redress (Redress MOU) and developed a comprehensive Redress SOP to ensure watchlist information for redress complainants is accurate, complete, and current.

The frontline screening agencies, such as DHS and the State Department, receive complaints from persons seeking relief, or "redress," related to the terrorist watchlist screening process. Matters believed to be related to a terrorist watchlist identity or an encounter involving the watchlist are forwarded to and reviewed by the TSC.¹⁹ The TSC Redress Office conducts an examination of the watchlist records, reviews other screening and intelligence databases, and coordinates with partner agencies for additional information and clarification. The TSC determines if any watchlist records need to be modified or even removed from the watchlist, ensures these identified changes are made, and notifies the referring frontline screening agency of its resolution. The frontline screening agency is then responsible for responding to the complainant. TSC policy requires that responses to complainants neither confirm nor deny the existence of watchlist records relating to the complainant. According to TSC officials, this nondisclosure policy protects U.S. counterterrorism operations and intelligence objectives and safeguards the personnel involved in these sensitive activities.

We judgmentally selected 20 redress complaints received by the TSC between January 2006 and February 2007 and reviewed the corresponding files to determine if the TSC followed its Redress SOP for resolving

¹⁹ On occasion, the TSC receives a redress complaint referral from a screening agency and determines that the complaint does not relate to a terrorist watchlist identity or an encounter involving the watchlist. The TSC returns such complaints to the referring agency for resolution.

REDACTED FOR PUBLIC RELEASE

complaints. We found that in each of the sampled cases the TSC complied with its Redress SOP, including reviewing the applicable screening and intelligence databases, coordinating with partner agencies, and reaching appropriate resolutions. However, the TSC's redress activities identified a high rate of error in watchlist records. In addition, we believe the TSC needs to address the timeliness of redress complaint resolutions.

Significant Watchlist Record Changes Following TSC Redress Review

As part of our review, we analyzed TSC data on the resolution of terrorist watchlist redress complaints. Between January 2005 and February 2007, the TSC closed 388 of the 438 redress complaints it received. Through its comprehensive redress review process, the TSC concluded that 45 percent of the watchlist records related to redress complaints required modification or deletion from the watchlist. In some instances, the TSC stated that redress resolution may have been simultaneous to current watchlist record updates. We also found instances where the TSC Redress Office found inaccuracies in the watchlist record or discovered additional, relevant information that had not been passed to the TSC.

The Privacy Officer acknowledged that the high percentage of records requiring modification or removal may point to deficiencies in the terrorist watchlist nomination process and with nominating agencies not providing the TSC additional information important for appropriately updating terrorist records. We believe that the results of the TSC's redress reviews are a further indicator that watchlist data needs continuous monitoring and attention.

Untimely Resolution of Redress Complaints

The TSC is responsible for adjudicating watchlist-related complaints through its review process and working with nominating and screening agencies to resolve the matters in a timely fashion. The Redress MOU states that one of the goals of the redress process is to provide a timely review, which ensures any required changes to the watchlist are implemented efficiently so that watchlist records do not continue to be inaccurate.

We reviewed TSC files and statistics for closed redress matters to determine the efficiency of redress reviews. This data revealed that it took the TSC, on average, 67 days to close its review of a redress inquiry. For redress matters referred to the TSC during the last semiannual period in our review (July through December 2006), it took the TSC an average of 57 days to finalize its review. In addition to these closed matters, we also

REDACTED FOR PUBLIC RELEASE

analyzed the 50 open redress complaints as of February 27, 2007, and determined that these matters had been open an average of 61 days. Of these complaints, 38 percent were open over 60 days, including 2 inquiries that were pending over 180 days.

Open TSC Redress Matters
(as of February 27, 2007)

Number of Days Open	Number of Open Redress Matters	Percentage of Total Open Redress Matters
180 days or more	2	4%
90-179 days	12	24%
60-89 days	5	10%
30-59 days	11	22%
less than 30 days	20	40%
Total	50	100%

Source: The Terrorist Screening Center Redress Office

Our review of redress files indicated that delays were primarily caused by three factors: (1) the TSC took a long time to finalize its determination before coordinating with other agencies for additional information or comment, (2) nominating agencies (the FBI and NCTC) did not provide timely feedback to the TSC or did not process watchlist paperwork in a timely manner, and (3) certain screening agencies were slow to update their databases with accurate and current information. For example, our file review found that the State Department and the DHS's Customs and Border Protection did not revise encounter records in a screening database in a timely fashion to reflect modified or removed terrorist identities.

TSC officials acknowledged that it has not developed response timeframes for redress matters with its partner agencies. While the Redress MOU states that one of the goals of the redress process is to provide a timely review, the MOU does not define what constitutes a reasonable timeframe. We believe that timeliness measures could be used as standards to evaluate the U.S. government's efficiency in resolving terrorist watchlist redress inquiries and responding to complainants. Because the TSC is central to resolving any complaint regarding the content of the consolidated terrorist watchlist, we encourage the TSC to organize the U.S. government's effort to develop timeliness measures for the entire watchlist redress process.

REDACTED FOR PUBLIC RELEASE

More Proactive Efforts Needed to Mitigate Incidence and Effect of Watchlist Misidentifications

The TSC does not have any policy or procedures to proactively use information from encounters to reduce the incidence and impact of terrorist watchlist misidentifications. For example, the TSC could program its encounter tracking system to automatically generate a quality assurance lead for the TSC to perform a comprehensive review of watchlist records that have been the subject of a certain number of encounters. Moreover, the TSC's strategic plan does not include goals or actions associated with reducing the incidence of misidentifications or the impact on misidentified persons other than that covered by a formal redress process. Considering that nearly half of all encounters referred to the TSC Call Center are negative for a watchlist match, we believe the TSC should consider misidentifications a priority and develop strategic goals and policy specific to mitigating the adverse impact of the terrorist screening process on non-watchlist subjects, particularly for individuals who are repeatedly misidentified as watchlist identities.

Conclusion and Recommendations

We found that since our June 2005 report the TSC has enhanced its staffing and implemented practices to handle redress matters and help ensure the quality of terrorist watchlist information. Our review also found that the TSC's processes for examining watchlist records as part of its special project (the No Fly list examination) and redress complaint reviews were comprehensive and improved watchlist data quality.

However, we found continued weaknesses in other watchlist processes and significant deficiencies in watchlist data. We determined that the FBI's fragmented international terrorism nomination process caused many terrorist identity records to be inaccurate, incomplete, and inconsistent across watchlist systems. Additionally, the TSC's single review queue and encounter-driven quality assurance processes were not successful in ensuring the quality of watchlist records. We also found that TSC quality assurance analysts employed disparate procedures in their reviews, and the TSC did not have a mechanism for conducting oversight of its quality assurance efforts.

We believe the TSC should consider incorporating elements from its more comprehensive reviews in its other quality assurance processes to help better ensure the quality of watchlist data. Further, the TSC should develop detailed, comprehensive standard operating procedures and an oversight function for quality assurance matters.

REDACTED FOR PUBLIC RELEASE

In addition to these process deficiencies, we found suspected or known terrorists still missing from the watchlist or downstream screening systems, incorrect terrorist handling codes on watchlist records, and duplicate identity records within the TSDB. Moreover, our testing of specific watchlist records revealed that records submitted to a TSC quality assurance review contained significant errors –38 percent of the records tested contained data that was inaccurate, incomplete, inconsistent, or not current. Further, our examination of TSC redress data for positive-match encounters showed that the TSC determined that 45 percent of the watchlist records referred for review required modification or removal. In addition, watchlist agencies, including the TSC and nominating and screening agencies sometimes caused unnecessary delays in closing redress inquiry reviews.

The results of our testing of watchlist records, as well as the TSC finding that many records involved in its redress reviews required modification or removal, indicate a deficiency in the integrity of watchlist information. We recommend that the TSC resolve current process weaknesses – within the TSC and at nominating agencies – that are contributing to the weaknesses we identified in the watchlist data. The TSC also needs to develop and implement a plan to complete a sufficient analysis of all watchlist records in a timely fashion.

This report contains 18 recommendations to help the TSC improve its operations and the quality of watchlist data. These recommendations include two recommendations to the FBI directly for matters pertaining to its operations outside the TSC.

**FOLLOW-UP AUDIT OF THE
TERRORIST SCREENING CENTER**

TABLE OF CONTENTS

INTRODUCTION 1

 PURPOSE OF THE CONSOLIDATED WATCHLIST 2

 OVERVIEW OF WATCHLIST NOMINATION AND SCREENING PROCESSES 3

 TSC ENCOUNTER MANAGEMENT 6

 NUMBER OF TERRORIST WATCHLIST RECORDS 7

 HANDLING INSTRUCTIONS 8

 OIG’S AUDIT APPROACH 10

FINDINGS AND RECOMMENDATIONS 12

I. DATA ACCURACY AND TIMELINESS 12

 STRUCTURE OF THE TSDB 12

 RECORDS NOT DESIGNATED FOR ANY WATCHLISTING 17

 FBI PROCEDURE FOR PROCESSING WATCHLIST DATA 18

 DUPLICATE RECORDS 20

 INCLUSION OF KNOWN TERRORISTS IN THE TSDB 24

 CONCLUSION 24

 RECOMMENDATIONS 25

II. QUALITY ASSURANCE 27

 OVERVIEW OF THE TSC’S QUALITY ASSURANCE PROCESS 27

 OIG ANALYSIS OF TSC QUALITY ASSURANCE EFFORTS 31

 QUALITY ASSURANCE MANAGEMENT AND OVERSIGHT 35

 TSC EFFORTS TO ENHANCE TERRORIST WATCHLISTING 41

 CONCLUSION 42

 RECOMMENDATIONS 43

III. TERRORIST WATCHLIST REDRESS 45

 OVERVIEW OF THE TSC’S REDRESS EFFORTS 45

 MULTI-AGENCY REDRESS AGREEMENT 47

 OVERVIEW OF THE TERRORIST WATCHLIST REDRESS PROCESS 47

 DISPOSITION OF REDRESS COMPLAINTS 51

 TIMELINESS OF PROCESSING REDRESS COMPLAINTS 53

 RESPONSE TO REDRESS COMPLAINANTS 56

 APPEAL OF REDRESS DISPOSITION 57

 PROACTIVE REDRESS 57

 CONCLUSION 59

 RECOMMENDATIONS 60

STATEMENT ON INTERNAL CONTROLS..... 61
STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS 62
APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY..... 63
APPENDIX II: SYSTEMS USED IN THE TERRORIST
WATCHLIST PROCESS 67
APPENDIX III: DIAGRAM OF TERRORIST WATCHLIST DATAFLOW... 69
APPENDIX IV: ACRONYMS 70
APPENDIX V: TERRORIST SCREENING CENTER RESPONSE 71
APPENDIX VI: OFFICE OF THE INSPECTOR GENERAL
ANALYSIS AND SUMMARY OF ACTIONS
NECESSARY TO CLOSE THE REPORT 77

INTRODUCTION

Prior to the establishment of the Terrorist Screening Center (TSC), the federal government relied on at least a dozen separate terrorist watchlists maintained by different federal agencies. The TSC was created by Homeland Security Presidential Directive-6 (HSPD-6), signed on September 16, 2003. In that directive, the TSC was required to integrate the existing U.S. government terrorist watchlists and provide 24-hour, 7-day a week responses for agencies that use the watchlisting process to screen individuals who, for example, apply for a visa, attempt to enter the United States through a port-of-entry, attempt to travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation. HSPD-6 mandated that the TSC achieve initial operating capability by December 1, 2003.

The TSC is a multi-agency organization administered by the Federal Bureau of Investigation (FBI). Following the issuance of HSPD-6, the Attorney General, the Director of Central Intelligence, and the Secretaries of the Department of Homeland Security (DHS) and the Department of State (State Department) entered into a Memorandum of Understanding (MOU) describing the new organization and the level of necessary cooperation, including the sharing of staff and information from the four participating agencies. The MOU stipulated that the Director of the TSC would report to the Attorney General through the FBI and required that the Principal Deputy of the TSC be an employee of DHS. Since fiscal year (FY) 2004, the participating agencies have shared responsibility for funding and staffing the TSC, and for FY 2007 the TSC has a budget of approximately \$83 million and 408 positions.²⁰

In June 2005, the Department of Justice (DOJ) Office of the Inspector General (OIG) issued an audit report that examined the TSC's operations from the time of its inception.²¹ The OIG reported that although the TSC had made significant strides in becoming the government's single point-of-contact for law enforcement authorities requesting assistance in identifying individuals with possible ties to terrorism and had developed a consolidated terrorist watchlist database, the TSC had not ensured that the information in that database was complete and accurate. For example, we found instances where the consolidated database did not contain names that should have been

²⁰ As of June 2007, the TSC had 323 personnel on board.

²¹ Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center*, Audit Report 05-27, June 2005.

REDACTED FOR PUBLIC RELEASE

included on the watchlist. In addition, we found inaccurate or inconsistent information related to persons included in the database. In that review, we also found problems with the TSC's management of its information technology (IT), an integral part of the terrorist screening process.

TSC officials attributed some of these deficiencies to the immediate need during the earliest days of the TSC to develop a comprehensive database of potentially high-risk suspects. TSC officials explained that blending different types of data in various formats from multiple sources with varying technological infrastructures had resulted in data inconsistencies and inaccuracies. In addition, technology challenges and frequent record additions, deletions, and modifications affected the TSC's ability to ensure the quality of the watchlist data. Our report included 40 recommendations to the TSC addressing areas such as database improvements, data accuracy and completeness, and staffing.

The purpose of our current follow-up review of the TSC was to determine if accurate and complete records are disseminated to and from the watchlist database in a timely fashion, as well as to assess the TSC's current processes for ensuring the quality of the known or suspected terrorist information. Further, we examined the TSC's efforts to minimize the impact on individuals misidentified as watchlist subjects.

Purpose of the Consolidated Watchlist

One goal of the nation's counterterrorism efforts is to identify suspected terrorists and keep them out of the United States and from harming U.S. citizens both at home and abroad. An essential element of these efforts is the maintenance of a consolidated watchlist containing the names of known and suspected terrorists. This consolidated watchlist should include the most current and complete information and not contain inaccurate, inconsistent, or inappropriate information. Further, similar names and limited information in the watchlist can impair a frontline screening agent (such as a border patrol officer, visa application reviewer, or local police officer) from distinguishing between a suspected terrorist and a mistakenly identified individual. Deficiencies in the terrorist watchlist information also increase the opportunity for a terrorist to go unnoticed or not be properly handled when encountered. Additionally, inadequate information increases the possibility of individuals being misidentified as terrorist watchlist subjects and thereby being detained for more rigorous screening procedures.

Overview of Watchlist Nomination and Screening Processes

When a law enforcement or intelligence agency has identified an individual as a potential terrorist threat to the United States and wants that individual watchlisted, the source agency must nominate that person for inclusion in the consolidated watchlist maintained by the TSC. Similarly, as additional information is obtained that either enhances the identifying information or indicates that the individual has no nexus to terrorism, the record should be either updated or deleted.

All nominations from source agencies to the consolidated watchlist are vetted through the FBI or the National Counterterrorism Center (NCTC).²² Analysts at NCTC or the FBI review the nomination information and decide whether or not the person is an appropriate candidate for inclusion on the consolidated watchlist. This review includes an evaluation of the information supporting the nomination, an examination of the quality and accuracy of the identifying information, and an examination of whether sufficient identifying information is available.²³ The FBI and NCTC are responsible for providing the TSC an unclassified subset of identifying information for individuals known or suspected to be or have been involved in activities related to terrorism.²⁴

²² As stated in the TSC MOU, source agencies responsible for U.S. counterintelligence, counterterrorism, and law enforcement provide information to the FBI and NCTC on suspected or known terrorists who are nominated for inclusion on the consolidated terrorist watchlist maintained by the TSC. The FBI is responsible for submitting to the TSC all domestic terrorist identity nominations, and NCTC is responsible for international terrorist identity nominations. While the FBI is a source agency for domestic and international terrorist information; it forwards relevant information to NCTC on suspected or known international terrorists. Domestic terrorist information is defined as information about U.S. persons that has been determined to be purely domestic terrorism information with no link to foreign intelligence, counterintelligence, or international terrorism.

²³ The TSC's general criterion for including a record on the consolidated watchlist is that the nominating agency must have provided evidence of a nexus to terrorism. From a data perspective, the minimum criteria for inclusion of a terrorist identity into the TSDB are that the record contains at least a partial name (e.g., given name, surname, or both) and at least one additional piece of identifying information (e.g., date of birth).

²⁴ The TSC also has an emergency nomination process, which is used when there is an imminent threat and a watchlist record needs to be highlighted or created quickly. Under the emergency process, a requesting agency informs the TSC directly and the TSC adds the individual to the consolidated watchlist. The TSC then forwards all the information gathered on the subject to NCTC for subsequent additional vetting and creation of a record at NCTC.

REDACTED FOR PUBLIC RELEASE

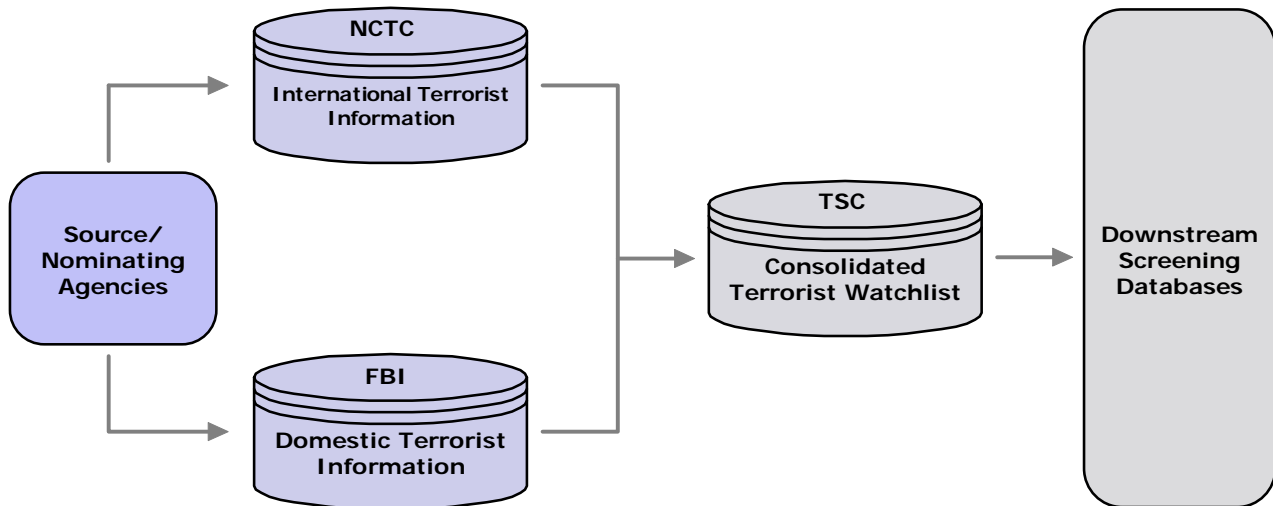
The TSC shares the terrorist information contained in its Terrorist Screening Database (TSDB) by exporting or sending data “downstream” to other screening systems, such as the State Department’s Consular Lookout and Support System (CLASS), DHS’s Interagency Border Inspection System (IBIS), the Transportation Security Administration’s (TSA) No Fly list, the FBI’s Violent Gang and Terrorist Organization File (VGTOF) within its National Crime Information Center (NCIC) system, and others.²⁵ Watchlist information is then available for use by U.S. law enforcement and intelligence officials across the country and around the world.

