Review of the Terrorist Screening Center

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

Audit Report 05-27
June 2005

REDACTED FOR PUBLIC RELEASE

REVIEW OF THE TERRORIST SCREENING CENTER*

EXECUTIVE SUMMARY

On September 16, 2003, the President signed Homeland Security Presidential Directive-6 (HSPD-6), requiring the establishment of an organization to "consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes." Specifically, the Attorney General was directed to create a new organization to consolidate terrorist watch lists and provide 24-hour, 7-day a week operational support for federal, state, local, territorial, tribal, and foreign government as well as private sector screening across the country and around the world.[1] As a result of this presidential directive, the Terrorist Screening Center (TSC) was created. As of the end of fiscal year (FY) 2004, the TSC was a $27 million organization with approximately 175 staff.

The Office of the Inspector General (OIG) initiated this audit to examine whether the TSC: 1) has implemented a viable strategy for accomplishing its mission; 2) is effectively coordinating with participating agencies; and 3) is appropriately managing terrorist-related information to ensure that a complete, accurate, and current consolidated watch list is developed and maintained.[2]

Identifying the Need for a Screening Agency

Prior to the establishment of the TSC, the federal government relied on information from numerous separate watch lists maintained at a variety of federal agencies to prevent terrorists from obtaining visas or entering the United States illegally, and to track suspected terrorists within U.S. borders.

*** The full version of this audit report includes a limited amount of information that the Federal Bureau of Investigation (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] "Screening" refers to a process that may include, but is not limited to, government officials searching for available information on an individual in various databases. For example, a person may go through a screening process when: 1) applying for a visa, 2) attempting to enter the United States through a port of entry, 3) being stopped by a local law enforcement officer for a traffic violation, or 4) attempting to travel internationally on a commercial airline.

[2] Appendix I contains detailed information on the audit's objectives, scope, and methodology.

In 2002, the President and Congress recognized this fragmentation and called for the consolidation of terrorist information to unify the government's counterterrorism efforts.

In July 2002, the President issued the National Strategy for Homeland Security, which created a "comprehensive plan for using America's talents and resources to enhance our protection and reduce our vulnerability to terrorist attacks."[3] One aspect of the President's strategy was for the FBI to create a consolidated terrorism watch list that would serve as a central point for information about individuals of investigative interest. This list was seen as an answer to the uncoordinated and ad hoc approach that the U.S. government was then pursuing.

In addition, the 9/11 Congressional Joint Inquiry Committee reported in December 2002 that the U.S. government was not adequately collecting and integrating terrorism-related information from all domestic and foreign sources. As a result, the Joint Inquiry also recommended the creation of a national watch list center to facilitate the appropriate collection, declassification, and sharing of information on known or suspected terrorists.

In April 2003, the Government Accountability Office (GAO) issued a report identifying 12 separate watch lists used for various purposes.[4] The following table lists the systems identified by the GAO.

[3] Office of Homeland Security, National Strategy for Homeland Security (July 2002).

[4] *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, Government Accountability Office (GAO-03-322, April 2003).

TERRORIST-RELATED WATCH LISTS IDENTIFIED BY THE GOVERNMENT ACCOUNTABILITY OFFICE IN APRIL 2003[5]		
	Description	**Agency**
1	TIPOFF System	Department of State (DOS)
2	Violent Gang and Terrorist Organizations File (VGTOF)	FBI
3	Interagency Border Inspection System (IBIS)	Department of Homeland Security (DHS)
4	National Automated Immigration Lookout System (NAILS)	DHS
5	Consular Lookout and Support System (CLASS)	DOS
6	No-Fly List	DHS
7	Selectee List	DHS
8	Integrated Automated Fingerprint Identification System (IAFIS)	FBI
9	Automated Biometrics Identification System (IDENT)	DHS
10	Warrant Information Network	U.S. Marshals Service
11	Top Ten Fugitives	Department of Defense, U.S. Air Force
12	Interpol Terrorism Watch List	Department of Justice (DOJ)
Source: GAO Report Number GAO-03-322		

Establishing the TSC

In a September 2003 news release announcing the signing of HSPD-6 and the creation of the TSC, the White House directed that the organization to consolidate watch lists should begin operations by December 1, 2003. Following the issuance of HSPD-6, the Attorney General, the Secretary of Homeland Security, the Secretary of State, and the Director of Central Intelligence signed a Memorandum of Understanding (MOU) entitled "Integration and Use of Screening Information to Protect Against Terrorism." The MOU, dated September 16, 2003, designated the FBI as the lead agency responsible for administering the TSC.

The MOU provided details related to the watch list consolidation effort, including the data that should be included and the cooperation required from the participating agencies. The MOU and HSPD-6 also mandated that federal agencies continually provide the FBI with domestic terrorism information, defined as information about U.S. persons with no connection to foreign intelligence, counterintelligence, or international terrorism. In addition, the agencies were required to provide, on an ongoing basis, the Terrorist Threat Integration Center (TTIC) with all other terrorist information in their custody or control. In turn, the FBI and TTIC were to provide domestic and international

[5] A complete listing of the acronyms used in this report is found in Appendix II.

terrorist information to the TSC for consolidation.[6] The goal was to create a unified, *unclassified* terrorist watch list, not to replace existing watch lists. Federal agencies were expected to continue gathering and developing terrorist information and to maintain separate systems to fulfill their distinctive missions.

Standing-up the TSC

In October 2003, the Attorney General appointed the Director of the TSC, and within one month two deputy directors were brought on board. An additional deputy director arrived in December 2003. TSC management initially developed working groups with participating agencies to establish an initial planning document detailing how the new organization would function. Also, the TSC designed a process flow chart to illustrate how terrorist information should be received, shared, and ultimately consolidated into an unclassified database.

The TSC's initial planning document stated that personnel detailed from the DOJ, DOS, DHS, and other agencies would make up the staff at the TSC. These individuals would represent their respective Departments while supporting the functions of the TSC and reporting to the TSC Director.

Initial Operating Capability

In accordance with the President's mandate, the TSC began operating on December 1, 2003, as the primary point of contact for screening individuals with ties to terrorism. The TSC's initial capabilities were limited, and its primary operations consisted of maintaining a 24-hour, 7-day-a-week call center staffed with personnel temporarily assigned to the TSC from agencies such as the FBI and the DHS.[7] Although TSC staff had begun developing the first consolidated watch list, it was not ready to be used for screening purposes by December 1. Instead, the TSC's protocol was to separately query a variety of existing agency watch listing systems, including: 1) Transportation Security Administration's No Fly and Selectee lists; 2) TIPOFF; 3) the FBI's National Crime Information Center (NCIC), namely the Violent Gang and Terrorist Organizations File (VGTOF); and 4) the Treasury Enforcement Communications

[6] The Terrorist Threat Integration Center 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. On August 27, 2004, the President signed an Executive Order establishing the National Counterterrorism Center (NCTC), to which all functions and activities of the TTIC were transferred. Regardless of the time period being discussed, all future references to this organization in our report will use the acronym NCTC.

[7] Throughout this report, we refer to this operation as the "call" center. However, inquiries related to some activities, such as visa applications processed through the State Department, are handled through various modes of communication.

System (TECS), which includes the Interagency Border Inspection System (IBIS) and the National Automated Immigration Lookout System (NAILS).

The Consolidated Watch List

A major challenge for the TSC was to integrate different types of information in varying formats from agencies' existing systems into a comprehensive index of watch listed individuals. The new system would ultimately need to provide real-time connectivity to users and be able to incorporate evolving technology, such as advanced name-search capability and biometric data.

To meet this goal, TSC officials and partner agency members formed a working group to define existing database structures and determine the basic functionality and future uses of the planned consolidated database. As a result of the identification of several barriers to the timely implementation of the consolidated database (such as differences in legacy systems and a shortage of qualified employees or contractors), the TSC divided the creation of the consolidated database, which was named the Terrorist Screening Database (TSDB), into three phases: 1) TSDB 1A, 2) TSDB 1B, and 3) Advent TSDB.

TSDB 1A

The TSDB 1A database, which became operational on March 12, 2004, and was discontinued on April 1, 2005, was created using proprietary software owned by a contractor. According to TSC officials, they chose this approach in an effort to consolidate the information in the most expedient way possible. The TSDB 1A was populated with data received directly from the individual supporting agencies' watch list systems. According to TSC officials, they recognized that this consolidation effort caused some names that appeared on multiple watch lists to be present in the database many times.