Personnel working for these organizations routinely encounter individuals as part of their regular duties during various government processes. For example: (1) DHS agents of the U.S. Customs and Border Protection (CBP) agency examine individuals at various U.S. ports-of-entry and search IBIS to determine if a person can be granted access to the United States, (2) State Department officials process visa applications from non-U.S. citizens wishing to visit the United States and search CLASS to determine if the individual should be granted a U.S. visa, and (3) state and local law enforcement officers review the identifying information of individuals encountered through the criminal justice system and query the FBI’s NCIC system. In turn, these databases contain terrorist watchlist records so that the federal, state, and local law enforcement screening agents can identify persons that the U.S. government has determined are known or suspected terrorists.

An overview of the flow of watchlist information from nominating agencies to the TSC and ultimate distribution to downstream screening databases is displayed in Exhibit 1-1.

²⁵ NCIC is a nationwide information system maintained by the FBI that provides the criminal justice community with immediate access to information on various law enforcement data, such as criminal history records and missing persons. The FBI’s Criminal Justice Information Services Division is responsible for managing the NCIC database. A description of each of the downstream screening systems is contained in Appendix II.

EXHIBIT 1-1
Terrorist Watchlist Dataflow Diagram²⁶



Source: The National Counterterrorism Center

Screening Activities and Hits Against the Terrorist Watchlist

When a name appears to be a match against the terrorist watchlist, requestors receive a return message through their database informing them of the preliminary match and directing them to call the TSC. When a call is received, TSC staff in the 24-hour call center assist in confirming the subject's identity.

To do this, the TSC Call Center staff search the TSDB and supporting databases to locate any additional information that may assist in making a conclusive identification. The caller is immediately informed of any negative search result – such as the subject of the inquiry does not match the identity of an individual on the watchlist.

In general, if the subject is positively identified as a watchlist hit or the match attempt is inconclusive, the TSC call screener forwards the call to the FBI's Terrorist Screening Operations Unit (TSOU), the FBI's 24-hour global command center for terrorism prevention operations. The TSOU is then responsible for making further attempts to confirm the subject's identity and, if necessary, coordinating the law enforcement response to the encounter, including deploying agents to take appropriate action.

²⁶ A diagram providing a more detailed look at the flow of data in the U.S. government's terrorist watchlisting process is located in Appendix III.

REDACTED FOR PUBLIC RELEASE

Not all encounters are face-to-face. According to State Department officials at the TSC, when a person located overseas submits an application for a visa, State Department officials search the CLASS database, which receives watchlist information from the TSC. If the search reveals a possible identity match with an individual recorded in the TSDB, the official sends the TSC a cable (a secure, electronic communication). A State Department representative at the TSC reviews the cable along with information from supporting agency databases to determine if the person requesting a visa is an individual with ties to terrorism. This information is then used by U.S. government officials overseas to either process or deny the application.

TSC Encounter Management

To manage information related to "hits" or possible matches against the watchlist, called "encounters," the TSC uses a software application, called the Encounter Management Application (EMA). This system was implemented in July 2004 and includes a record of all encounters since the inception of the TSC. EMA contains the details of all incoming calls, including information about the inquiring law enforcement agency, the databases the TSC staff searched and the information obtained from these systems, the status of the TSC's efforts to confirm an identity match against a watchlist record (i.e., positive, negative, or inconclusive), whether the caller was forwarded to TSOU for further action, and the final disposition of the call. For every inquiry that TSC call screeners refer to the TSOU, the TSC screeners are responsible for obtaining feedback on the disposition of the encounter, such as whether the subject was arrested, questioned, or denied entry into the United States.

EMA provides the TSC with the ability to generate detailed statistics and prepare reports for analysis. Daily status reports are generated from EMA identifying the specific call information, which is reviewed by the TSC's Tactical Analytical Team to identify patterns or threatening circumstances. If any such patterns are identified, the TSC forwards this information to the appropriate intelligence and law enforcement agencies for further review.

As of April 2007, the TSC Call Center had recorded nearly 97,000 watchlist encounters referred by screening agencies since its creation in December 2003. More than 50 percent of this total resulted in a positive identity match. As shown in Exhibit 1-2, 60 percent of the total calls received by the TSC Call Center originated from the U.S. Customs and Border Protection agency.

EXHIBIT 1-2		
Watchlist Encounters Referred to the TSC Call Center by Organization		
<i>(December 1, 2003, through April 30, 2007)</i>		
Referring Agency	Number of Referrals	Percent of Referrals
DHS – CBP	58,266	60
Other Federal	19,965	21
State and Local	17,967	19
Foreign Government	513	<1
Total	96,711	100%

Source: The Terrorist Screening Center

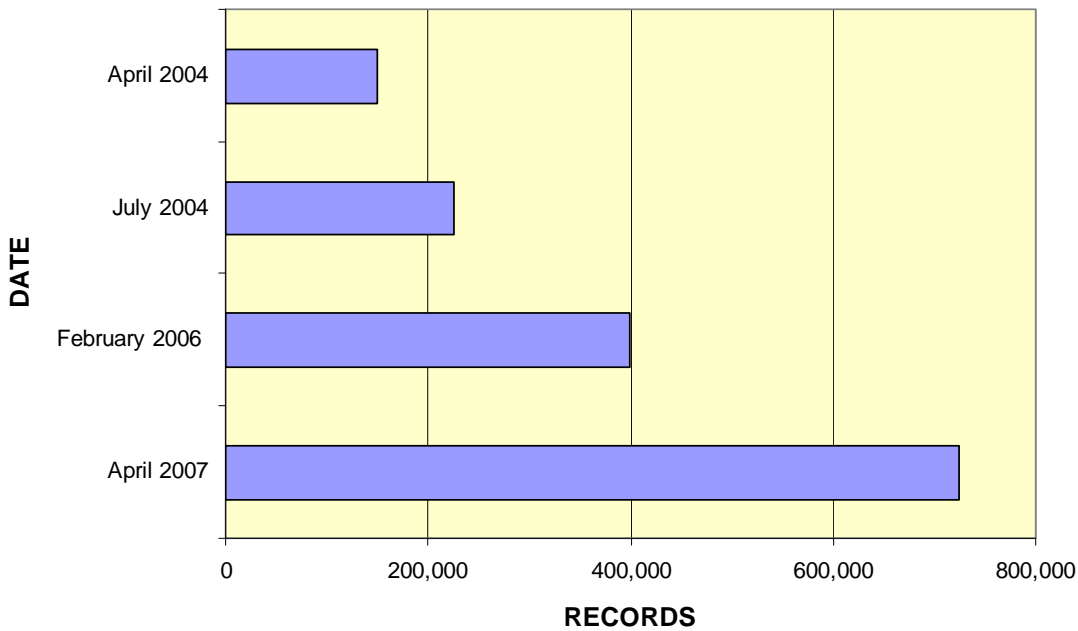
Number of Terrorist Watchlist Records

Since the creation of the TSC in December 2003, the number of records in the consolidated U.S. government watchlist of known or suspected terrorists has significantly increased. We compiled a summary of available database size information, which illustrates the continued growth of the watchlist.

According to TSC officials, there were approximately 150,000 records in the TSDB in April 2004.²⁷ TSC data indicate that by July 2004 the number of records had increased to about 225,000 records, representing approximately 170,000 unique terrorist identities. Eighteen months later, in February 2006, the TSC reported that the database contained approximately 400,000 records. Most recently, information we obtained from the TSC indicates that the TSDB contained a total of 724,442 records as of April 30, 2007. The vast majority of these records are international terrorist records – less than 1 percent of records related to the identities of suspected domestic terrorists. As shown in Exhibit 1-3, the number of watchlist records contained in the TSDB has more than quadrupled since its inception in 2004.

²⁷ The reported figure represents the number of *records* in the system. This does not equate to the number of known or suspected terrorists in the system as a single person may have multiple records to account for the use of aliases, alternate identities, and multiple identifying documents. As such, the number of records generally will be larger than the number of suspected or known terrorists on the watchlist.

EXHIBIT 1-3
Number of Terrorist Watchlist Records



Source: OIG analysis of Terrorist Screening Center data

Handling Instructions

Each record within the consolidated watchlist database is designed to contain information about the law enforcement action to be taken when encountering an individual on the watchlist. This information is conveyed through two separate “handling codes” or instructions – one handling code for the FBI and one for the DHS.

FBI Handling Codes - each individual nominated for inclusion in the FBI’s screening database, National Crime Information Center’s (NCIC) Violent Gang and Terrorist Organization File (VGTOF), is assigned a code used to provide instruction for handling the individual. These codes are assigned based on whether there is an active arrest warrant, a basis to detain the individual, or an interest in obtaining additional intelligence information regarding the individual.²⁸ Following are the definitions for each code.

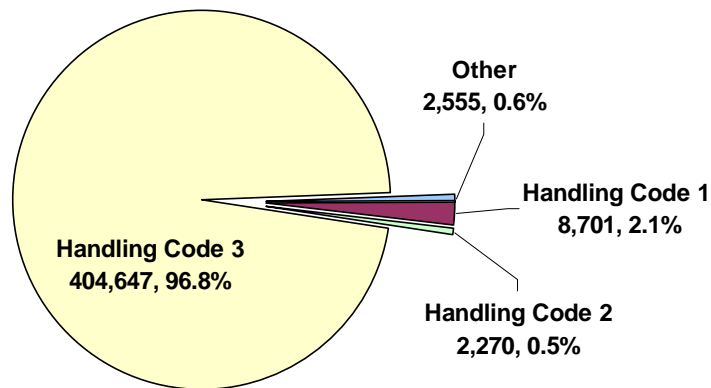
- Handling Code 1 - [SENSITIVE INFORMATION REDACTED]
- Handling Code 2 - [SENSITIVE INFORMATION REDACTED]

²⁸ Practices and procedures regarding one handling code are classified Secret, and are not, therefore, discussed here.

- Handling Code 3 - [SENSITIVE INFORMATION REDACTED].

All records in the consolidated watchlist database that are eligible for export to VGTOF should have a handling code assigned. Based on our review, we determined that all eligible records contained in the TSDB contained a VGTOF handling code. As depicted in Exhibit 1-4, the majority of the records in the TSDB are designated as Handling Code 3.

EXHIBIT 1-4
Distribution of VGTOF Handling Codes
(as of March 6, 2007)²⁹

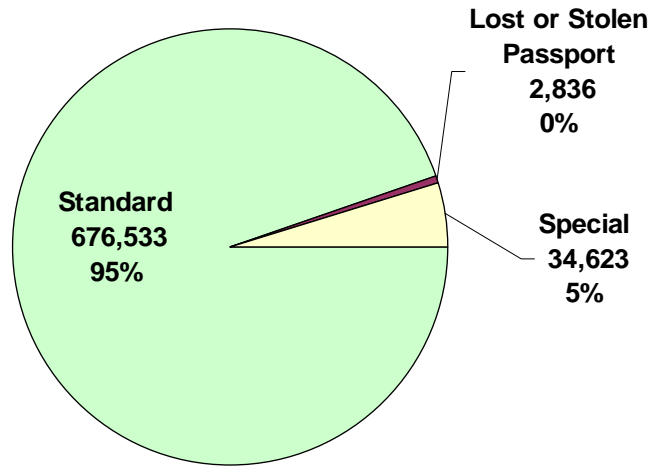


Source: The Terrorist Screening Center

DHS Handling Instructions – each individual nominated for inclusion in the DHS’s screening database is assigned one of three codes that provide instructions to law enforcement officials at ports-of-entry. According to TSC officials, each instruction requires the individual to receive additional screening. However, one code provides a less intrusive method for handling known or suspected terrorists because the law enforcement officer is directed to not meet the individual at the arriving plane and not alert the subject of his or her possible watchlist status. Based on our review, we determined that all eligible records in the TSDB contained an IBIS handling instruction. As shown in Exhibit 1-5, approximately 5 percent of the records in the TSDB that are eligible for export to IBIS are designated with this special handling instruction.

²⁹ The other category relates to the handling code practices and procedures that are classified at the Secret level.

EXHIBIT 1-5
Distribution of IBIS Handling Instructions
(as of April 30, 2007)



Source: The Terrorist Screening Center

OIG's Audit Approach

The objectives of this OIG audit were to: (1) determine if accurate and complete records are disseminated to and from the watchlist database in a timely fashion; (2) review the TSC's efforts to ensure the quality of the information in the watchlist database; and (3) assess the TSC's efforts to address complaints raised by individuals who believe they have been incorrectly identified as watchlist subjects.

To accomplish these objectives, we interviewed more than 45 TSC officials, including the Director, the former Acting Director and Deputy Directors, as well as officials at NCTC, the FBI, and DHS. In addition, we interviewed participating agency representatives and toured facilities to ensure that we obtained a detailed understanding of the working relationships utilized, assistance provided, and communication flow during the terrorist screening process.

To evaluate the accuracy and completeness of the consolidated watchlist, we divided our review into two separate tracks. First, we analyzed the consolidated database as a whole, including a review of the number of records in the database, any duplication that existed within those records, and the associated watchlist processes. Second, we tested individual records within the database for accuracy and completeness. This included reviewing a sample of FBI and other government agency nominated domestic and international terrorist records and tracing these records to the TSDB to determine if the individuals were included in the database and that

REDACTED FOR PUBLIC RELEASE

the information was accurate, complete, and consistent. In addition, we also checked whether known terrorist names were in the database.

To assess the TSC's efforts to ensure the quality of the information in the watchlist database, we examined the TSC's quality assurance activities and reviewed records subjected to these processes. We also examined the timeliness of the TSC's efforts to resolve matters arising from its review of the accuracy and completeness of the data. This included an evaluation of the TSC's progress to conduct a system-wide, record-by-record review and to improve its quality control processes as a result of recommendations in our previous audit.

To fulfill our third objective, we examined the TSC's policies and procedures for handling inquiries related to individuals who raised complaints following their involvement in a screening encounter. This process is referred to as redress. We evaluated the TSC's efforts to coordinate redress response efforts with other participating agencies, reviewed a sample of redress inquiries, and assessed the timeliness of the TSC's responses to redress inquiries.

Detailed information regarding our audit objectives, scope, and methodology is contained in Appendix I.

FINDINGS AND RECOMMENDATIONS

I. DATA ACCURACY AND TIMELINESS

Our prior audit in June 2005 found that the TSC was operating two vastly different versions of the TSDB and the TSC lacked sufficient internal controls to ensure the integrity of the databases, resulting in names excluded from the watchlist and inaccurate and incomplete records. In our current review, we found that the TSC was operating two versions of the TSDB in tandem and the TSC had not taken adequate steps to ensure that the content of the two databases was identical. Further, we found significant numbers of duplicate records. In addition, because of internal FBI watchlisting processes, we found that the FBI bypasses NCTC and the TSC and enters a nomination into a downstream screening system prior to submitting the nomination to NCTC. As a result, the TSC is unable to ensure that consistent, accurate, and complete terrorist information is disseminated to frontline screening agents in a timely manner. Moreover, the TSC had determined that the TSDB contained over 2,000 watchlist records that did not belong in the database. This TSC review also identified at least eight records that were missing from the downstream databases and were therefore not available to frontline screening agents. While we recognize that no process will be perfect, omissions of a terrorist identity, as well as the existence of inaccurate, incomplete, or outdated watchlist records can have significant ramifications. Our findings indicate that the TSC needs to further improve its controls over the TSDB to help ensure the integrity and effectiveness of the watchlist.

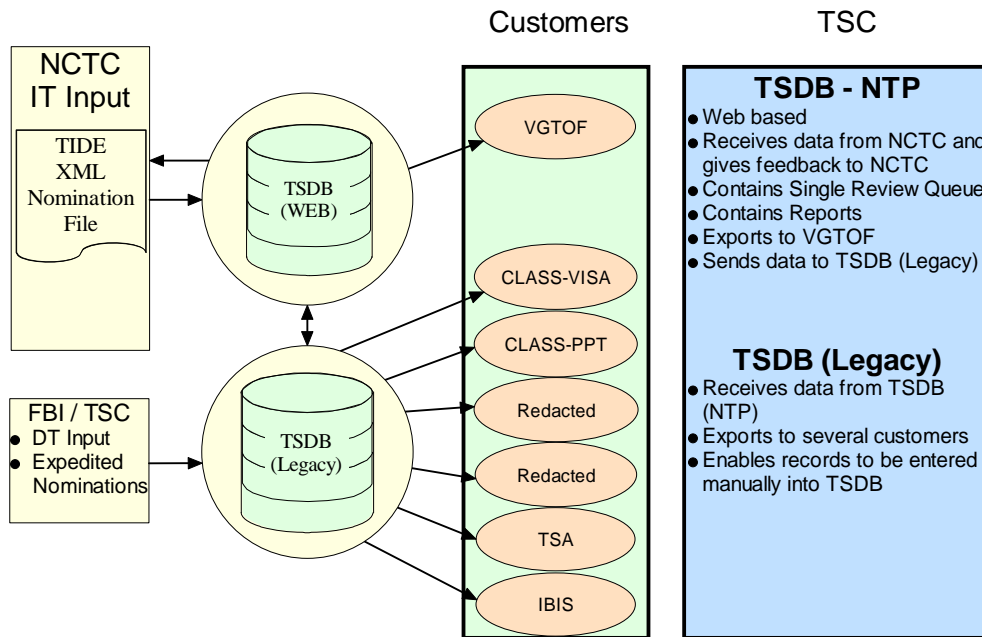
Structure of the TSDB

In concert with NCTC's implementation of its Terrorist Identities Datamart Environment (TIDE) database, the TSC developed a web-based version of the TSDB called the Nomination Tracking Processor (TSDB NTP) in March 2005. As shown in Exhibit 2-1, the TSDB NTP facilitates the receipt of data from NCTC, provides direct connectivity to the NCIC VGTOF data system, and enables the initiation and monitoring of data quality assurance efforts of the TSC.³⁰ However, the TSDB NTP system is unable to export watchlist data to most screening agencies or process expedited and domestic

³⁰ Direct connectivity to the NCIC VGTOF system and quality assurance functionality were established in May 2005 and March 2006, respectively.

terrorist nominations into the TSDB. As a result, the TSC has retained a legacy version of the TSDB to accommodate these processes.³¹ These two versions of the TSDB are interconnected to help ensure that nominations are properly exported to downstream watchlist agencies.

**EXHIBIT 2-1
TSDB Operating Environment**



Source: The Terrorist Screening Center

TSC officials stated that while this operating environment is not optimal, they needed to maintain the legacy version of the TSDB because the TSDB NTP is unable to process expedited nominations or connect electronically with all of the related downstream screening databases. With two versions of the TSDB, however, it is critical that the TSC maintain strong controls to ensure that each name nominated for inclusion in the TSDB NTP is appropriately included in the legacy version and accurately marked for export to the relevant downstream supporting systems in a timely manner.

However, we determined that the TSC did not implement the necessary controls to ensure that both databases contained a complete and accurate version of the terrorist watchlist. Specifically, the NTP and legacy databases were not synchronized, which caused inconsistent record counts between the two systems. As a result, names were omitted from the downstream screening databases. In addition, we noted that records had

³¹ In June 2004, the TSC upgraded its original watchlist, which facilitated the electronic exchange of data with participating agencies' systems.

REDACTED FOR PUBLIC RELEASE

been inappropriately maintained in the TSDB without any watchlist designation. These findings are discussed in detail below.

Inconsistent Record Counts

At the beginning of this audit, we were informed by the TSC Chief Information Officer (CIO) that the NTP and legacy versions of the TSDB were interconnected to help ensure that the watchlist was properly exported to frontline screening agencies. Therefore, the two databases should be identical in content and should contain the same number of records. However, on March 16, 2007, we found that the TSDB legacy database had 689,631 records while the NTP had 689,613 records – a difference of 18 records. Although the difference is a small portion of the universe of records, omitted records can result in a missed opportunity to identify a known or suspected terrorist.

We brought the record discrepancy to the attention of the TSC CIO, who said he was surprised to learn that the systems were not in balance. Upon further review, the CIO learned and reported to us that the IT staff at the TSC was aware that the record counts sometimes varied. Despite the increased risk created by continual transactions between the two databases as well as recent system modifications, the TSC IT staff did not appear to have examined the differences, researched a valid explanation for the discrepancies, or sought a correction for whatever condition was causing the record counts to be out of balance.

Through subsequent analysis, on March 26, 2007, the TSC determined that the record difference between the two databases had increased to 38 records – 5 records were missing from the TSDB legacy system while at the same time it contained an additional 33 records that were not in the TSDB NTP system. These omissions and inaccuracies resulted from problems in a number of different areas.

Records Missing from the TSDB Legacy Database

Because the TSDB legacy database facilitates the export of data to downstream screening databases, any information that is missing from the system is not made available to all appropriate law enforcement and intelligence officials for screening of persons against the watchlist. As a result of our review, the TSC identified five records that were missing from the TSDB legacy system, which caused the exported watchlist to be incomplete.

- One record, nominated on December 22, 2006, was never transmitted from the TSDB NTP system. As a result, this known

REDACTED FOR PUBLIC RELEASE

or suspected terrorist record was not watchlisted for over 3 months. TSC officials were unable to determine why the record was not sent. However, as a result of our review, the TSC subsequently added this record to the watchlist.

- Three records nominated on March 5, 2007, were transmitted by the TSDB NTP system but were never imported into the TSDB legacy system. According to TSC officials, the import process for the file containing these records was interrupted. The individual processing the file should have received a notification that the process failed. However, because multiple files are processed each day, TSC officials could not readily identify who processed the file nor provide an explanation as to why corrective action had not been taken. The TSC CIO stated that as a result of our review, the TSC has taken corrective action by modifying the software so that if the transfer process is interrupted again and the user restarts the program, the application returns to the last successfully imported identity and restarts the process to ensure that no records are lost by the interruption.
- On December 20, 2006, the NTP system appropriately processed a request for the deletion of one record. However, the record was not deleted from the TSDB legacy system at the same time. As a result, this name continued to be inappropriately exported to downstream screening databases for nearly 2 months. On February 6, 2007, the individual was re-nominated by NCTC through the TSDB NTP, resulting in the two systems being synchronized for this record. On February 21, 2007, the original request for deletion was inappropriately processed in the TSDB legacy system resulting in the name not being watchlisted for approximately 1 month until we brought it to the TSC's attention in early March 2007.

TSC officials explained that earlier versions of the TSDB legacy database could not process multiple actions for a single record, such as both a modification and a deletion, within one daily import file. TSC officials also theorized that for this record it appears that the December 20, 2006, file contained both a modification and a deletion. Because the TSDB legacy system processed the modification first, the deletion did not process, remained within the queue, and was processed 2 months after it was submitted. TSC officials stated that they have modified the processing order of the queue to prevent this anomaly from occurring again.

REDACTED FOR PUBLIC RELEASE

Additional Records in the TSDB Legacy Database

As a result of our review, the TSC identified 33 additional records contained within the TSDB legacy system that were omitted from the TSDB NTP system. According to TSC officials, the errors associated with each of the 33 records resulted from deficient historical data and technological complications.³² TSC officials agreed that none of the records should have been included in either database. TSC officials stated that they have now ensured that these records have been submitted to the internal quality assurance unit for corrective action.

Inaccurate Display of Watchlist Designation

The State Department's Consular Lookout and Support System (CLASS) is one of the downstream screening systems that receives watchlist information from the TSDB. CLASS consists of two modules – CLASS/Visa and CLASS/Passport, which are used for processing visa and passport applications. According to State Department policies, individuals who are designated as a U.S. citizen or a U.S. person are ineligible for inclusion in the CLASS/Visa module.³³ Non-U.S. persons are eligible for inclusion in both CLASS/Visa and CLASS/Passport. Therefore, an individual's TSDB record can be exported to CLASS/Visa, CLASS/Passport, or both data systems based upon their status as a non-U.S. person. The TSC has included these criteria in the TSDB legacy software to ensure that watchlist records are correctly nominated and exported to the appropriate CLASS module during the data transfer process.

TSC users viewing the TSDB NTP system see check boxes that clearly identify the downstream screening systems to which each record is disseminated. However, the series of check boxes includes only one CLASS box that does not delineate between CLASS/Visa and CLASS/Passport and has the generic label "CLASS."

The TSC plans to correct the CLASS designation in the TSDB NTP system to appropriately reflect that U.S. persons are not eligible for export to CLASS/Visa. In addition, as part of its planned system upgrades, the TSC

³² Many of these deficiencies are attributable to data inconsistencies and inaccuracies that resulted from the TSC's immediate need during its earliest days to develop a comprehensive database of known or suspected terrorists.

³³ According to TSC standard operating procedures, a U.S. person is defined as either: (1) a citizen of the United States; (2) an alien lawfully admitted for permanent residence; (3) an unincorporated association with a substantial number of members who are U.S. citizens or are aliens lawfully admitted for permanent residence; or (4) a corporation that is incorporated in the United States.

REDACTED FOR PUBLIC RELEASE

intends to modify the TSDB NTP to accommodate designations for both CLASS/Visa and CLASS/Passport. This will help ensure that once the TSC begins to use the NTP system to export watchlist records to the downstream databases, the appropriate records are sent to each of the CLASS modules and individuals are watchlisted in the correct systems.

Future of the TSDB

We were told by TSC officials that they intend to streamline the TSDB by incorporating the functionality of the legacy system into the TSDB NTP and eliminating the legacy version. To minimize the impact on operations, the TSC plans to implement the changes in an incremental and phased approach. TSC officials anticipate that the project will be completed by the end of calendar year 2007.

It is essential that the TSC maintain and distribute to frontline screening agents a complete subset of known or suspected terrorist identity information. Therefore, the TSC should work aggressively to implement its plan to consolidate the TSDB NTP and legacy systems. Further, we believe that for as long as the TSC must maintain its current operating environment, the TSC must closely monitor the content of each to ensure that the record counts agree and that all watchlist records are accounted for and disseminated as appropriate. As a result of our audit, the TSC CIO stated that he had implemented a policy whereby the contents of the two systems are reconciled manually on a daily basis.

Records Not Designated for Any Watchlisting

According to its governing MOU, the TSC is responsible for regularly reviewing the contents of the TSDB and promptly adjusting or deleting outdated information. During the course of our review, we were informed by TSC officials that in September 2006 they had identified 2,682 records that were not being exported to any downstream screening database. Working with NCTC, the TSC confirmed that 2,118 of these records did not belong in the TSDB and needed to be removed from the consolidated watchlist.³⁴ TSC officials conducted a manual review of the remaining 564 records and determined that 8 had not been appropriately watchlisted and needed to be renominated to the TSDB.³⁵

³⁴ On April 27, 2007, the TSC implemented an information technology solution to delete these records.

³⁵ The TSC determined that the 564 records represented 443 unique identities. As of June 15, 2007, the TSC had resolved 413 of the 443 records.

REDACTED FOR PUBLIC RELEASE

Despite being responsible for removing outdated or obsolete data from the TSDB, however, the TSC did not have a process for regularly reviewing the contents of the TSDB to ensure that the database does not include records that do not belong on the watchlist. TSC officials told us that they intend to begin performing a periodic review of the database to identify any records that are being stored in the TSDB that are not being exported to any downstream systems. We believe it is essential that the TSC regularly review the TSDB to ensure that all outdated information is removed, as well as to affirm that all records are appropriately watchlisted.

FBI Procedure for Processing Watchlist Data

The FBI's Terrorist Review and Examination Unit (TRES) receives requests from FBI agents to include individuals with known or suspected ties to terrorism on the terrorist watchlist. These requests are provided on nomination forms, which are also used to modify previous submissions or remove records from the watchlist. Analysts at TRES review the nomination information for accuracy and completeness. Once verified, nomination forms for known or suspected *domestic* terrorists are electronically forwarded to the TSC where a TSC analyst manually enters the information into the TSDB. This information is electronically distributed to the downstream screening agency data systems, including the FBI VGTOF, part of the NCIC system.

By contrast, once the TRES analyst verifies an FBI-generated *international* terrorist nomination, the analyst enters the information into VGTOF directly and then submits the nomination form to NCTC. Following its review and vetting, the NCTC analyst manually enters the information into its database – TIDE – that in turn feeds the information to the TSDB. Because TRES has already entered the record into VGTOF, it is not necessary for the TSC to export the record it receives from TIDE to VGTOF. Therefore, these records are not exported from the TSDB to VGTOF.³⁶ Because these VGTOF records will not receive electronic modifications or deletions from the TSDB, the TSC and TRES have agreed that TRES will be responsible for ensuring FBI-originated international watchlist records in VGTOF are accurate, complete, and current.

The FBI's direct entry of international terrorist watchlist nomination data into a downstream screening database bypasses NCTC and the TSC and makes it difficult for these agencies to carry out their responsibilities related to watchlist nominations and records. In our opinion, this process

³⁶ To alert the TSC of this non-standard entry of records into the TSDB, the TSC implemented a special flag, referred to as "FBI sole source," for FBI-originated international records. This designation precludes all future electronic transactions, including related modifications and deletions, from being exported from the TSDB to VGTOF.

REDACTED FOR PUBLIC RELEASE

does not comport with the nomination and data flow procedures outlined in the MOU and agreed to by the partner agencies, which requires agencies to provide directly to NCTC, rather than directly into a downstream database, information related to known or suspected international terrorists. Additionally, we believe the FBI's practice is cumbersome for the TSC and creates unnecessary data errors, anomalies, and inconsistencies as described below.

To test for data accuracy and consistency, we reviewed a judgmental sample of 50 FBI-originated additions or modifications to the watchlist.³⁷ We found that while the records for the domestic terrorist nominations were generally accurate, the international terrorist nominations were not. We identified 16 records with 28 instances in which the identifying information related to international terrorists was inconsistent between the nomination form, VGTOF, TIDE, TSDB, or other screening systems. According to TSC personnel, TREX analysts frequently augment the data on the nomination forms with information they glean from FBI case files and enter this additional information into the VGTOF system. However, this supplemental case information is not forwarded to NCTC and as a result the information is not included in TIDE, not sent to the TSDB, and not made available, if appropriate, to downstream screening systems. Further, because TREX enters the record into VGTOF before the addition of any other existing information from other government databases to which NCTC has access, this additional information is often not included in VGTOF. As a result, vital information on watchlist subjects is not being shared with all appropriate screening agencies.

In addition, we found that the FBI's procedures for processing international terrorist watchlist nominations are cumbersome for the TSC and can inadvertently create an incomplete watchlist. The difference in procedures between the FBI's and other agencies' watchlist nominations requires TSC analysts to review every incoming international terrorist nomination and indicate within the record whether it is an FBI source record. If a terrorist watchlist record is improperly designated as an FBI source record, the subset of terrorist watchlist records in VGTOF will be incomplete because that record will not be exported to or modified within VGTOF. TSC staff told us that they were also concerned about this because, when reviewing nominations from NCTC, it is often difficult to distinguish between FBI source records and nominations received from other agencies. TSC staff stated that there was a period of time (possibly as long as a year) in which many records had been improperly designated as an FBI-originated

³⁷ The total sample of 50 records consisted of 25 each for domestic and internationally known or suspected terrorists.

REDACTED FOR PUBLIC RELEASE

record or not. In March 2007, the TSC and NCTC addressed this problem by developing a method to permit TSC analysts to more easily identify FBI source records.

In response to these concerns, FBI officials informed us that they had implemented nomination procedures to ensure that FBI international terrorist information was entered into VGTOF in the most efficient manner. Yet, our review of 70 FBI record transactions (50 nominations previously mentioned and 20 deletions) revealed that although the transactions were entered into VGTOF in a timely manner, the transactions were not incorporated in the TSDB in a timely fashion.³⁸ Specifically, 18 of the 70 transactions took more than 5 days for TREX to process, with 1 transaction taking 35 days. In addition, we identified 2 instances in which TREX erroneously delivered nomination forms for domestic terrorists to NCTC that resulted in delays of 6 and 16 days, respectively.

Delays in including terrorist information in the consolidated database present a significant vulnerability to the integrity of the consolidated watchlist. Further, the FBI's current practice of bypassing NCTC and the TSC and entering international terrorist-related data directly into VGTOF increases the likelihood that watchlist information within the TSDB, TIDE, VGTOF, and other downstream databases is inaccurate and incomplete. As a result, we recommend that the FBI, NCTC, and TSC work together to design a more consistent and reliable process by which FBI-originated international terrorist information is provided to NCTC for inclusion in TIDE and disseminated to the TSDB and downstream screening systems, including VGTOF.

Duplicate Records

As shown in Exhibit 2-2, the TIDE and TSDB systems store all information known about an individual in a single "identity" record using five core identifying fields, including [SENSITIVE INFORMATION REDACTED]. However, the downstream screening agency data systems do not store information at the identity level. Rather, the identity information is split into separate watchlist records to reflect unique combinations of the five core fields.

³⁸ Officials from NCTC, the TSC, and TREX stated that each agency attempts to process nominations to the watchlist within 1 day.

EXHIBIT 2-2
Record Overview

[SENSITIVE INFORMATION REDACTED]

Source: The Terrorist Screening Center

Multiple records containing the same unique combination of identifying information can increase the number of records that a call screener must review when researching a specific individual. In addition, when multiple records for a single identity exist, it is essential that identifying information and handling instructions be consistent. Otherwise, the screener may mistakenly rely on one record while a second, more complete or accurate record may be ignored. This can result in important information being missed. Further, inconsistent handling instructions may pose a safety risk for law enforcement officers.

In our June 2005 report, we identified 31 instances in which 5 core identifying fields were the same and recommended that the TSC implement corrective action to address the duplicate records and develop an ongoing process to review the TSDB for duplicate records.

In our current audit, we identified a significant increase in duplicated records – 2,533 repeated combinations in these 5 fields involving over 6,262 watchlist records. For example, one unique combination of the 5 core fields had 19 associated records.

In response to the apparent duplicates we identified, TSC officials explained that the duplicates were the result of multiple TIDE identity records for a single individual, system-generated duplicate records, and

REDACTED FOR PUBLIC RELEASE

improperly processed expedited nominations. TSC officials stated that, while they did not have an ongoing process by which they reviewed the TSDB for duplicate records, as a result of our finding the TSC will review the TSDB on a weekly basis for duplicate records. The results will be forwarded to the TSC's internal quality assurance unit for further review and action.

Multiple Identity Records for the Same Individual

Of the 2,533 instances in which the core identifying fields were the same, TSC stated that most were not necessarily duplicate records. Rather, because the records have different TIDE record numbers, the TSC was unable to independently determine whether these records were duplicates. TSC officials explained that NCTC has indicated to them that many of these occurrences are inherent to old data. For example, prior to the implementation of HSPD-6 in 2003, both the FBI and the State Department may have maintained information regarding a single terrorist identity. During the blending of all sources of international terrorist information, both records may have been included in the TIDE data system resulting in duplicated data. In addition, TSC officials explained that some terrorist information remained classified and, as a result, could not be linked to unclassified data.³⁹ To ensure that the most complete subset of unclassified information was disseminated, NCTC created multiple identity records for some individually known or suspected terrorists. As a result, rather than the optimal one identity record with multiple watchlist records, some individuals have multiple identity records that contain multiple identical watchlist records.

Through additional data analysis of the duplicate records we identified, the TSC identified at least one instance in which both the FBI and another government agency nominated the same individual. Because both records pertain to the same individual, the identifying information and instructions for handling the subject should be consistent. However, we identified significant differences in the handling instructions and warnings for the individual. Specifically, one record indicated that the individual was "armed and dangerous with violent tendencies" and also had a valid federal arrest warrant. The other record did not contain this information. Moreover, our analysis of the instances in which the five identifying fields were the same indicates that at least 20 percent have some discrepancy in handling instruction, identifying information, or watchlist export designation. These

³⁹ By August 2004, the Attorney General, the Director of Central Intelligence, and the Secretaries of Homeland Security, State, Treasury, and Defense signed Addendum A to the original governing MOU. Addendum A contained provisions for the declassification and sharing of terrorist information, including [SENSITIVE INFORMATION REDACTED]. However, the provisions only covered information obtained after August 2004.

REDACTED FOR PUBLIC RELEASE

descriptions and instructions are used by frontline law enforcement personnel to assess and determine the level of threat posed by the individual encountered and help to protect themselves and others. Therefore, it is essential that this information be accurate and consistently applied to all records related to one individual.

Because these multiple records occur in TIDE, the TSC believes the review of the 2,533 possible duplicates more appropriately falls to NCTC. In June 2006, NCTC implemented an Identity and Person Merge project. Through this project, NCTC intends to resolve the duplication of identity data across multiple TIDE identity record numbers. However, until the identity information is consolidated, NCTC analysts should apply new information for an existing individual to each TIDE identity record for the individual. Through this process, NCTC intends to ensure that users of TIDE do not miss information about an individual that is potentially relevant to their work because they viewed the "wrong" TIDE identity when conducting their analysis. NCTC and the TSC anticipate that NCTC initiatives will help to alleviate many of these multiple identity records. However, until corrected we believe that these multiple records can affect a screening agent's ability to protect against terrorism and can also pose significant risks to the safety of frontline law enforcement officers.

System-Generated Duplicates

According to TSC officials, the TSDB should not contain multiple watchlist records for a single identity from TIDE with identical information in the five core identifying fields. We determined that the TSDB contained one TIDE identity with two associated watchlist records with duplicated identifying information. The TSC determined that these two records resulted from a nomination from NCTC in February 2005 in which the two records were either improperly included in the daily import file or an error occurred during the import process on that day. Based on our review, the TSC submitted this record to its internal quality assurance unit, and the duplicate record was deleted.

Expedited Nominations

When the TSC is informed about an individual who poses an imminent threat, it creates an "expedited" watchlist record directly into the TSDB. The TSC then forwards all of the information gathered on the subject to NCTC or the FBI for subsequent creation of a record through the standard nomination process. Once the record is submitted through the standard processes, the original expedited record should be deleted. However, our review of the duplicate record issue identified three expedited records that had been

REDACTED FOR PUBLIC RELEASE

improperly processed and not deleted from the TSDB after the record was submitted through the standard nomination process.