This database was manually updated on a daily basis using diskettes of new or revised information from participating agencies. While operating, the entire TSDB 1A database was overwritten each day when the new data file was loaded. Given the design of the TSDB 1A database, this overwriting was the only method to update the terrorist-related information. However, this process eliminated the ability to retrieve historical data from the system. In addition, the TSDB 1A could not automatically export data to the participating agencies. Rather, TSC staff was required to send manual update files to participating agencies using diskettes.

TSDB 1B

The TSDB 1B came on-line in June 2004 in a parallel environment with the 1A database.[8] In this second phase of developing the consolidated database, the TSC sought to improve connectivity between the TSDB and other databases. In creating TSDB 1B, the TSC obtained batches of records primarily from the FBI and NCTC.

On April 1, 2005, the TSC stopped using TSDB 1A, and the 1B database became the single consolidated watch list. In contrast to the TSDB 1A, the 1B database can communicate with the participating agencies' systems and provides for the electronic exchange of data. As a result, since its creation, the TSDB 1B system has been used to export records to the databases of the various participating agencies. In addition, unlike the 1A database, the TSDB 1B is updated only with additions, deletions, and modifications to the existing records in the database, and therefore the system retains a history of all changes made.

Advent TSDB and the Future of the Consolidated Database

In the next phase of its development of the consolidated database, Advent TSDB, the TSC plans to establish automatic, real-time connectivity with participating agency databases. However, most of the supporting agency database systems cannot currently accommodate this type of connection and will need to upgrade their systems. While the TSC expects that it will take years to fully implement this plan, the first segment (real-time connectivity with the FBI's NCIC) is planned for completion in FY 2005.

Also, in FY 2005 the TSC expects to receive biometric data from NCTC and export that data to NCIC. This process is not expected to be fully mature for some time and, in its initial phase, will allow for only text fields to be shared. TSC officials stated that graphic files, such as a picture of biometric data, can be made available in the TSDB 1B system, but this information would not be searchable. TSC officials said development of a plan to incorporate data into the TSDB database in this way is expected to be complete by spring 2005.

Evolution of IT Management

While the TSDB is constantly evolving, we found that the TSC's management of its information technology (IT), a critical part of the terrorist

[8] Despite the TSDB 1B coming online, TSC officials had concerns about the completeness of the records in the TSDB 1B and decided to run the TSDB 1A and 1B in parallel until these concerns could be fully addressed. Our review did reveal significant differences in the number of records between TSDB 1A and 1B. This is discussed further in the report in Chapter 7.

screening process, has been deficient. From its inception, the TSC's IT Branch – staffed with numerous contractors – did not have strong, effective, and focused leadership over the agency's IT functions. In addition, the TSC has experienced significant difficulty in hiring qualified staff with adequate security clearances to perform IT functions.

The TSC did not establish a formal technical advisory group until June 2004 and in August 2004 hired its first Chief Information Officer (CIO). Unfortunately, many major IT decisions had been made prior to this time, such as the creation and implementation of TSDB 1A and 1B and various support systems, as well as the establishment of controls and standards for operating and administering these systems. The TSC CIO acknowledged that the TSC has been operating in an immature IT environment since its inception. He told us that the need to expeditiously create a consolidated database hindered systems planning. He further stated that the IT Branch was understaffed and had not been sufficiently focused on establishing controls to ensure data integrity.

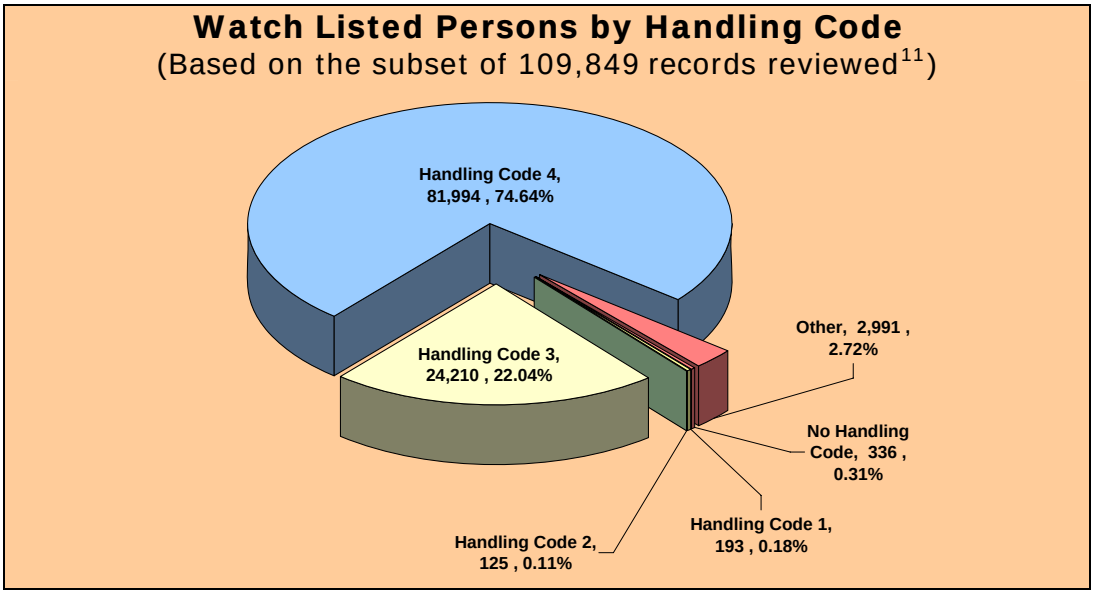
Content of the Consolidated Watch List

Each record within the consolidated watch list is designed to contain information about the law enforcement action to be taken when encountering an individual on the watch list, which provides insight into the level of threat posed by that individual. This information is conveyed through a "handling code" that provides law enforcement personnel with instructions on what to do when a suspected terrorist is encountered. These handling codes are defined as follows:

HANDLING CODE DEFINITIONS
[SENSITIVE INFORMATION REDACTED]
Source: The Terrorist Screening Center

To gain a general understanding of the distribution of individuals on the watch list, we reviewed a sample of 109,849 records in the TSDB 1B database and found that the vast majority of watch listed individuals were included in

the two lowest categories.[9] As depicted in the following graph, approximately 75 percent of the records we reviewed were categorized at handling code 4 (the lowest handling code), and 22 percent were categorized at the second to lowest level, handling code 3.[10] Only 318 records of the 109,849 records in the watch list subset that we reviewed were categorized at the two highest levels, handling codes 1 and 2. This means that the records for the overwhelming majority of watch listed individuals indicated that encounters with these persons required the lowest levels of law enforcement response and that these individuals [SENSITIVE INFORMATION REDACTED].



Source: TSC Management

We asked the TSC Director about the content of the TSC's consolidated watch list. She informed us that, to err on the side of caution, individuals with any degree of a terrorism nexus were included on the consolidated watch list, as long as minimum criteria was met (i.e., the person's name was

[9] Our sample consisted of all records in the TSDB 1B database that were eligible for sharing with the FBI's VGTOF as of October 7, 2004. The VGTOF system is queried by most federal, state, and local law enforcement officers because it is part of the National Crime Information Center (NCIC). This universe of 109,849 records represented 53 percent of the total of 207,553 records in the TSDB 1B. We selected these records for review in consultation with TSC IT staff.

[10] Records for individuals categorized as a handling code 4 often do not have enough identifying information to categorize the individual at a higher handling code. In addition, individuals at a handling code 4 level could be associates of a suspected terrorist and therefore may not pose a direct terrorist threat.

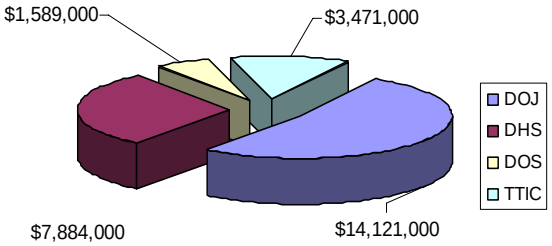
[11] The "Other" handling codes refer to one record in the subset of 109,849 records that was was transferred to the TSDB 1B from the TIPOFF database with a non-existent handling code (handling code 5). The TSC informed us that this record has been corrected. The remaining 2,990 records [SENSITIVE INFORMATION REDACTED].

partially known plus one other piece of identifying information, such as the date of birth). The Director further explained that one of the benefits of watch listing individuals who pose a lower threat was that their movement could be monitored through the screening process and thereby provide useful intelligence information to counterterrorism investigators. In addition, she stated that lower-threat level individuals can have associations with higher-threat level terrorists, and watch listing lower-threat individuals may lead to uncovering the location of other watch list individuals.