According to TSC officials, these duplicated records (the expedited and subsequent routine nomination) should contain identical information. Our analysis revealed two instances in which either an additional date of birth or passport number was missing. According to the TSC CIO, these three expedited nominations have been submitted to the TSC's internal quality assurance unit for further review, and the duplicated records have been deleted.

Inclusion of Known Terrorists in the TSDB

We also performed limited testing on the TSDB to examine the completeness of the watchlist by determining if known terrorists were included in the consolidated database. We selected for our review a total of 49 names: 10 from NCTC, 4 from news media accounts, 17 from the FBI's Most Wanted list, 16 from the State Department's List of Terrorists under Executive Order 13224, and 2 from the Rewards for Justice website.⁴⁰ We searched the TSDB for these 49 names, and found that each was recorded in the TSDB. TSC officials also said they regularly checked their database against names reported in the news, broadcast on television, or included on lists such as the FBI's Most Wanted.

However, our review of the 49 known terrorist names also revealed that the handling instructions for individuals from the FBI's Most Wanted list had significant discrepancies. Specifically, two VGTOF records indicated that the watchlist subjects were armed and dangerous, but the TSDB records did not reflect this handling instruction. In addition, we identified four records containing discrepancies in identifying information between TIDE and TSDB. As previously discussed, it is essential that the TSC ensure that individuals are properly and consistently recorded in the TSDB and downstream screening systems, so that appropriate actions are taken if the individual is encountered by a frontline screening agent.

Conclusion

It is critical that the TSC ensure that the TSDB contains comprehensive information and that each watchlist record is appropriately disseminated to downstream screening systems in a timely manner. While we recognize that

⁴⁰ The State Department maintains a list of the most wanted terrorist organizations and individuals as specified by Executive Order 13224. The Rewards for Justice website is an organization operated by the FBI, CIA, DOJ, and the State Department.

REDACTED FOR PUBLIC RELEASE

no process will be perfect, the potential effect of omissions of a terrorist identity, or the existence of an inaccurate, incomplete, or obsolete watchlist record, requires the TSC and its partner agencies to take all available actions to minimize such errors.

Despite our identification in our June 2005 audit of deficiencies related to the TSC's information technology management and overall database reliability, our current audit determined that the TSC has not yet implemented routine processes to ensure that the TSDB contained all proper watchlist nominations and did not contain duplicate data resulting from improperly processed records, system malfunctions, and historical data deficiencies. Moreover, despite being responsible for removing outdated or obsolete data from the TSDB, the TSC did not have a process for regularly reviewing and verifying the contents of the TSDB. We believe that it is essential that the TSC regularly review the TSDB to ensure that all obsolete and out-of-date information is removed. Finally, because of internal FBI watchlisting processes, the TSC cannot ensure that accurate and complete terrorist information has been disseminated to downstream screening systems in a timely manner.

Recommendations

We recommend that the TSC:

1. Implement its plan to consolidate the TSDB NTP and legacy databases in a timely manner. In the interim while the two systems coexist, the TSC should establish a formal procedure to regularly review the TSDB NTP and legacy databases to ensure that the information in these systems remains synchronized.
2. Develop procedures to regularly review and test the information contained in the TSDB to ensure the data is complete, accurate, and non-duplicative.
3. Modify the TSDB NTP to accommodate designations for both CLASS/Visa and CLASS/Passport. In addition, the TSC should review and correct the records identified in the TSDB NTP to appropriately reflect that U.S. persons are not eligible for export to CLASS/Visa.
4. Review and correct the records identified in the TSDB NTP to ensure that the IBIS handling instructions are appropriately applied.

REDACTED FOR PUBLIC RELEASE

5. Develop procedures to regularly review the information in the TSDB to ensure that outdated or obsolete data is removed in a timely manner.

We recommend that the FBI:

6. Working with the TSC, revise the watchlist nomination process to provide international terrorist nominations directly to NCTC for inclusion in TIDE, submission to the TSC, and dissemination to all downstream databases, including VGTOF.

II. QUALITY ASSURANCE

Our review indicated that the TSC had the foundations of a sound quality assurance plan that will improve the accuracy of the TSDB. The TSC is also continuing its efforts to perform a record-by-record review of the TSDB. However, we are concerned the TSC has not instituted adequate internal controls to ensure that its quality control initiatives are properly implemented. In addition, the TSC's quality assurance efforts have been hampered by the growth in workload as the size of the watchlist increases.

To test the quality assurance plan, we reviewed 120 TSDB records that had been through the TSC's quality assurance process in FYs 2006 and 2007 and identified several instances in which the individual was not appropriately watchlisted, as well as inconsistencies between the TSDB record and other available information. These inconsistencies make it more difficult for screening agents to determine if encountered individuals are on the watchlist.

Overview of the TSC's Quality Assurance Process

In our June 2005 audit report, we identified weaknesses in the completeness and accuracy of the TSDB. During the TSC's earliest days, it had 12 staff assigned responsibility for nominations and data integrity tasks, including one staff member that was dedicated solely to quality assurance matters. During our initial audit, TSC management acknowledged that the organization needed to focus more attention on ensuring the quality of the watchlist. We recommended that the TSC regularly review and test the information contained in the TSDB to ensure data is complete, accurate, and non-duplicative. We also recommended that the TSC coordinate with participating agencies and establish procedures to identify and resolve missing and conflicting record information.

In response to our recommendations, the TSC increased its quality assurance efforts and implemented a data quality improvement plan that detailed the TSC's intent to conduct a record-by-record review of the TSDB. As of March 2007, the TSC had 34 staff on-board in its Nominations and Data Integrity Unit (NDIU), which is responsible for performing or overseeing

REDACTED FOR PUBLIC RELEASE

all of the TSC's activities related to ensuring the quality and accuracy of the watchlist, including:⁴¹

- Reviewing incoming watchlist data (referred to as the single review queue).
- Performing reviews of historical records following an encounter where the TSC identifies a potential discrepancy in watchlist records.
- Conducting special quality assurance projects, such as performing a targeted review of the No Fly list or individuals with particular handling codes.

Single Review Queue

Implemented in March 2006, the single review queue is a feature of the TSDB that segregates the incoming data feed from NCTC so that quality assurance analysts can test each record before releasing that record for inclusion in the TSDB. Prior to the implementation of the single review queue, each watchlist addition or modification the TSC received underwent numerous, separate reviews by individual subject matter experts (persons who were knowledgeable about the requirements of the specific databases used by various screening agencies). In implementing the single review queue, the TSC sought to make the nomination acceptance and review process more efficient. The single review queue was designed to have individual analysts in the NDIU be responsible for guiding individual records through the process of loading the information into the TSDB. The single review queue begins with the use of a computer program that analyzes incoming records against more than 45 business rules.⁴² A business rule is an automated information technology function in which the record is analyzed for specific deficiencies and compliance with criteria.

Once the business rules have been applied to all of the records received, the records are routed to the NDIU for manual review. Although the TSC has drafted a standard operating procedure (SOP) describing the single review queue process, it does not detail how NDIU analysts should conduct this manual record review. We observed NDIU analysts reviewing records in the single review queue and found that, in general, the review

⁴¹ The NDIU's 34 staff included 7 individuals whose primary duty was to function as a subject matter expert. The remaining 27 staff members were assigned to specific quality assurance tasks and assisted with other quality assurance efforts as necessary.

⁴² The TSC also uses 55 business rules to ensure watchlist criteria are met in exporting records to downstream databases.

REDACTED FOR PUBLIC RELEASE

included: (1) determining whether the person met the criteria for inclusion in the TSDB (i.e., nexus to terrorism and quantity of identifying information); (2) confirming the supporting downstream screening systems to which the record should be exported; (3) resolving any issues identified during the execution of the business rules; and (4) comparing information contained in watchlist nominations, such as [SENSITIVE INFORMATION REDACTED], to source documents and source databases. The NDIU has seven individuals serving as subject matter experts who are consulted when NDIU analysts are unable to resolve all issues related to watchlist nominations prior to these nominations being sent to downstream screening databases. Generally, each record is reviewed by fewer persons than before the implementation of the single review queue. As of March 2007, 10 of the 34 staff members in the NDIU were dedicated to the single review queue.

Encounter-Driven Quality Assurance Reviews

In addition to data integrity work that is performed when new or modified data is processed through the single review queue, the NDIU receives referrals from the TSC Call Center for data checks on specific TSDB records. If a call center operator identifies a potential discrepancy in a watchlist record or obtains additional data relevant to a watchlist subject, the operator alerts the NDIU to perform a quality assurance review of the record. Generally, this occurs following a frontline screening agency's encounter with a watchlist subject.

In April 2005, TSC management began requiring call center operators to perform limited data quality tests while handling encounters. Because the operators have access to all of the databases that interact with the TSDB, they were in a position to point out inconsistencies in the information contained in the records on specific individuals in the various databases. This process was modified slightly in November 2006 when the TSDB was upgraded to incorporate quality assurance activities. As a result of the upgrade, individual watchlist records in the TSDB now contain a record (referred to as a QA ticket) in which TSC staff can record all quality assurance work that has been performed on that record.⁴³ With the upgrade, call center screeners were instructed to create a QA ticket in the

⁴³ Prior to the November 2006 TSDB upgrade, NDIU analysts first used an electronic spreadsheet and then a database commonly referred to as the "quality assurance tracker" to monitor quality assurance matters. NDIU analysts continued to use the quality assurance tracker for matters requiring classified correspondence because classified information cannot be placed into the QA ticket, which is housed within the TSDB – an unclassified system. In April 2007, the quality assurance tracker program was discontinued due to a number of concerns; the concerns and the TSC's interim solution for recording classified quality assurance matters are discussed on page 39.

REDACTED FOR PUBLIC RELEASE

TSDB for each positive screening encounter for which they identified any erroneous or inconsistent information in the database records.⁴⁴ In addition, the call screeners were told to create a QA ticket if they obtained new information that should be added to the watchlist records.⁴⁵

When a call center operator prepares a QA ticket, the TSDB electronically routes the QA ticket to the NDIU for further action. An encounter-driven QA ticket indicates that the encounter revealed that information needs to be added or modified, or it will indicate that a call screener identified a discrepancy with the completeness and accuracy of the records. Upon receipt of QA tickets, dedicated NDIU staff review the information from the call center screener and perform a full quality assurance review of all affected records. The QA ticket is closed when all necessary changes have been communicated to the source agencies and fed back into the TSDB, which then updates the downstream screening databases. As of March 2007, the NDIU had 9 individuals dedicated to responding to QA tickets.⁴⁶

Special Quality Assurance Projects

The TSC also examines historical TSDB records for accuracy and completeness through targeted reviews of specific subsets of the watchlist records. Examples of special projects that the TSC has conducted include a review of TSDB records for individuals on the No Fly list and individuals with particular handling codes. As of March 2007, the TSC assigned 8 of the 34 NDIU staff to these kinds of special projects.

⁴⁴ Each encounter is positive, negative, or inconclusive. A negative encounter occurs when a screening agency contacts the TSC because during a screening event an individual is a potential match to a TSDB record, and the TSC (or other law enforcement responder) determines that the individual is not a match to the name on the watchlist. Conversely, a positive encounter is where the individual encountered is a match to the watchlist. An inconclusive encounter occurs when the TSC is unable to determine if the individual encountered is a match to an individual on the watchlist.

⁴⁵ Encounters offer law enforcement agents an opportunity to obtain additional information about watchlist subjects. For example, if a watchlist subject is positively identified during an attempted border crossing, the federal agent may obtain previously unknown information, such as a new passport number, eye color, or current address.

⁴⁶ These NDIU staff members also address QA tickets generated from TSC quality assurance efforts other than encounter-driven reviews, such as through the single review queue and during ad hoc record quality reviews.

OIG Analysis of TSC Quality Assurance Efforts

To examine the TSC's efforts to ensure the quality of the information in the TSDB, we examined the TSC's review of records in the single review queue and its review of encounters and special projects. In total, we examined 156 TSDB records. Of these 156 records, 36 involved a request for deletion. We determined that each of these records had been appropriately deleted from the consolidated watchlist. Using the remaining sample of 120 records, we performed tests to determine if the watchlist records were accurate. We found that, in general, the TSC's actions to review records as part of a targeted special project successfully ensured the quality of the data, and we identified virtually no errors in the 15 records we tested in connection with special project reviews. In contrast, our examination of 105 records subjected to the single review queue or post-encounter quality assurance reviews revealed that 38 percent of these tested records continued to contain errors or inconsistencies that were not identified through the TSC's quality assurance efforts. Our results are discussed in detail below.

Review of TSC No Fly List Special Project

The first major subset of TSDB records that the TSC began reviewing as a special project was the Transportation Security Administration (TSA) No Fly watchlist records. The No Fly list includes individuals who, in general, are considered a threat to civil aviation and should be prevented from boarding commercial aircraft.⁴⁷

To assist the TSC in its review of the No Fly list, the DHS temporarily assigned 10 federal air marshals to the TSC. The process included a review of the available information for each individual listed on the No Fly list and a determination of whether the individual should remain on the No Fly list. In addition to reviewing each entry on the No Fly list, the TSC performed a concomitant quality assurance review of all information contained in the TSDB's records for individuals on the No Fly list. As a result, all of the TSDB's records associated with individuals who were on the No Fly list underwent a comprehensive quality assurance review.

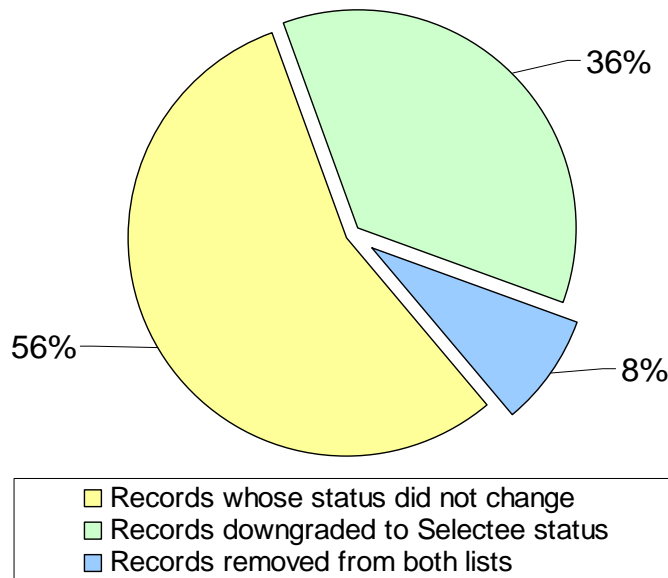
When the TSC began its review in July 2006, the No Fly list contained 71,872 records. As a result of the review, the TSC identified 22,412 records for removal from the No Fly list and placement on the TSA's Selectee list.⁴⁸

⁴⁷ [SENSITIVE INFORMATION REDACTED]

⁴⁸ [SENSITIVE INFORMATION REDACTED]

For another 5,086 records, the TSC determined that the individual did not require inclusion on either the No Fly or Selectee list. The resulting No Fly list changes the TSC identified are displayed in Exhibit 3-1. As of January 31, 2007, the TSC had determined that the No Fly list should contain 34,230 records.⁴⁹

EXHIBIT 3-1
Results of TSC Review of No Fly List



Source: The Terrorist Screening Center Nominations and Data Integrity Unit

We reviewed a sample of 15 TSDB records that had undergone a quality assurance review as part of the TSC's review of the No Fly list. We did not find any data inaccuracies or inconsistencies in the records we reviewed. Each record's basic information [SENSITIVE INFORMATION REDACTED] were shown consistently in all of the affected databases, and each record remained the same or was downgraded from the No Fly list in accordance with the final recommendation from the NDIU.

We did, however, identify an issue with the implementation of the status changes that the TSC identified during its review of the No Fly list. TSC officials told us that although the No Fly records were reviewed at the TSC, the status changes for known or suspected international terrorists could not be reflected in the TSDB until the changes were processed in TIDE

⁴⁹ During its review of the No Fly list, the TSC continued to receive routine No Fly list additions, modifications, and deletions through the watchlist nomination process. As a result, it is not possible to subtract the special project-driven No Fly list changes from the starting point of 71,872 records and obtain the correct number of No Fly records as of January 31, 2007.

at NCTC. The correct watchlisting status could then be uploaded from TIDE to the TSDB during the normal daily data feed. In turn, the TSC would export the No Fly and Selectee lists to the TSA for dissemination to the airlines on a daily basis.

According to TSC officials, NCTC and the airlines told the TSC that they could not effectuate all of the 27,498 changes (22,412 downgrades from the No Fly to the Selectee list plus 5,086 removals from the No Fly list) at once due to resource limitations. TSC management had previously decided not to send any record changes to NCTC until this special project was nearing completion. TSC management explained that TSC analysts needed the time to complete their quality assurance checks for each individual, particularly those with multiple TSDB records. The first changes were sent to NCTC on January 19, 2007. We were told that NCTC and the airlines could only process between 500 and 1,000 record changes a day. As a result, the TSC agreed to limit the number of changes it provided to NCTC and the airlines each day.

This piecemeal approach to implementing the changes in all of the databases meant that the status of many individuals was incorrectly shown on the TSA's No Fly and Selectee lists for a period of time.⁵⁰ According to TSC officials, all of the changes had been passed back to NCTC as of March 21, 2007. However, as of May 31, 2007, the TSC and NCTC were in disagreement about the proper No Fly-list status of 108 records.

Review of Routine Quality Assurance Matters

Unlike our review of the No Fly list special project, our examination of records passed through other TSC quality assurance processes revealed that the reviewed records were still likely to contain errors or inconsistencies. We selected a judgmental sample of 105 new and historical TSDB records that had undergone the single review queue or encounter-driven quality assurance processes.⁵¹ We examined the records to ensure that each record was exported to the appropriate screening databases. Additionally, we reviewed the records to determine if basic information [SENSITIVE

⁵⁰ The period of time for which a record would have been inappropriately watchlisted to the No Fly list could range from a minimum of 1 day to a maximum of about 9 months.

⁵¹ We have consolidated our single review queue and encounter-driven quality assurance sample selection and testing results here for ease of presentation. Although we selected records from different subsets of the TSDB, each had been subjected to the same quality assurance steps in the NDIU, making this consolidation possible. Details of our sample selection and the populations from which we selected them are provided in Appendix I.

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED] was shown consistently in all of the affected databases.

Watchlist Designation and Handling Code Errors

Our review revealed that 7 of the 105 TSDB records examined were not being exported to all appropriate downstream watchlists. Specifically, three records were not exported to CLASS Visa. Moreover, these three records and an additional three records were not exported to [SENSITIVE INFORMATION REDACTED].⁵² Additionally, one record was not properly exported to the Interagency Border Inspection System (IBIS).

We discussed these records with NDIU officials who agreed with our findings. As a result of the TSC's failure to export the four records to IBIS or CLASS Visa, which are used by U.S. screening agencies, the watchlisted individuals could be issued a U.S. visa erroneously or inappropriately allowed to enter the United States. The TSC's failure to export the six records to [SENSITIVE INFORMATION REDACTED] can prevent U.S. allies from identifying known or suspected terrorists and sharing additional intelligence.