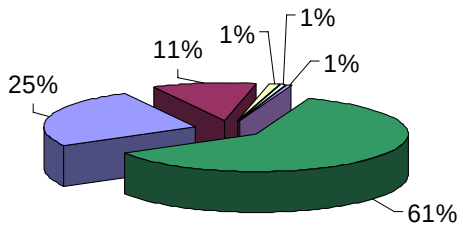
TSC Operations

The TSC's FY 2004 budget consisted of contributions totaling about $27 million from four participating agencies. As of November 2004, the TSC had 177 staff members, which included permanent and detailed personnel. Also, as detailed in the following staffing chart, contract personnel made up 61 percent of the total TSC staffing.

FY 2004 TSC Funding Allotments by Department



TSC Staffing Level by Agency as of November 9, 2004



Source: FBI Budget Formulation Office and the TSC Administrative Unit

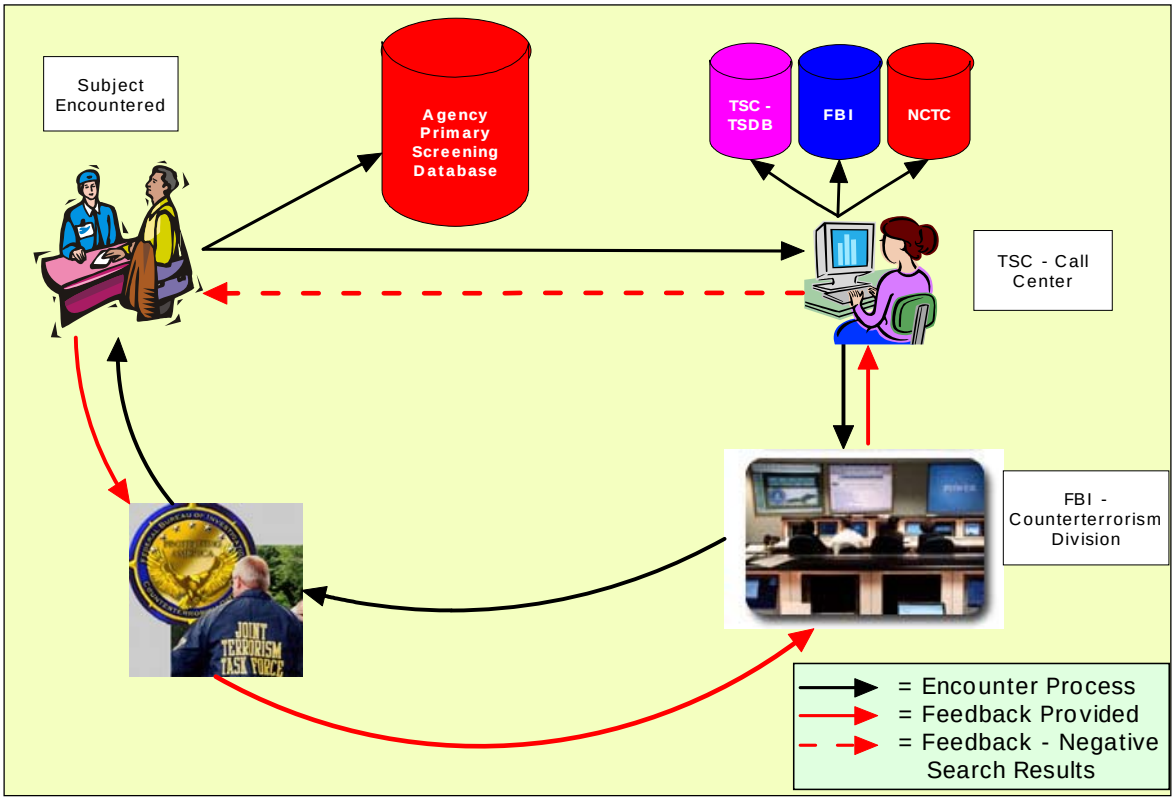
In FY 2005, the TSC's budget of $29 million was incorporated into the FBI's overall appropriation. This eliminated the need to transfer funds between agencies.