Our review also revealed that in two instances the TSDB records did not correctly indicate how the record would be seen within the IBIS system. When records are exported from the TSDB to the IBIS system, watchlist records can be identified with a special, less-intrusive handling code, as described earlier. We identified two TSDB records that were exported to IBIS with the special handling designation but should not be because the subjects were considered armed and dangerous or were not deemed a U.S. person. In addition to incorrect IBIS handling designations, an additional three records contained improper VGTOF handling codes. As discussed earlier, VGTOF handling codes instruct law enforcement officers how to properly handle an encounter with a watchlist subject. Incorrect watchlist designations and handling codes can place frontline screeners at increased risk.

Inconsistent or Incomplete Watchlist Records

Our review of the 105 TSDB records submitted to the TSC's single review queue or encounter-driven quality assurance examinations also revealed that 35 TSDB records and the source or downstream records contained inconsistent identifying information in one or more data fields. In total, we identified 54 instances of inconsistent information. Our results are displayed in Exhibit 3-2:

⁵² [SENSITIVE INFORMATION REDACTED]

EXHIBIT 3-2
TSDB Record Inconsistencies

TSDB Record Field	Inconsistencies ⁵³
-------------------	-------------------------------

[SENSITIVE INFORMATION REDACTED]

TOTAL **54**

Source: OIG analysis of TSDB, TIDE, and VGTOF watchlist records

During our review, it became apparent that both the TSC's quality assurance efforts and our reviews of watchlist records identified errors and inconsistencies in incoming records from the source agencies – NCTC and the FBI. We discussed the watchlist nomination process with NCTC and FBI officials, and both agency representatives stated that records are reviewed for accuracy, completeness, and consistency before the records are forwarded to the TSC. However, these efforts are failing to identify a significant number of deficiencies in the nominated records. The TSC's quality assurance efforts, therefore, are hampered by the inaccurate and incomplete source material.

However, inconsistent records can confuse or delay TSC Call Center operators in their efforts to determine if encountered individuals are a positive match for watchlisted known or suspected terrorists. Further, inconsistent information among databases involved in terrorism screening indicates that at least one record may be incorrect. Incorrect records can also misinform frontline screening agents and contribute to the misidentification and delay of an innocent person or the inappropriate release or admittance of a dangerous individual.

Quality Assurance Management and Oversight

In general, we believe the actions the TSC has taken to improve quality assurance since our last audit are positive steps. We also recognize

⁵³ Each entry in this column represents a TSDB record for which we determined that the identified TSDB record field was not in agreement with TIDE and VGTOF. (We limited our review to those databases.) It is possible for one record to have more than one error, and the overall total is the number of field errors.

REDACTED FOR PUBLIC RELEASE

that it is impossible to completely eliminate the potential for errors. However, we identified inaccuracies in the TSDB that persisted even after undergoing the quality assurance process. This underscores the need for additional actions to ensure that the TSDB is a reliable source of information about known or suspected terrorists. Specifically, as described below, we believe that the TSC should: (1) work with the participating agencies to improve coordination related to quality assurance work, including establishing areas of responsibility and timeframes for following up on quality assurance matters; (2) develop a comprehensive standard operating procedure for quality assurance matters; (3) regularly review the NDIU's quality assurance work; (4) develop a reliable and secure method for tracking quality assurance matters that involve classified correspondence; and (5) develop quality assurance benchmarks to monitor the TSC's progress in conducting a record-by-record review of the TSDB.

Coordinating with Participating Agencies

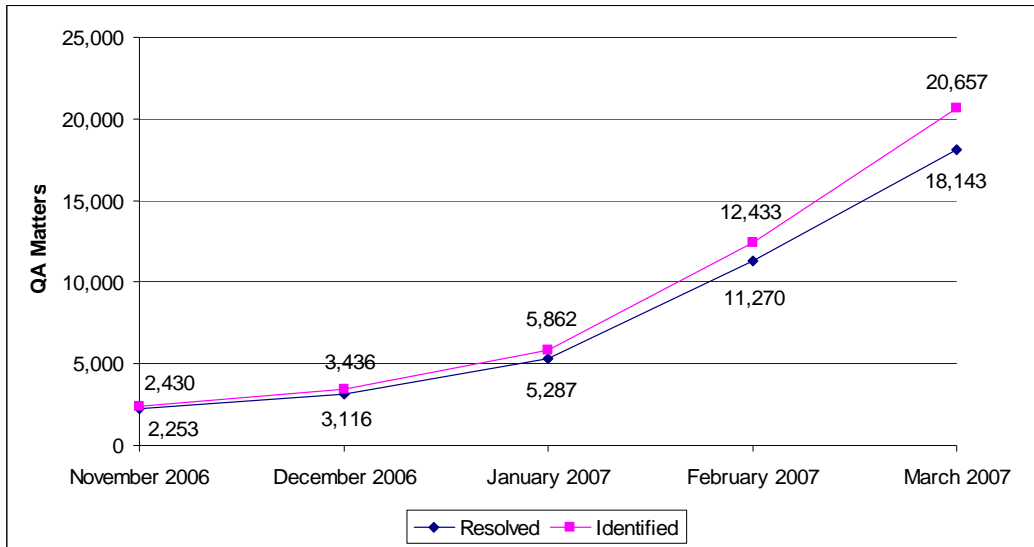
According to TSC personnel, NDIU analysts should follow up on all quality assurance matters every 30 days. However, the TSC does not have a mechanism such as a standardized report or digital dashboard that catalogs all outstanding quality assurance matters.⁵⁴ As a result, NDIU analysts are not prompted to follow up on long-outstanding quality assurance matters for which the TSC is waiting for a response from another agency, such as NCTC. Rather, it is up to each individual analyst to take follow-up action.

We examined a sample of 51 quality assurance matters opened between February 2006 and February 2007 and found that the matters were open from 0 days (the matter was closed the same day as it was opened) to 329 days. On average, quality assurance matters in our sample were open for 80 days. We also obtained TSC data related to the number of quality assurance matters identified and resolved between November 2006 and March 2007.⁵⁵ This data shows that the TSC is identifying incomplete or inaccurate information in TSDB records faster than the matters are being resolved.

⁵⁴ A digital dashboard is a business management tool to visually display the status of a business project. The dashboard can provide warnings, next steps, action notices, and summaries of a project.

⁵⁵ The TSC could provide historical data on quality assurance matters only since November 2006 when the latest version of the TSDB was deployed.

**EXHIBIT 3-3
Cumulative Growth in Quality Assurance Matters**



Source: The Terrorist Screening Center

Exhibit 3-3 shows that the cumulative difference between quality assurance matters identified and addressed has increased from 177 in November 2006 to 2,514 in March 2007. A significant portion of the increase in quality assurance matters processed by the TSC resulted from its implementation of its No Fly special project in January 2007. However, the TSC is regularly identifying errors or concerns with known or suspected terrorist records. To resolve inaccuracies and inconsistencies in watchlist records, the TSC usually must involve the source agencies – NCTC and the FBI. TSC officials acknowledged that the TSC and the participating agencies have not established timeframes for the resolution of quality assurance matters.

We believe that the TSC needs to work more closely with watchlisting agencies to better coordinate quality assurance efforts. This includes setting a standard for the timeliness of response to quality assurance matters, as well as delineating the roles and responsibilities of the various agencies involved. To improve the overall quality of the watchlist, the TSC needs the source agencies to provide records that are accurate, complete, and consistent, and to respond to quality assurance matters within a reasonable time. Without such an agreement, the TSC must expend additional effort to resolve errors that should have been identified earlier in the nomination process and continue to remind watchlist agencies about individual quality assurance matters.

Further, the delayed closure of quality assurance matters directly affects the accuracy of the consolidated watchlist database because records

can contain inaccurate and incomplete information for extended periods of time while the matter is being resolved. Therefore, in concert with the development of established timeframes for resolving quality assurance matters, we recommend that the TSC develop a tickler system or aging schedule for its quality assurance work.

Standard Quality Assurance Procedures

During our audit, we personally observed NDIU analysts conducting quality assurance reviews of watchlist records. We noted that the analysts' method of performing their reviews was not always consistent. For example, some analysts inspected all of the documents supporting a TSDB record, while other analysts relied solely upon summary information. We also found that the analysts were not documenting their quality assurance work consistently. The TSC has an SOP for its quality assurance efforts which was last revised on August 16, 2005. The document did not provide complete guidance to the analysts on the processing of quality assurance matters. Further, this SOP informs the analysts to review the record, but does not detail what fields, supporting information, and other aspects of the record the analysts should be verifying and comparing. In addition, these procedures do not instruct the analysts on the necessary actions to take when inaccurate or incomplete information is identified. Moreover, this protocol does not mention the existence of special projects within the TSC's quality assurance efforts. We believe that the TSC should develop a detailed, comprehensive quality assurance SOP to better guide the NDIU analysts through all aspects of their work.

NDIU Analyst Oversight

The TSC provides only a few days of training to its quality assurance analysts in the NDIU. Following the completion of that training, the analysts begin working independently and no additional routine training or refresher courses are required. However, staff meetings are held on an ad-hoc basis to discuss specific issues that have been encountered. The TSC does not have a mechanism for regularly spot-checking the work of its quality assurance analysts to help ensure that the analysts are performing appropriate reviews and keeping abreast of any process changes. We believe that the TSC should develop a system for performing regular spot-checks of NDIU analysts' work to identify any weaknesses and needs for additional training. This process should be included within the comprehensive quality assurance SOP.

Handling Classified Quality Assurance Matters

Prior to April 2007, the TSC was using an in-house system called quality assurance tracker to catalog all classified correspondence related to quality assurance matters.⁵⁶ However, TSC officials determined that the database: (1) had reached its storage capacity, (2) temporarily lost an estimated 2,000 records in January 2007, (3) did not have a reliable process for backing up the data, (4) did not create any standard management reports, (5) had no method for audit tracking, (6) had not been examined and tested thoroughly by the FBI, and (7) was used by very few staff. Therefore, the TSC shut down the database in April 2007 to prevent any more problems with its use.

The TSC researched several possible long-term methods for tracking classified quality assurance correspondence. As of April 2007, the TSC's temporary method was to use electronic folders on a classified server. We believe that this method will not be an effective method for tracking classified correspondence. In addition, a quality assurance analyst in the NDIU told us that the electronic folder method will be more time-consuming and less useful than tracking their individual correspondence within e-mail accounts and, as a result, some analysts do not plan to use the temporary system. We believe the TSC needs to develop a more effective and user-friendly means for temporary tracking of classified quality assurance correspondence.

⁵⁶ The TSC cannot place classified information into its QA tickets because this information is stored within the TSDB, which is an unclassified system.

REDACTED FOR PUBLIC RELEASE

Progress on the TSC's Record-by-Record Review of the TSDB

In responding to our earlier audit, TSC officials reported that they planned to conduct a record-by-record review of all records within the TSDB. In February 2006, TSC officials estimated that this review would not be complete until 2012. At the time of our current audit, the record-by-record review was ongoing through the three-pronged strategy of the NDIU – the single review queue, encounter-driven quality assurance reviews, and special projects. TSC officials told us that they plan to examine the TSDB following the completion of the on-going special projects and determine how many TSDB records have not yet been reviewed. The TSC then plans to review any previously unexamined records in an effort to examine the entire TSDB.

In February 2007, TSC officials told us that since the inception of the single review queue in March 2006 over 670,000 TSDB records had been reviewed and the agency had revised its estimated completion date. TSC officials now project that the record-by-record review will be complete by the end of 2007.

Yet, we believe that the TSC may have overstated the number of records reviewed and is underestimating the amount of time and effort that it will take to complete its review of the entire TSDB. We base these conclusions on the following factors:

- As previously discussed, the TSC's single review queue and encounter-driven quality assurance processes do not sufficiently ensure the quality of the watchlist records. Therefore, the TSC should reconsider records examined in these processes in its count of records reviewed.
- The number of records reviewed is not limited to the review of unique records. Rather, the TSC's quality assurance process allows for one record to be reviewed multiple times: through the single review queue, following each request to modify or delete the record, in accordance with one or more special projects, and subsequent to each encounter. Therefore, we believe that the TSC's cumulative tally of records reviewed can include records counted multiple times.
- Between September 2006 and April 2007, the TSDB grew at an average rate of over 20,000 records per month, or approximately 174,000 additional records during this 8-month period. This growth adds to the analysts' workload. Since

REDACTED FOR PUBLIC RELEASE

April 2004, the TSDB has more than quadrupled in size, growing from 150,000 to 724,442 records in April 2007.

- In February 2007, there were about 3,000 open quality assurance matters that required follow-up.

We believe that, if the number of records in the TSDB continues to grow at the current rate and the number of quality assurance matters similarly increases, the NDIU will not complete the record-by-record review of the TSDB by the end of 2007 as anticipated. We recommend that the TSC accurately determine the magnitude of the unexamined portion of the TSDB so that agency officials can implement a sound plan for examining those records and develop a realistic completion date for the endeavor. Further, the TSC should establish benchmarks against which it can measure its progress.

TSC Efforts to Enhance Terrorist Watchlisting

Although we identified several actions that the TSC should take to help improve the accuracy and completeness of watchlist records, our audit also revealed a recent TSC initiative that we believe is a noteworthy practice for enhancing watchlist records. Specifically, we noted that the TSC runs a report each week of NCIC hits in VGTOF and compares these hits to positive encounters in its Encounter Management Application (EMA) database to determine if each hit was called into the TSC Call Center. Performing this review offers the TSC an opportunity to educate local law enforcement officers about the importance of the TSC mission and determine if there have been additional known or suspected terrorist encounters of which the TSC was previously unaware. If the encountered individual was a positive identity match to a terrorist watchlist record, then any new information obtained during the encounter should be added into the TSDB record to enrich the record and provide added value to the intelligence community. TSC officials stated that currently they are identifying an average of 40 to 70 encounters each week that are not being called into the TSC. When the TSC identifies a hit that was not called into the call center, this information is relayed to the FBI. In turn, the local FBI field office is asked to follow up with the local law enforcement agency that ran the NCIC check. The FBI field office sends an agent to the local, state, or tribal law enforcement agency to obtain any information about the encounter and to remind the law enforcement agency that they should call all NCIC hits for known or suspected terrorists into the TSC Call Center.

We believe this practice can provide useful information for enriching the watchlist records. However, we noted that although the NCIC hit report

REDACTED FOR PUBLIC RELEASE

is run on a weekly basis, it is taking an additional 2 weeks to notify the FBI of these encounters. Our concern with the 2-week time lag is that some local, state, and tribal law enforcement personnel will not remember clearly the encounter by the time they are contacted by the FBI, which can result in a missed opportunity to obtain new information. TSC officials told us that they are working with the FBI to expedite this process.

We were also told that other law enforcement agencies do not always follow up with the TSC to inform them about any newly obtained encounter information. Considering that approximately 60 percent of the encounters are identified by the CBP, the TSC should explore methods for performing similar enrichment exercises related to other screening agency encounters.

Conclusion

The TSC has made significant strides in its quality assurance efforts since our last review, including the creation of the NDIU and the development of new quality assurance processes. In addition, the TSC's goal to perform quality assurance testing of all new and historical records in the TSDB is a positive step. However, we believe that more needs to be done to ensure the accuracy of the watchlist records.

The number of quality assurance matters identified by the TSC increased from about 2,500 in November 2006 to over 20,000 in March 2007, with the number of unresolved matters increasing from 177 to 2,514 during this period. Additionally, the overall size of the consolidated terrorist watchlist has quadrupled in size since the TSC's inception, increasing from about 150,000 records in April 2004 to over 700,000 as of April 2007. This growth further adds to the amount of work for the TSC quality assurance staff to ensure the quality of the records in the consolidated watchlist database.

Our review found that the TSC has not developed a detailed plan of action and benchmarks or milestones to accomplish its goal of reviewing every record in the watchlist database. Additionally, we found errors in records that had undergone routine TSC quality assurance reviews, but a higher quality for watchlist records examined in TSC special project reviews.

We also found that the TSC's SOP for quality assurance matters did not provide sufficient guidance for analysts to use in performing their examinations of watchlist records. Further, the TSC's oversight and internal controls over the quality assurance process did not detect the continued existence of significant record errors and omissions. Finally, we believe the

REDACTED FOR PUBLIC RELEASE

TSC is hampered by the lack of agreements with the nominating and screening agencies. Such agreements could improve the timeliness for resolving quality assurance matters and help ensure that additional information is obtained during encounters with known or suspected terrorists.

Without a standardized process, adequate internal controls, and agreements with source and watchlist agencies, watchlist records may remain inaccurate and incomplete for an unnecessary amount of time. Before the records are corrected or updated, law enforcement agencies may encounter watchlisted individuals. Additionally, inaccurate records can cause screeners to unnecessarily delay or detain individuals misidentified as a known or suspected terrorist.

Recommendations

We recommend that the TSC:

7. Correct the records identified by the OIG containing incorrect watchlist designations, handling code errors, and inaccurate and inconsistent information.
8. Coordinate with NCTC and the FBI to implement an agreement that establishes the areas of responsibility and the timeframes for data quality assurance matters.
9. Develop a comprehensive standard operating procedure that describes the TSC's three-pronged quality assurance strategy and details the methodology to be used in performing quality assurance reviews.
10. Develop a process to perform regular spot-checks of NDIU analysts' work to identify any weaknesses and need for additional training.
11. Develop an improved and user-friendly process for tracking classified correspondence related to quality assurance matters.
12. Develop a tickler system or digital dashboard for all pending quality assurance matters.
13. Develop a comprehensive plan, including benchmarks or milestones, to complete the record-by-record review of the TSDB.

REDACTED FOR PUBLIC RELEASE

14. Coordinate with other partner agencies to establish a formal process for relevant encounter information to be captured by frontline screening agents and returned to the TSC to update watchlist records.

III. TERRORIST WATCHLIST REDRESS

The TSC has developed comprehensive procedures, has dedicated staff, and coordinates with partner agencies to help ensure that it effectively and efficiently processes complaints from individuals experiencing delays or difficulties due to terrorist watchlist screening. Our review found that the TSC was following its procedures and reaching appropriate resolutions in such redress reviews. TSC redress disposition data indicated that nearly half of the total closed redress reviews resulted in a modification to or removal of a terrorist watchlist record. We believe that the TSC's redress review results provide a further indicator that watchlist data needs continuous monitoring and attention.

We also found that there are excessive delays in closing redress matters. Additionally, we believe that the TSC should use information related to terrorist watchlist identities that are frequently the subject of watchlist encounters to proactively initiate redress reviews before complaints are filed.

Overview of the TSC's Redress Efforts

Persons stopped as a result of watchlist matches may be actual watchlist subjects, individuals misidentified to a terrorist identity, or someone mistakenly included on the watchlist. As a result of the terrorist watchlist screening process, individuals may complain that they were adversely affected and seek relief. Individual government agencies involved in terrorist watchlist screening should have a redress process to effectively resolve the complaint and respond to the complainant. Similarly, the TSC should have reasonable procedures to provide redress for individuals from faulty watchlist identifications.

When we initiated our first TSC audit in 2004, the TSC did not have an established process for handling inquiries related to private individuals who sought watchlist information following their involvement in a screening encounter. In January 2005 the TSC assigned staff to address terrorist watchlist screening complaints and began to develop a strategy for redress matters. In our previous audit report, we recommended that the TSC develop formal procedures for handling redress inquiries. In response, the

REDACTED FOR PUBLIC RELEASE

TSC formalized its process by implementing an official Redress SOP in July 2005 and a revised version in May 2007.⁵⁷

In brief, individuals who believe they were unnecessarily and adversely affected by watchlist-related screening procedures may file a redress complaint with the agency involved in the event. For example, if an individual is prohibited from boarding a commercial airline flight, the person would contact the TSA to file a redress complaint. If the TSA determines that the event was related to terrorist watchlist screening, the complaint is forwarded to the TSC for review. Once the TSC has completed its examination, it makes any necessary changes to associated watchlist records and forwards its results back to the TSA, which provides feedback to the complainant.

In November 2005, the TSC created a separate Redress Office to process redress matters. As of April 2007, the TSC Redress Office was managed by the Redress Officer and supported by four analysts and one management assistant. TSC officials said they plan to expand the Redress Office to seven analysts.⁵⁸ The analysts in this office are responsible for reviewing redress inquiries, corresponding with partner agencies for clarification or additional information, and recommending to the Redress Officer how to dispose of an inquiry. The Redress Officer is responsible for supervising the analysts, reviewing each redress evaluation, facilitating coordination with other agencies, and finalizing the disposition of the redress inquiry.

We believe the TSC has taken a number of other positive steps to address redress matters since our prior audit. For example, the TSC helped to spearhead the creation of a multi-agency agreement addressing watchlist redress. In addition, the TSC has enhanced its own procedures for handling redress matters.

However, in this audit we identified areas in need of continued improvement and further development, such as the timeliness of redress

⁵⁷ The TSC's revised May 2007 Redress SOP includes more detailed guidance and reflects changes within the TSC, such as technology improvements, organization structure, and staffing. The revised Redress SOP also expanded TSC redress disposition categories and provided more detailed instructions on its redress processing as well as the incorporation of new technology and terminology.

⁵⁸ As of April 2007, the TSC allocated six analyst positions to its Redress Office, of which four positions were filled. The TSC reported that it expected to add an additional analyst position for a total of seven.

matter resolution and utilizing encounter information to provide redress without a complaint being submitted. These issues are discussed below.

Multi-agency Redress Agreement

In December 2006, a multi-agency agreement entitled Memorandum of Understanding on Terrorist Watchlist Redress Procedures (Redress MOU) was developed by a working group of representatives from the various agencies involved in terrorist watchlisting and screening. Representatives from the Privacy and Civil Liberties Oversight Board of the Executive Office of the President were also included in the development of the MOU.⁵⁹ As of April 2007, the Redress MOU was being circulated for signature by the heads of the TSC, DOJ, DHS, State Department, the Office of the Director of National Intelligence (ODNI), the FBI, the Central Intelligence Agency (CIA), NCTC, the Department of Defense (DOD), and the Department of the Treasury.⁶⁰

The Redress MOU formalizes the responsibilities of each agency in adjudicating redress inquiries. The agreement requires each agency to assign redress responsibilities to a senior official and commit necessary resources to ensure the efficiency of the redress process and compliance with the Redress MOU. The Redress MOU notes that the TSC has ultimate authority on redress decisions related to the terrorist watchlist.⁶¹

Overview of the Terrorist Watchlist Redress Process

On February 20, 2007, DHS and the State Department implemented the Traveler Redress Inquiry Program (TRIP). This program established a centralized portal for persons to file complaints regarding difficulties experienced at screening points during travel, such as airports, train stations, and border crossings. DHS headquarters officials informed us that TRIP will also help coordinate the resolution of complaints, monitor trends in complaints, and measure redress process efficiencies.

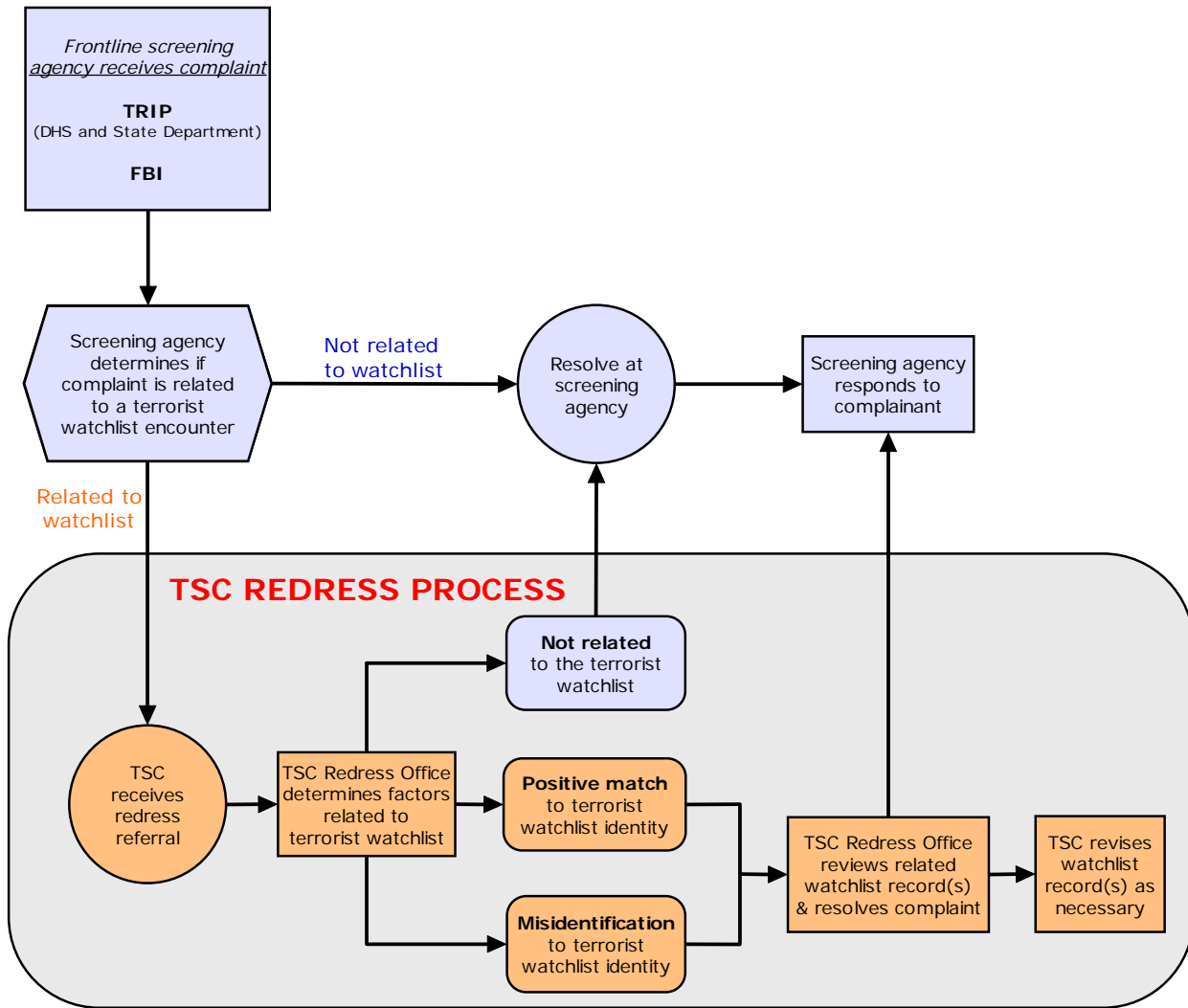
Exhibit 4-1 shows a basic illustration of the U.S. government's process for addressing redress inquiries related to the terrorist watchlist.

⁵⁹ The Privacy and Civil Liberties Oversight Board advises the President and other senior executive branch officials on matters with respect to privacy and civil liberties.

⁶⁰ The TSC reported that as of April 18, 2007, all agencies had signed the agreement except the DOD, the CIA, and the State Department.

⁶¹ The TSA makes final decisions on No Fly list redress appeal matters.

EXHIBIT 4-1
Flowchart of Terrorist Watchlist Redress Process



Source: The Terrorist Screening Center

Receipt of Redress Complaints

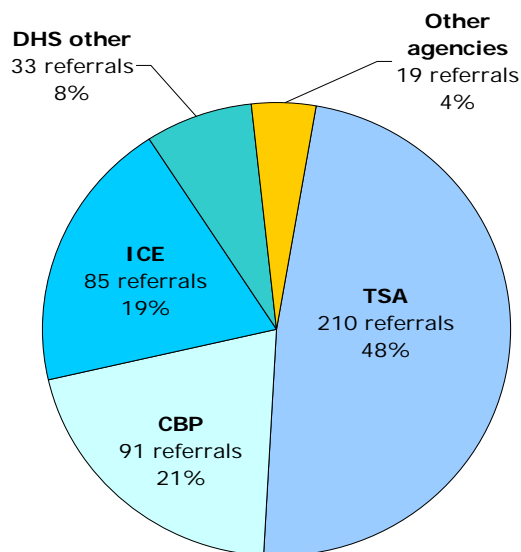
Complainants file redress inquiries with the frontline screening agencies involved in the encounters, such as to the FBI or through TRIP for DHS and the State Department.⁶² As shown in Exhibit 4-1, the screening agency reviews the complaint and determines if the inquiry relates to a possible terrorist watchlist match.

⁶² The FBI is typically not the agency encountering the individual, but its NCIC system is used in the screening process. Therefore, the FBI is considered the screening agency in such instances.

Individuals can also be affected by screening protocols unrelated to the terrorist watchlist, such as through random search procedures or other security screening practices. Despite someone's actual presence or non-presence on the terrorist watchlist, individuals may assume they have been mistakenly included on the watchlist or misidentified to a terrorist watchlist identity and submit a complaint requesting relief. If the screening agency determines that the complaint is not related to the terrorist watchlist, it should resolve the matter internally and respond to the complainant. For example, an airline may deny a person from boarding an airplane because of drunkenness or disorderly behavior. Complaints related to these types of matters and others unrelated to the terrorist watchlist should not be referred to the TSC.

However, the screening agency should refer to the TSC all redress inquiries determined to pertain to a possible watchlist match. From January 2005 through February 2007, the TSC received 438 such redress referrals. As illustrated in Exhibit 4-2, 96 percent of the redress inquiries referred to the TSC were forwarded by DHS components (CBP, TSA, Immigration and Customs Enforcement (ICE), and other DHS entities). The TSA referred nearly one-half of all redress inquiries received by the TSC. Non-DHS agencies referred a total of 19 redress matters, including the FBI (9 referrals), the State Department (3 referrals), state and local law enforcement agencies (6 referrals), and the Executive Office of the President (1 referral).

EXHIBIT 4-2
TSC Redress Referrals by Referring Agency
(January 2005 through February 2007)



Source: The Terrorist Screening Center Redress Office

REDACTED FOR PUBLIC RELEASE

TSC Redress Process

When the TSC receives a redress complaint, the TSC Redress Office analyst assigned responsibility for resolving the complaint determines the relationship of the complainant to the terrorist watchlist and places the individual in one of the following three categories: (1) non-related, (2) positive match, and (3) misidentified.

Non-related – The analyst may determine that the complainant does not match a terrorist watchlist identity and was not the subject of an encounter involving a potential match. Essentially, the inquiry should not have been referred to the TSC in the first place. In these cases, the TSC returns this matter to the appropriate screening agency for resolution.

Positive Match – A complainant who matches an identity on the terrorist watchlist and was the subject of at least one watchlist-related encounter is considered a positive terrorist watchlist match. For positive match redress referrals, a Redress Office analyst conducts a complete review of the watchlist records to ensure information on the individual meets the criteria for watchlisting and is accurate, complete, and current. This review will also include contacting the nominating agency to obtain any new information on the individual not yet available to the TSC.

After reviewing this information, the analyst recommends that a record: (1) remain unchanged, (2) be modified, or (3) be removed from the watchlist. If it is determined that the watchlist record is accurate, complete, and current, the analyst then recommends that no changes be made to the record or the watchlist status of the individual.

For some redress inquiries, the analyst recommends a modification to the record. This could entail updating the record with new information or correcting errors in the record. Another recommended revision may include changing the watchlist status of an individual, such as removing a person from the Selectee list or escalating a person's watchlist status from the Selectee list to the No Fly list.

The last disposition scenario for a positive match record involves removing the identity record from the terrorist watchlist altogether. Based on a review of relevant and current information, the analyst may determine that an identity does not meet the criteria for inclusion on the terrorist watchlist.

Misidentification – An individual who is the subject of a terrorist-related screening but whose identity is not on the terrorist watchlist is

REDACTED FOR PUBLIC RELEASE

considered to have been misidentified. Redress referrals for misidentified complainants are processed by the TSC similarly to positive match referrals. The Redress Office analyst assigned the inquiry reviews the terrorist watchlist record involved in the misidentification and ensures that the record is accurate, complete, and current. The analyst then recommends any necessary changes to the record or watchlist status.

If, as a result of a redress review, the TSC recommends a change to the watchlist record or status (for either a positive match or misidentification referral), the Redress MOU and the TSC Redress SOP both require that the TSC discuss its findings with the nominating agencies. While the nominating agencies may provide input, the TSC has the ultimate authority to resolve all terrorist watchlist redress matters. Finally, the TSC Redress Office ensures that the necessary changes are made to watchlist records before closing its review and alerting the frontline screening agency of its resolution. The TSC does not respond to the complainant. Rather, the TSC coordinates with the frontline screening agency, which should submit a formal reply to the complainant.

The TSC's revised May 2007 Redress SOP includes an expansion of the redress disposition categories. The non-related category was expanded to capture two additional situations: (1) instances in which the TSC administratively closes its review because screening agencies do not comply with TSC redress requirements, and (2) occasions that a redress complaint was considered moot because the terrorist identity to which the redress inquiry refers was already removed from the watchlist through normal watchlist modification or quality assurance procedures. In addition, the TSC renamed its misidentification category to "near match." Lastly, the TSC added one disposition category to use when the TSC Call Center incorrectly identified an individual as a positive watchlist match. The TSC believes its expansion of disposition categories will allow it the ability to better track its redress resolutions and to identify areas in the watchlist process that could be improved. For instance, the Redress Office could find that the TSC Call Center's percentage of incorrect identifications has increased significantly and recommend that a thorough review be conducted.

Disposition of Redress Complaints

The TSC tracks its processing and disposition of redress inquiries in a TSC database. At the time of our review, the database included only those disposition categories used by the TSC prior to the revision of the TSC's Redress SOP. The disposition for the 388 redress inquiries closed by the TSC between January 2005 and February 2007 is shown in Exhibit 4-3.

EXHIBIT 4-3
TSC Redress Complaint Disposition
(January 2005 through February 2007)

Disposition	Number of Complaints	Percentage of Complaints
Misidentification	52	13%
Positive Match (no change)	136	35%
Positive Match (remove record)	76	20%
Positive Match (modify record)	97	25%
Non-related	27	7%
Total	388	100%

Source: The Terrorist Screening Center Redress Office

Misidentified Complainants

TSC redress complaint disposition data show that 13 percent of the 388 closed redress inquiries were for complainants who were misidentified to a terrorist identity and were not an actual watchlist subject.

According to the TSC, the most common cause of a misidentification is name similarity. As previously discussed, the watchlist is identity-based and relies on name searches in order to vet persons against the watchlist. This can result in a person with an identical or similar name being identified as a terrorist watchlist identity. In many instances the screening agency can use additional identifying information, such as a date of birth or a passport number, to eliminate the individual as a terrorist watchlist match.⁶³

Positive Watchlist-Match Complainants

Of the 388 redress complaints reviewed by the TSC between January 2005 and February 2007, 80 percent involved complainants who were on the terrorist watchlist. Through its redress review process, the TSC determined that watchlist records for 35 percent of the closed positive

⁶³ Screening agencies have also developed programs to assist persons repeatedly misidentified to terrorist watchlist identities. For instance, an individual can voluntarily submit personal-identifying information to the TSA and request to be placed on the TSA Cleared List. If approved for placement on the Cleared List, the individual's name and personal-identifying information can be used to more quickly determine that the individual is not on the No Fly or Selectee lists. Similarly, the CBP and the State Department have implemented procedures to annotate records of misidentified persons in their databases to help avoid future port-of-entry screening and visa application delays. These actions are particularly helpful for a non-watchlist individual with an exact or a very similar name match to a known or suspected terrorist.

REDACTED FOR PUBLIC RELEASE

watchlist-match redress complaints required no change, 25 percent required some modification to the watchlist records, and 20 percent necessitated removing the complainant's identity from the watchlist.

Therefore, the TSC determined through its review that 45 percent of the watchlist records related to redress complaints were inaccurate, incomplete, not current, or incorrectly included.⁶⁴ TSC officials stated that, in some instances, at the same time that a nominating agency was going through the process of having an individual removed from the watchlist, that individual filed a redress complaint. In other instances, the TSC Redress Office found inaccuracies in the watchlist record or discovered additional, relevant information that had not been passed to the TSC.

Specifically, in 76 redress reviews, the TSC determined that the individual should not be watchlisted. In an additional 97 instances, the TSC found that the watchlist record was inaccurate or incomplete. The TSC's redress review results indicate that the watchlist includes individuals that should not be watchlisted and that other records contain deficiencies. These results are further evidence that watchlist data needs continuous monitoring and attention.

At the time of our review, the TSC did not track whether a change to the watchlist record was the result of a TSC redress review or whether the change was coincidental to a concurrent nominating agency submission of information to update the watchlist record. The TSC believes its expanded disposition categories will better account for these scenarios and provide a more accurate picture of redress resolution. The TSC Privacy Officer acknowledged that the high percentage of records requiring modification or removal may point to deficiencies in the terrorist watchlist nomination process and with nominating agencies not providing the TSC additional information important to appropriately update terrorist records.

Timeliness of Processing Redress Complaints

For each redress complaint it receives, the TSC develops a file folder and inputs information into a redress tracking database. The redress file contains information obtained, verified, and developed by the Redress Office. The file contains the Redress Office's review of relevant databases, correspondence with partner agencies, rationale for the resolution of the complaint, and management review.

⁶⁴ This 45 percent does not include the terrorist records that were modified or removed as part of a redress inquiry by a misidentified individual because the TSC did not specifically track those types of dispositions.

REDACTED FOR PUBLIC RELEASE

We judgmentally selected 20 redress inquiries the TSC received between January 2006 and February 2007 and reviewed the corresponding redress files to determine if the TSC followed its Redress SOP for resolving a redress complaint. We found the TSC complied with its Redress SOP in all 20 cases, including reviewing the applicable screening and intelligence databases, coordinating with partner agencies, and reaching appropriate resolutions.

We also reviewed TSC redress files and statistics to determine the efficiency of redress reviews. Our analysis of TSC data reveals that it took the TSC, on average, 67 days to close its review of a redress inquiry.⁶⁵ For redress matters referred to the TSC during the last semiannual period in our review (July through December 2006), it took the TSC an average of 57 days to finalize its review.

In addition to closed matters, we also analyzed the number of days that pending TSC redress matters had been open. The TSC had a total of 50 open redress inquiries as of February 27, 2007 and the average number of days these matters were open was 61. Of these inquiries, 38 percent were open over 60 days, including 2 inquiries that were pending over 180 days. Exhibit 4-4 details the number of days the 50 redress matters were open as of February 27, 2007.