The TSC Call Center

The basic tasks performed by call center staff — fielding inquiries, researching terrorist information, and facilitating the identification and apprehension of terrorists — remain the same as the functions performed at the point of the TSC's initial operating capability on December 1, 2003. However, the creation of the consolidated watch list has allowed the call center staff to begin its research with a single database – the TSDB.

The consolidated information within the TSC database is searchable by law enforcement and intelligence officials across the country and around the world.[12] Names are searched in supporting agency databases during encounters at ports-of-entry or by federal, state, or local law enforcement agencies. When a name appears to be a match against the terrorist watch list, requestors receive a return message informing them of the preliminary match and are directed to call the TSC. When a call is received, TSC call center staff assist the caller in identifying the subject. To do this, the call screeners search the TSDB to determine if an identity match exists. In addition, they search supporting agency databases to locate any additional information that may assist in making a conclusive identification. The caller is immediately informed of any negative search results (i.e., the subject of the call does not match the identity of an individual on the watch list). The following diagram displays the process of handling hits against the watch list.

CALL SCREENING PROCESS FLOW[13]



Source: The Terrorist Screening Center

[12] Although other agencies cannot connect directly to the TSDB, the TSC exports records within its consolidated database to all supporting agency databases eligible to receive the data.

[13] This diagram depicts the general process for call screening. There can be variances based on the type of encounter, such as a border inquiry that would require the border patrol agent to first call the Department of Homeland Security's call center (the National Targeting Center), which in turn would contact the TSC.

If the subject is positively identified or the match attempt is inconclusive, the TSC call screener forwards the call to the FBI's Counterterrorism Watch Unit (CT Watch), the FBI's 24-hour global command center for terrorism prevention operations. CT Watch is then responsible for coordinating the law enforcement response to the encounter, including making further attempts to establish positive identity and, if necessary, deploying agents to take appropriate action. For every inquiry that TSC call screeners refer to CT Watch, the TSC screeners are responsible for obtaining feedback on the disposition of the encounter, such as whether or not the subject was arrested, questioned, or denied entry into the United States.

According to State Department officials at the TSC, when a person overseas applies for a visa, U.S. government officials search the CLASS database, which receives watch list information from the TSC. If this search reveals a possible identity match with an individual recorded in the TSDB, the official will send the TSC a cable (a secure, electronic communication). A State Department representative at the TSC will review the cable along with information within supporting agency databases to determine if the person requesting a visa is an individual with ties to terrorism. This information will be used by the U.S. government officials overseas to either issue or deny the visa application.[14]

Database Accuracy and Completeness

Although we found that the TSC had successfully created and deployed a consolidated watch list database, we also determined that the TSC could not ensure that the information in that database was complete and accurate. We found instances where the consolidated database did not contain names that should have been included on the watch list. In addition, we found inaccurate information related to persons included in the database.

We split our review of the terrorist watch list into two separate tracks. First, we analyzed the database as a whole, including identifying duplicate records, available fields of information, and handling instructions applied to individuals on the watch list. Second, we performed testing of the accuracy and completeness of individual records within the database. In this second track, we also identified a sample of known terrorist names and determined whether those individuals were on the watch list.

[14] The State Department's visa application review activities represent, in general, a process that existed prior to the creation of the TSC and continues to be conducted by DOS personnel. Our review of TSC activities focused on domestic and border processes and encounters.

Overall Review of the Consolidated Databases

We first reviewed the TSDB 1A and 1B to gain an overall understanding of the databases. This review included the records that each database maintained, the structure for each record, and the categories and handling instructions assigned to individual terrorist records.[15]

Database Records – As of January 2005, the TSDB 1A and 1B included a total of 455,002 and 237,615 records, respectively. Since both databases were maintained and updated simultaneously, theoretically both should have had the same number of records. However, TSDB 1A had 217,387 more records than TSDB 1B. Primarily, this difference resulted from the TSC's decision, in its early days of operation, to accept less than optimal data in order to quickly develop a comprehensive database.[16] In implementing TSDB 1B in June 2004, officials at the TSC have had more of an opportunity to identify data errors and duplications in the databases, although discrepancies found during our review indicate that the TSDB 1B also is not free of errors or duplication. Because the TSDB 1B now represents the single consolidated watch list, it is crucial that the 1B database contain all unique known or suspected terrorist records.