EXHIBIT 4-4
Open TSC Redress Matters
(as of February 27, 2007)

Number of Days Open	Number of Open Redress Matters	Percentage of Total Open Redress Matters
180 days or more	2	4%
90-179 days	12	24%
60-89 days	5	10%
30-59 days	11	22%
less than 30 days	20	40%
Total	50	100%

Source: The Terrorist Screening Center Redress Office

Our analysis of closed and open redress matters indicates that it takes, on average, about 2 months for the TSC to finalize its review of a redress inquiry. TSC redress files included copies of e-mails and records of discussion between the TSC Redress Office and nominating agency personnel, as well as an accounting of other significant actions taken by TSC

⁶⁵ Redress matters pending as of February 27, 2007, were not included in our analysis of closed redress matters.

REDACTED FOR PUBLIC RELEASE

analysts to resolve the inquiry. TSC officials stated that each redress review is unique and that more complex cases require a longer review period.

Our review of TSC redress files revealed that long review periods were caused by a variety of factors. In some instances, the TSC took a significant amount of time to finalize its determination before coordinating with other agencies for additional information or comment. A TSC official involved in redress also stated that the Redress Office staffing level sometimes affected the TSC's ability to reach timely determinations. At times, the Redress Office used staff from other TSC units on a collateral, part-time basis. These persons would process redress matters when not performing their primary responsibilities and as time permitted. However, the TSC determined that this collateral assignment method did not provide the most efficient or effective means of resolving redress matters and, as a result, stopped this practice as of April 2007.

Other lengthy redress reviews were affected by nominating agencies not providing timely feedback to the TSC or not efficiently processing watchlist paperwork. The coordination TSC conducts with nominating agencies on redress matters includes corresponding with subject matter experts and case agents for clarification or updated information, requesting necessary watchlist processing documents (such as the FBI's terrorist watchlist nomination and modification form), and resolving differences of opinion between the TSC and nominating agency. For two redress matters, we found that the TSC repeatedly requested the FBI to file necessary paperwork in order to modify the watchlist records, and that it was finally able to close the matters over 140 days after its original requests. Further, we reviewed another redress file showing the FBI closed a preliminary investigation on an individual in November 2005. However, it did not notify the TSC that it determined the individual had no nexus to terrorism and should be removed from the watchlist. The TSC's redress review finally effected the overdue removal of this individual from the watchlist in January 2006.

Additionally, our file review found that certain screening agencies were slow to update their databases with accurate and current information. For instance, the State Department and the CBP did not revise encounter records in the IBIS database in a timely fashion to reflect modified or removed terrorist identities. For example, in one case the CBP did not make a TSC-requested change for more than 130 days.

TSC officials noted that no response timeframes have been established with partner agencies for redress matters. The Redress MOU states that one of the goals of the redress process is to provide for a *timely* review, but

explicit timeframes are not defined. We believe that timeliness measures should be established for resolving terrorist watchlist redress complaints and responding to complainants. The TSC Privacy Officer stated a next step in improving terrorist watchlist-related redress coordination among government agencies is to negotiate timeframes for redress processing. Given the TSC's responsibility for the content of the consolidated terrorist watchlist and its role in developing the Redress MOU, we recommend that the TSC attempt to coordinate timeliness measures for the entire watchlist redress process.

Response to Redress Complainants

The TSC does not respond to complainants filing redress inquiries. Instead, the TSC notifies the frontline screening agency of its disposition decision as it relates to the terrorist watchlist. The frontline screening agency involved in the watchlist-related encounter prompting the complaint is responsible for responding to the complainant. TSC policy dictates that responses to complainants neither confirm nor deny the existence of watchlist records relating to the complainant. This nondisclosure policy exists to protect U.S. counterterrorism operations and intelligence objectives and to safeguard the personnel involved in these sensitive activities. The TSC works with screening agencies such as the TSA in developing appropriate language for responding to complainants.

While the FBI is not the user of the NCIC database during a terrorist watchlist-related encounter involving a state or local law enforcement officer, it is the de facto screening agency in instances involving its NCIC database, and therefore responsible for responding to redress complaints concerning its database.⁶⁶ In May 2007, the FBI implemented a watchlist redress policy, identifying its Terrorist Review and Examination Unit (TRES) as responsible for processing the FBI's review of redress matters and for responding to complainants for NCIC-related complaints.⁶⁷ However, before it developed this policy, the FBI had not decided how it would respond to complainants, and we found that as of June 2007 it had not responded to a

⁶⁶ A typical NCIC-related encounter involves a state or local law enforcement officer conducting a routine traffic stop. The officer searches the subject's identification information (full name and date of birth) through the NCIC system to check for any outstanding warrants on the person. In the event the person is a possible terrorist watchlist identity match, the NCIC system will instruct the officer to contact the TSC to confirm the identity of the individual as an actual watchlist subject and to be instructed on the proper handling procedures for this individual.

⁶⁷ As stated earlier, only 4 percent of the redress referrals provided to the TSC from January 2005 through February 2007 were from non-DHS components such as the FBI.

REDACTED FOR PUBLIC RELEASE

redress complainant on a matter the TSC had closed on February 13, 2007, and had forwarded to the FBI for action.

Appeal of Redress Disposition

If a complainant is not satisfied with the disposition of an initial redress inquiry, the complainant may file an administrative appeal where available by the screening agency. The Redress MOU outlines the responsibilities for each agency in processing an administrative appeal of an original redress inquiry determination. Additionally, the TSC adopted a separate Redress Appeals SOP in November 2006 to expressly describe its administration of an appealed redress decision. The TSA is the only frontline screening agency that has developed its own process for redress appeals.

The TSC Redress Appeals SOP stipulates that a complete analysis of the appeal be performed by the TSC Legal Department, a unit separate from the Redress Office. The TSC prohibits the TSC Redress Office and any personnel involved in the original redress review from direct involvement in the redress appeal process. According to the SOP, the TSC will alert NCTC and the nominating agency that an appeal has been submitted, and it will facilitate necessary communication between the nominating and screening agencies. The final recommendation or decision is determined by the TSC Redress Appeals Board, comprised of TSC Deputy Directors. For an appeal involving a No Fly watchlist status, the TSC recommends a disposition and the TSA has the final decision authority.

As of May 1, 2007, the TSC had received four redress appeals. It resolved two appeals, and these resulted in downgrading the watchlist status of the individuals. The remaining two appeals had been pending resolution for 83 and 167 days, according to the TSC. The TSC stated that staffing constraints hindered its ability to more quickly resolve these redress appeals. The TSC informed us that in April 2007 it was able to assign redress appeal duties to a permanent staff position and the TSC believes that this action will improve the TSC's timeliness in resolving redress appeals.

Proactive Redress

It is possible for the TSC and other watchlist agencies to use available information to provide unsolicited relief to non-watchlist persons identified by the terrorist watchlist process. Besides its standard redress reviews, the TSC Redress Office also conducted ancillary evaluations of persons reported to have been identified by terrorist watchlist screening who had not filed a formal complaint. Additionally, the U.S. government, including the TSC and screening agencies, has information on persons misidentified as a terrorist

REDACTED FOR PUBLIC RELEASE

watchlist subject in the various screening databases. However, the U.S. government, including the TSC, is not currently coordinating the use of this data in attempts to proactively reduce the incidence and impact of misidentifying persons as watchlist subjects.

TSC Informal Redress Reviews

Typically, the TSC undertakes a redress review only when an individual submits a formal redress request. Occasionally, however, the TSC Redress Office reviews records outside this formal process. The TSC may be asked by a government official to look into a matter or it may acquire from a news media publication the name of a person possibly stopped due to the terrorist watchlist. For instance, a newspaper may publish an article explaining that a foreigner was not allowed to board a flight destined for the United States and the TSC Redress Office believes that the TSC should research the events. In such a case, the TSC Redress Office performs an evaluation similar to its formal redress review for such matters. First, it determines if the person was the subject of a terrorist watchlist-related encounter. If so, it reviews the related watchlist record for accuracy and completeness, making changes and updates as necessary.

The TSC Redress Office maintains a log that records the intake and resolution of these proactive reviews. Our review of this log shows that since this initiative began in December 2005, the TSC had resolved 76 cases through March 1, 2007, tracking them according to its redress disposition categories. Exhibit 4-5 shows that over 80 percent of these reviews involved an individual who experienced a watchlist-related encounter (misidentification and positive-match categories). Of the 32 positive matches, terrorist records were modified or removed from the watchlist for 16 of the reviews.

EXHIBIT 4-5
TSC Informal Redress Reviews
(December 2005 through March 1, 2007)

Disposition Category	Number	Percent
Misidentification	32	42%
Positive Match	32	42%
Non-related	10	13%
Further Investigation ⁶⁸	2	3%
Total	76	100%

Source: The Terrorist Screening Center Redress Office

⁶⁸ Two of the TSC Redress Office's informal reviews required further investigation in order to determine the relationship of the individual to a watchlist identity.

Use of Watchlist Encounter Information for Misidentified Individuals

The TSC has a record of all potential terrorist watchlist encounters referred to its call center, including information on positive, negative, and inconclusive encounters.⁶⁹ Therefore, the TSC has knowledge of the watchlist records involved in the negative encounters referred to its call center, as well as information on the individual that was misidentified as a potential terrorist for a period of time.

The TSC does not have any policy or procedures to proactively use information from negative encounters to reduce the incidence and impact of terrorist watchlist misidentifications. Moreover, the TSC's strategic plan does not include goals or actions associated with reducing the incidence of misidentifications or the impact on misidentified persons, other than that covered by the formal redress process. Considering that 43 percent of all encounters referred to the TSC Call Center are negative for a watchlist match, we believe the TSC should develop strategic goals and policy specific to mitigating the adverse impact of the terrorist screening process on non-watchlist subjects, particularly for individuals who are repeatedly misidentified as potential watchlist subjects.

Additionally, we believe the TSC should consider developing the ability within its encounter tracking system or consolidated watchlist database to alert the TSC to take proactive action on watchlist records that have been the subject of a certain number of encounters. For example, the system could be programmed to automatically generate a quality assurance lead for the TSC to perform a comprehensive review of the terrorist record. Such a function would help certify that a watchlist record frequently the subject of encounters, whether the encounters are positive, negative, or inconclusive, is accurate, complete, and current. This is important for both appropriately handling suspected or known terrorists and for reducing the adverse effects on persons misidentified as watchlist subjects.

Conclusion

Screening agencies across the federal government are in the process of instituting an interagency agreement that will formalize the U.S. government's review of redress inquiries from individuals who complain they were adversely affected during watchlist screening. Additionally, the

⁶⁹ Not all potential watchlist matches are referred to the TSC. If possible, screening agencies resolve negative encounters without contacting the TSC by comparing information on the encountered individual to the potential terrorist watchlist identity match. Screening agencies contact the TSC Call Center on all encounters where it cannot definitively make this determination.

TSC has developed its own SOP for processing redress complaints. We found that the TSC generally followed these procedures, the procedures are comprehensive, and TSC staff resolved redress matters logically and accurately.

However, our examination of TSC redress files also revealed that the TSC's comprehensive redress reviews often resulted in watchlist record changes and removals. We believe that the high percentage of redress reviews resulting in changes to or removals of watchlist records provides further evidence that watchlist data needs continuous monitoring and attention.

Our review also revealed that watchlist agencies, including the TSC and nominating and screening agencies, sometimes caused unnecessary delays in closing redress inquiry reviews. We recommend that the TSC coordinate efforts for the watchlist agencies to develop timeliness measures for each stage in the redress process.

Recommendations

We recommend that the TSC:

15. Organize a working group comprised of representatives from agencies involved in the terrorist watchlist redress process to develop timeliness measures for each phase in the redress process.
16. Develop goals and measures for its strategic plan to reduce the incidence and impact of misidentifications.
17. Develop procedures to proactively review terrorist watchlist identities that are frequently the subject of watchlist encounters, no matter if the encounter was positive, negative, or inconclusive.

We recommend that the FBI:

18. Develop and implement timeliness measures to ensure that the FBI responds in a timely manner to redress inquiries from complainants subject to terrorist watchlist-related encounters involving the NCIC database, including the complainant identified by the OIG whose complaint has been pending since February 2007.

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit of the TSC, we considered its control structure for the purpose of determining our audit procedures. This evaluation was not made for the purpose of providing assurance on the TSC management control structure as a whole. However, we noted certain matters involving management controls that we considered to be reportable conditions under the *Government Auditing Standards*.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operations of the management control structure that, in our judgment, could adversely affect the TSC's ability to maintain and disseminate accurate and complete information on known or suspected terrorists used during watchlist screening. We identified weaknesses in the TSC's internal control structure that resulted in inaccurate and incomplete watchlist records and terrorist identities not being correctly exported to downstream watchlist databases. These issues are discussed in Findings I, II, and III of the report.

Because we are not expressing an opinion on the TSC's management control structure as a whole, this statement is intended solely for the information and use of the TSC management. This restriction is not intended to limit the distribution of the report.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

In connection with this audit of the TSC, as required by generally accepted government auditing standards, we reviewed management processes and records to obtain reasonable assurance about the organization's compliance with laws and regulations that, if not complied with, in our judgment, could have a material effect on TSC operations. Compliance with laws and regulations applicable to the management of the TSC is the responsibility of the TSC's management.

Our audit included examining, on a test basis, evidence about laws and regulations related to the maintenance and sharing of information on suspected or known terrorists. The specific laws and regulations we reviewed included the relevant portions of:

- Intelligence Authorization Act, Public Law 108-177;
- Homeland Security Presidential Directive 6; and
- Homeland Security Presidential Directive 11.

Our tests of the consolidated terrorist watchlist identified weaknesses related to the accuracy and completeness of the data which is discussed fully in Findings I, II, and III. The requirements for an accurate and complete watchlist are contained in HSPD 6.

With respect to areas that were not tested, nothing came to our attention that caused us to believe that the TSC management was not in compliance with the laws and regulations cited above.

APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY**Audit Objectives**

The objectives of the audit were to: (1) determine whether accurate and complete records are disseminated to and from the Terrorist Screening Center's (TSC) watchlist database in a timely fashion; (2) review the TSC's efforts to ensure the quality of the information in the watchlist database; and (3) assess the TSC's efforts to address complaints raised by individuals who believe they have been incorrectly identified as watchlist subjects.

Scope and Methodology

We performed our audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States, and accordingly, included such tests of the records and procedures that we considered necessary. Our audit covered but was not limited to the period of June 2005 through April 2007.

To accomplish our objectives, we conducted work primarily at the TSC, located in the Washington, D.C., metropolitan area. Additionally, we interviewed personnel at other federal agencies and offices whose work relates to TSC operations, such as NCTC, the FBI, DHS, and the White House Privacy and Civil Liberties Oversight Board.

To obtain an overall understanding of the TSC's role and responsibilities, we reviewed legislative materials related to the TSC's creation and watchlisting requirements, prior audit reports, and various other documents as needed, including financial documents, strategic plans, and staffing reports.

Accuracy and Completeness of Database Records

To obtain an understanding of the TSC's processes and procedures for ensuring the quality of data ingested into and exported from the Terrorist Screening Database (TSDB), we reviewed the TSC's procedures for processing database nominations and encounters. In addition, we interviewed:

- Contractors and representatives from the various participating Departments working within the TSC's Administration Branch, Operations Branch, Information Technology Branch, Call Center, Nominations and Data Integrity Unit, and other support areas.

- Program managers at NCTC.
- Supervisors from the FBI's Terrorist Threat Center, Terrorist Review and Examination Unit, and Terrorist Screening Operations Unit.
- The Executive Assistant Director of the FBI's National Security Branch and the Assistant Director and Deputy Assistant Director of its Counterterrorism Division.

Testing of Watchlist Database Records

As of March 16, 2007, there were 689,613 records in the web-based version of the TSDB. We performed various tests of a limited number of these records, and reviewed related records from the pertinent automated data systems used to store terrorist-related information maintained by the NCTC and FBI, to determine whether the records were accurate and complete, and any record changes were made in a timely fashion. The automated data systems were the TSDB, TSC's Encounter Management Application (EMA), NCTC's Terrorist Identities Datamart Environment (TIDE), and the FBI's Violent Gang and Terrorist Organization File (VGTOF).

In addition to querying the TSDB to identify duplicate records and determining whether records related to 20 FBI requests for removal had been deleted from the TSDB in a timely manner, our tests of judgmentally selected records included:

- Review of 50 TSDB records related to 25 FBI international terrorist and 25 FBI domestic terrorist nominations to determine whether basic identifying information [SENSITIVE INFORMATION REDACTED] listed on the FD-930 (the form used by the FBI for watchlisting nominations) were accurately entered into the databases. In addition, we analyzed key dates shown on the FD-930s to determine whether the names and other information were entered into the TSDB in a timely fashion.
- Review of a sample of 49 known terrorist names to determine whether the basic identifying information as well as citizenship and physical characteristics were accurately entered into the databases. Of these names, 10 were non-FBI originated international terrorist identities in the TIDE database, 17 were selected from the FBI's Most Wanted Terrorists list, 2 were selected from the Rewards For Justice website, 16 came from the State Department's Office of

Counter Terrorism, and 4 were obtained from various newspaper articles.

- Review of 51 TSDB records for which TSC staff had identified as having quality assurance issues, such as missing, outdated, or inaccurate information.⁷⁰ This review included identifying the quality assurance issue that was raised, determining whether the appropriate changes had been made to the TSDB, TIDE, and VGTOF records. In addition, we evaluated the timeliness of the revision and any additional follow-up performed by TSC staff to ensure that the necessary changes were made. Finally, we reviewed these records to determine whether the basic identifying information was accurately entered into the databases.
- Review of 20 TSDB records related to positive encounters with watchlist subjects, as recorded in EMA, to determine whether the basic identifying information was accurately entered into the databases and information obtained by law enforcement agencies as a result of the encounters was added to appropriate database records.
- Review of 15 TSDB records that TSC staff identified as having undergone a thorough quality assurance review as part of a special project to evaluate the adequacy of the TSC's review and to determine whether the basic identifying information was accurately entered into the databases.

Finally, we compared information in the TSDB records to watchlisting criteria to determine whether the individuals were nominated for the appropriate watchlists and were assigned an appropriate handling instruction.⁷¹

Watchlist Redress

To obtain an understanding of the TSC's role in the terrorist watchlist redress process and its efforts to reduce watchlist misidentifications, we reviewed the TSC's redress procedures and the U.S. government's

⁷⁰ 25 of the 51 records were selected from the TSC's Quality Assurance Tracker, the TSC's original system for monitoring TSDB records with quality assurance issues. The remaining 26 records were selected from quality assurance tickets, the TSC's current monitoring system.

⁷¹ The criteria used by the agencies hosting TSDB records are identified in Appendix II.

interagency agreement on terrorist watchlist redress. We judgmentally selected and examined 20 redress complaints reviewed by the TSC Redress Office to evaluate whether the TSC followed its Redress SOP for resolving a redress complaint.

We also conducted interviews with the TSC's Privacy and Redress Officers, and we reviewed the TSC's strategic plan to identify any goals related to redress or reducing the incidence and effect of watchlist misidentification. Additionally, to obtain an understanding of the partner agencies' roles in the redress process and how they coordinate with the TSC, we interviewed representatives from the White House Privacy and Civil Liberties Oversight Board, the DHS's Screening Coordination Office, TSA, and CBP.

From January 2005 through February 2007, 438 redress complaints were referred to the TSC. During this same period, the TSC closed 388 complaints. We performed various analyses of TSC's redress referral data, including calculating:

- the percent of cases referred to the TSC according to referring agency;
- the average amount of time cases were open, and evaluating the reasons affecting delays in closing the matters; and
- the TSC's disposition for its closed redress matters.

APPENDIX II: SYSTEMS USED IN THE TERRORIST WATCHLIST PROCESS

The Terrorist Screening Database (TSDB) is the U.S. Government's consolidated terrorist watchlist. The TSDB contains basic biographical information on known or appropriately suspected domestic and international terrorists. In this regard, the underlying derogatory information on individuals nominated for inclusion in the TSDB must demonstrate a reasonable suspicion of ties to terrorism.

Currently, TSDB records are exported to various U.S. and international government entities tasked with conducting terrorism screening. Each agency receiving TSDB records has established criteria that dictate what records it receives from the TSC. The TSC provided us with the following descriptions of the databases receiving watchlist records and the minimum criteria for exporting records to them:

CLASS

The Consular Lookout and Support System (CLASS) is maintained by the Department of State (State Department). CLASS, divided into CLASS/Visa and CLASS/Passport, is used by State Department representatives when processing visa and passport applications, respectively.

[SENSITIVE INFORMATION REDACTED]

IBIS

The Interagency Border Inspection System (IBIS) is maintained by DHS's U.S. Customs and Border Protection agency. IBIS is generally queried by federal law enforcement agents at ports of entry.

[SENSITIVE INFORMATION REDACTED]

No Fly and Selectee Lists

The No Fly and Selectee Lists are maintained by the Transportation Security Administration. These lists are used by public carriers, both airline and other modal, to screen their passengers. The No Fly list includes individuals who are prohibited from boarding an aircraft. The Selectee list includes individuals who must undergo additional security screening checks before being permitted to board an aircraft.

[SENSITIVE INFORMATION REDACTED]

- In addition, a minimum threshold of derogatory information for inclusion on the No Fly or Selectee lists was established on October 21, 2004, by the Homeland Security Council.

[SENSITIVE INFORMATION REDACTED]

VGTOF

Terrorist records contained in the Violent Gang and Terrorist Organization File (VGTOF) is one segment of the FBI's National Crime Information Center (NCIC) system. The NCIC is a database queried by federal, tribal, state, and local law enforcement agencies in performance of their duties.

Minimum Criteria:

In order for a known or suspected terrorist to be included in VGTOF, the following minimum biographical information is required:

- first name
- last name
- approximate year of birth

APPENDIX III: DIAGRAM OF TERRORIST WATCHLIST DATAFLOW

[SENSITIVE INFORMATION REDACTED]

APPENDIX IV: ACRONYMS

CBP	Customs and Border Protection
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CLASS	Consular Lookout and Support System
DHS	Department of Homeland Security
DOJ	Department of Justice
EMA	Encounter Management Application
FBI	Federal Bureau of Investigation
FY	Fiscal Year
HSPD-6	Homeland Security Presidential Directive-6
IBIS	Interagency Border Inspection System
ICE	Immigration and Customs Enforcement
IT	Information Technology
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NDIU	Nominations and Data Integrity Unit
NTP	Nomination Tracking Processor
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
TIDE	Terrorist Identities Datamart Environment
TREX	Terrorist Review and Examination Unit
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TSOU	Terrorist Screening Operations Unit
SOP	Standard Operating Procedure
VGTOF	Violent Gang and Terrorist Organization File

APPENDIX V: TERRORIST SCREENING CENTER RESPONSE



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 28, 2007

The Honorable Glenn A. Fine
Office of the Inspector General
United States Department of Justice
Room 4322
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Dear Mr. Fine:

This letter is submitted by the Federal Bureau of Investigation (FBI) in response to the audit report by the Office of Inspector General (OIG) entitled: Follow-up Audit of the Terrorist Screening Center (hereinafter the Report).

The FBI appreciates the opportunity to comment and agrees fully with the OIG that the mission and function of the Terrorism Screening Center (TSC) is a critical part of the layered national strategy to safeguard the Homeland from a future terrorist attack.

The FBI remains committed to ensuring the timely and accurate collection of watchlisting data for distribution to those government agencies responsible for screening, law enforcement and intelligence work. One of the TSC's highest priorities is to ensure the Terrorist Screening Database (TSDB) is accurate, current and thorough. When the consolidated watchlist was originally created, agencies and Departments provided all possible data from their holdings to serve as the foundation for terrorist watchlist information. Much of the original data provided to the TSC lacked a validation or review process by the originating agency, which presented initial challenges in quality of the TSDB. Since that time the quality of the TSDB data has vastly improved. For example, as of July 2007, TSC has completed a full vetting of the Department of Homeland Security's No-Fly list, resulting in an approximate 50% reduction of records.

The field work of the OIG has confirmed that the TSC has enhanced its efforts to ensure the quality of watchlist data, we have increased the level of staff assigned to data quality management and we have developed a process, complete with a separate office to respond to redress complaints filed by persons seeking relief from adverse effects related to terrorist watchlist screening.

I believe the TSC has improved the security of the Homeland by leading the effort to consolidate the terrorist watchlisting process and serving as the accountable entity pursuing watchlisting as its single core competency. The TSC's efforts combined with the U.S. Government's (USG) community effort to significantly increased information sharing at all levels of state, local and federal government, has lead to enhanced security. The TSC is fully committed to constantly examining its operations for enhancements in efficiency and effectiveness. The TSC has made significant progress in its mandate to consolidate the USG's approach to terrorism screening and its leadership makes every effort to ensure the most thorough, current and accurate information is provided to law enforcement and intelligence community partners for a safer and more secure nation. In that spirit, the FBI and the TSC offers the following responses to the specific recommendations made in the Draft Audit Report, *Follow-Up Audit of the Terrorist Screening Center*.

Recommendation # 1:

Implement its plan to consolidate the TSDB NTP and legacy systems in a timely manner. In the interim while the two systems coexist, the TSC should establish a formal procedure to regularly review the TSDB NTP and legacy systems to ensure that the information in these systems remains synchronized.

Response: The TSC has developed a project plan that guides the prioritization of tasks to achieve the objective of consolidating NTP component with the official record keeping component of the TSDB. The TSC has implemented a daily reconciliation process between the two components in the interim period for routine monitoring of the data.

Recommendation # 2:

Develop procedures to regularly review and test the information contained in the TSDB to ensure the data is complete, accurate, and non-duplicative.

Response: The TSC accepts this recommendation and notes that it has used informal procedures to review and test TSDB information in the past, but has now implemented procedures to formalize this process.

Recommendation # 3:

Modify the TSDB NTP to accommodate designations for both CLASS/Visa and CLASS/Passport. In addition, the TSC should review and correct the records identified in the TSDB NTP to appropriately reflect that U.S. persons are not eligible for export to CLASS/Visa.

TSC Response: The TSC agrees with this recommendation and will implement these changes as part of the transfer of exports to TSDB NTP.

Recommendation # 4:

Review and correct the records identified in the TSDB NTP to ensure that the IBIS handling instructions are appropriately applied.

Response: The TSC agrees with this recommendation and has corrected the records.

Recommendation # 5:

Develop procedures to regularly review the information in the TSDB to ensure that outdated or obsolete data is removed in a timely manner.

Response: The TSC accepts this recommendation and notes it has used previously undocumented procedures to remove outdated or obsolete data, and will now formalize this process to ensure it is removed in a timely manner.

Recommendation # 6:

Working with the TSC, revise the watchlist nomination process to provide international terrorist nominations directly to NCTC for inclusion in TIDE, submission to the TSC, and dissemination to all downstream databases, including VGTOF.

Response: The FBI and TSC watchlist nomination process was initially created to address a concern that watchlist nominations were not being processed in an expedient manner. Both the FBI and TSC conduct 24/7 operations that include near real-time submissions to the watchlisting process on weekend days and after normal business hours. The NCTC personnel assigned to the watchlisting process now work a 16 hour shift Monday through Friday. With the objective in-mind to ensure that all watchlisting nominations are processed timely. The FBI will continue to work to revise the current process recognizing watchlisting must take place when NCTC is not available.

Recommendation # 7:

Correct the records identified by the OIG containing incorrect watchlist designations, handling code errors, and inaccurate and inconsistent information.

Response: The TSC agrees this recommendation and has taken steps to correct the records under its purview.

Recommendation # 8:

Coordinate with NCTC and the FBI to implement an agreement that establishes the areas of responsibility and the timeframes for data quality assurance matters.

Response: The TSC accepts the recommendation to implement an agreement with both NCTC and the FBI's National Threat Center Section to establish areas of responsibility and timeframes for data quality assurance matters.

Recommendation # 9:

Develop a comprehensive standard operating procedure that describes the TSC's three-pronged quality assurance strategy and details the methodology to be used in performing quality assurance reviews.

Response: The TSC accepts this recommendation to document a comprehensive SOP which describes its quality assurance strategy and methodology.

Recommendation # 10:

Develop a process to perform regular spot-checks of NDIU analysts' work to identify any weaknesses and need for additional training.

Response: The TSC accepts this recommendation to document and perform a standardized methodology for NDIU spot-checks that will identify areas for targeted training, replacing its previously used undocumented process.

Recommendation # 11:

Develop an improved and user-friendly process for tracking classified correspondence related to quality assurance matters.

Response: The TSC agrees with this recommendation and has already implemented a solution. TSC will utilize the FBI's Automated Case Support (ACS) system to track all quality assurance classified correspondence. All classified correspondence, to include e-mails and electronic communications (EC), will be uploaded to a control file within ACS which will house such communications.

Recommendation # 12:

Develop a tickler system or electronic dashboard for all pending quality assurance matters.

Response: The TSC accepts this recommendation and has begun efforts to develop same.

Recommendation # 13:

Develop a comprehensive plan, including benchmarks or milestones, to complete the record-by-record review of the TSDB.

Response: TSC will develop a comprehensive plan that will ensure each record in the TSDB has undergone a quality assurance review in addition to those high priority projects currently underway.

Recommendation # 14:

Coordinate with other partner agencies to establish a formal process for relevant encounter information to be captured by frontline screening agents and returned to the TSC to update watchlist records.

Response: The TSC accepts this recommendation to establish a formal process to update watchlist records with encounter information and notes it has used an undocumented process to accomplish this recommendation since its inception.

Recommendation # 15:

Organize a working group comprised of representatives from agencies involved in the terrorist watchlist redress process to develop timeliness measures for each phase in the redress process.

Response: TSC accepts this recommendation; the implementation of which is underway and pending signatures by all parties.

Recommendation # 16:

Develop goals and measures for its strategic plan to reduce the incidence and impact of misidentifications.

Response: TSC accepts this recommendation and is developing appropriate goals and performance measures as part of the strategic plan.

Recommendation # 17:

Develop procedures to proactively review terrorist watchlist identities that are frequently the subject of watchlist encounters, no matter if the encounter was positive, negative, or inconclusive.

Response: TSC accepts this recommendation. TSC is currently developing the framework for a new program that will proactively review watchlist records related to frequently encountered individuals.

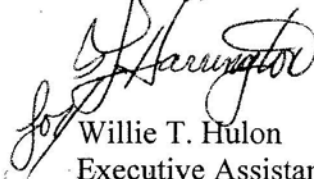
Recommendation # 18:

Develop and implement timeliness measures to ensure that the FBI responds in a timely manner to redress inquiries from complainants subject to terrorist watchlist-related encounters involving the NCIC database, including the complainant identified by the OIG whose complaint has been pending since February 2007.

Response: The FBI accepts this recommendation and has instituted new policy and process. The February 2007 complainant involves a unique and very sensitive matter which has been resolved.

The FBI, the TSC and our strategic partners will continue to pursue efforts to improve the terrorist watchlisting process.

Sincerely,



Willie T. Hulon
Executive Assistant Director
National Security Branch

**APPENDIX VI: OFFICE OF THE INSPECTOR GENERAL
ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO
CLOSE THE REPORT**

In its response to our draft audit report, the TSC concurred with each of our 18 recommendations and discussed the actions it has already taken and others it will implement in response to our findings. This appendix contains our analysis of the TSC's responses to our recommendations and the actions necessary to close each recommendation.

Status of Recommendations

1. **Resolved.** The TSC concurred with our recommendation that it implement its plan to consolidate the TSDB NTP and legacy databases in a timely manner, and the TSC stated that it developed a project plan to guide the future consolidation of the system. In the interim period while it is still necessary to operate both databases, the TSC stated that it implemented a daily reconciliation process between the TSDB NTP and legacy databases for routine monitoring of the data.

This recommendation can be closed when we receive evidence that the TSC has fully implemented its plan to consolidate the TSDB NTP and legacy databases. In the meantime, please provide evidence that the TSC has implemented a daily reconciliation process that identifies and addresses differences in database content.

2. **Resolved.** In its response to our draft report, the TSC concurred with our recommendation to develop procedures to regularly review and test the information contained in the TSDB to ensure the data is complete, accurate, and non-duplicative. The TSC noted that it has used informal procedures to review and test the information in the TSDB, and it now has implemented procedures to formalize this process.

This recommendation can be closed when we receive documentation or other evidence to support that the TSC has developed and fully implemented procedures to regularly review and test information in the TSDB to ensure the data is complete, accurate, and non-duplicative.

3. **Resolved.** The TSC concurred with our recommendation and stated that it will implement our recommended changes as part of its planned, phased improvements for the TSDB NTP, including the incorporation of the export capability of the legacy system.

This recommendation can be closed when we receive evidence that the TSC has modified the TSDB NTP to accommodate designations for both CLASS/Visa and CLASS/Passport, and that it has reviewed and corrected the records identified in the TSDB NTP to appropriately reflect that U.S. persons are not eligible for export to CLASS/Visa.

4. **Resolved.** The TSC concurred with this recommendation and stated that it had completed its review of watchlist records and made corrections to records in the TSDB NTP with incorrect IBIS handling instructions.

This recommendation can be closed when we receive evidence that the TSC identified and corrected the watchlist records with inappropriate IBIS handling instructions.

5. **Resolved.** In its response to our draft report the TSC concurred with this recommendation and stated that while it had used previously undocumented procedures, it will now formalize this process to ensure that outdated or obsolete data is removed in a timely manner.

This recommendation can be closed when we receive evidence that the TSC has developed and implemented formal procedures to regularly review the information in the TSDB to ensure that outdated or obsolete data is removed in a timely manner.

6. **Resolved.** The FBI concurred with our recommendation and stated that it will continue to work to revise the current nomination process. However, the FBI stated that it had implemented its current nomination process initially to address its concern that watchlist nominations were not being processed in a timely manner due to the operations schedule of the NCTC.

While we recognize that the FBI conducts its watchlisting operations on a continuous basis, we believe that the NCTC is operational during the time period in which the majority of watchlist nominations are submitted. Further, an additional emergency nomination process is available to the FBI for those instances in which the FBI determines a nomination is exigent and the NCTC may not be available. Given our identification of significant data errors and inconsistencies resulting from the FBI's non-standard nomination process for international terrorists, we believe that the FBI, NCTC, and TSC should work together to design a more consistent and reliable process by which FBI-originated international terrorist information is provided to the

NCTC for inclusion in TIDE and disseminated to the TSDB and downstream screening systems, including VGTOF. To close this recommendation, please provide us with information on specific steps taken to revise the FBI's watchlist nomination process for known or suspected international terrorists.

7. **Resolved.** The TSC concurred with this recommendation and stated that it has taken steps to correct the watchlist records under its purview. This recommendation can be closed when we receive evidence that the records we identified during our review that contained incorrect watchlist designations, handling code errors, and inaccurate and inconsistent information have been corrected.
8. **Resolved.** The TSC concurred with our recommendation to coordinate with NCTC and FBI to implement an agreement that establishes the areas of responsibility and the timeframes for data quality assurance matters.

This recommendation can be closed when we receive evidence supporting the implementation of a signed agreement between the NCTC and FBI that outlines areas of responsibility and the timeframes for data quality assurance matters.

9. **Resolved.** The TSC concurred with our recommendation to develop a comprehensive standard operating procedure that describes the TSC's quality assurance strategy and details the methodology to be used in performing quality assurance reviews.

This recommendation can be closed when we receive evidence that the TSC has finalized its quality assurance strategy and methodology and has trained its staff on using the standard operating procedure in performing quality assurance reviews.

10. **Resolved.** The TSC concurred with our recommendation to develop a process to perform regular spot-checks of NDIU analysts' work. This recommendation can be closed when we receive evidence that the TSC has developed, documented, and implemented a process to perform regular spot-checks of NDIU analysts' work to identify weaknesses and needs for additional training.
11. **Resolved.** In its response, the TSC concurred with this recommendation and stated that it had implemented a solution to remedy our finding. Specifically, the TSC stated that it will utilize the FBI's Automated Case Support (ACS) system to track all quality

assurance classified correspondence, including e-mails and electronic communications.

This recommendation can be closed when we receive evidence that the TSC has formally documented this process and communicated the policy to its staff.

12. **Resolved.** The TSC concurred with this recommendation and stated that it has begun developing a tickler system or electronic dashboard for pending quality assurance matters. This recommendation can be closed when we receive evidence that the TSC has implemented such a system.
13. **Resolved.** The TSC concurred with this recommendation and stated that it will develop a comprehensive plan to ensure that each record in the TSDB has undergone a quality assurance review.

This recommendation can be closed when we receive evidence that the TSC has developed a plan that: (1) includes specific milestones for the successful completion of this comprehensive review, (2) tracks its progress against these milestones, and (3) identifies actions to take if the milestones are not met.

14. **Resolved.** The TSC concurred with this recommendation and stated that since its inception the TSC has used an undocumented process to coordinate with other partner agencies to obtain relevant information captured by frontline screening agents during encounters with known or suspected terrorists. We recognize that the TSC has endeavored to update watchlist records by incorporating encounter information captured by frontline screening agents. However, without a formal process with which frontline screening agencies agree, the TSC is unable to ensure that it is receiving complete, accurate, and timely encounter information. This recommendation can be closed when the TSC provides documentation to support that a formal process has been developed and implemented between partner agencies to ensure that encounter data is appropriately returned to the TSC for updating watchlist records.
15. **Resolved.** The TSC concurred with this recommendation and stated that implementation to address this recommendation was underway and pending signatures by all parties. This recommendation can be closed when we receive the finalized agreement containing timeliness measures for processing watchlist redress matters agreed to and signed by the appropriate agencies.

16. **Resolved.** The TSC concurred with this recommendation and stated it is developing goals and performance measures relative to misidentifications for its strategic plan. This recommendation can be closed when the TSC provides its updated strategic plan that includes goals and performance measures to address reducing the incidence and impact of misidentifications.

17. **Resolved.** The TSC concurred with this recommendation, stating in its response that it is developing the framework for a program that will proactively review watchlist records related to frequently encountered individuals. This recommendation can be closed when the TSC provides documentation formalizing this new proactive redress program, as well as evidence that this program has been implemented.

18. **Resolved.** The FBI concurred with our recommendation and stated that it has instituted a new policy and process for resolving redress matters involving the NCIC database. Additionally, the FBI noted that the February 2007 redress matter that was pending at the time of our review has been resolved.

To close this recommendation, please provide us the FBI policy containing timeliness measures for processing NCIC-related redress matters. Additionally, please provide documentation to confirm that the February 2007 redress matter that was pending at the time of our review has been appropriately resolved.