TSC officials informed us in March 2005 that they had successfully addressed the significant difference we had identified in record counts between the databases. They reported that they reduced the difference to about 40,200 records existing in TSDB 1A but not in TSDB 1B. This group of records has undergone initial review and the TSC stated that it consists of 39,000 records awaiting additional vetting by NCTC and 1,200 that will require manual correction at the TSC.

Duplicate Records – We reviewed the TSDB 1B and found 31 duplicate records.[17] TSC officials could not explain why TDSB 1B contained duplicate records. However, based on our observations and analysis, one probable

[15] Where possible, we reviewed both the TSDB 1A and TSDB 1B because, at the time of our testing, both databases were in use at the TSC.

[16] TSC managers stressed that the TSDB 1A consolidation effort included all records from all sources with known duplications and inconsistencies. According to them, the purpose was to consolidate the data while attempting to ensure that no name was left off the list. The TSC created the TSDB 1B, in part, to address the problem of flawed and duplicative data, which is why TSDB 1B includes some of the records from TSDB 1A but not all.

[17] We did not perform similar tests for duplication in the TSDB 1A because TSC officials explained that 1A was developed by a contractor whose contract had already ended. No one at the TSC had knowledge of the database structure in order to perform our requested queries, and contractors engaged in other major TSC developments would have needed to expend significant time to learn the database structure.

cause was the transfer of duplicate information from NCTC to the TSC. Although the number of duplicates we identified was relatively small, duplicate records within the TSDB can be time-consuming and possibly confusing for call screeners when they research an individual. For example, the screener could mistakenly rely on one record while a second, more complete record may be ignored. Also, if update information was transferred for a record in the TSDB 1B that had duplicate entries, one of the duplicate records could be updated while the other might not.

Descriptive Categories – The international terrorist records that come to the TSC from NCTC include a reference to how the individual is associated with international terrorism. This reference, called an Immigration and Nationality Act (INA) code, must be one of 25 prescribed codes, and controls exist to ensure that each record has just one code assigned. The INA codes include categories such as: "Member of a Foreign Terrorist Organization," "Hijacker," and "Has Engaged in Terrorism." These INA codes are split into two primary types – individuals who are considered armed and dangerous and those who are not.

For records in the TSDB 1B, we compared the INA codes to the database's handling codes to determine if the two were consistent. We found records with handling codes that did not correspond to the level of threat that could be posed by the individual based on the descriptive category. Specifically, we identified at least 31,954 records with INA codes that were categorized as "armed and dangerous" but had handling instructions that were applicable for individuals at the lowest handling code, which does not require the encountering law enforcement officer to contact the TSC or any other agency. The INA codes for some of these records described these individuals as: 1) having engaged in terrorism; 2) likely to engage in terrorism if they enter the United States; 3) hijacker; 4) hostage taker; 5) [SENSITIVE INFORMATION REDACTED]; and 6) user of explosives or firearms. At the time of our field work, TSC officials could not explain this apparent mismatch. This situation, which represents a weakness in the database and places front-line law enforcement officers in a vulnerable position, should be addressed as quickly as possible.

Missing Handling Codes – According to TSC officials, all records in the consolidated watch list should be assigned a handling code. Based on our review, we found that 336 records in the TSDB 1B did not have any handling codes assigned. Of these records, at least 160 were described as armed and dangerous, according to the designated INA codes.

Necessary Field Improvements – During our review of records, we also noted improvements that could be made to the watch list record fields. For example, we found no separate fields were specifically designated to identify an individual's [SENSITIVE INFORMATION REDACTED] or [SENSITIVE

INFORMATION REDACTED]. In addition, the TSC directed the FBI to assign one of three possible INA codes to all domestic terrorist records that were included in the consolidated watch list. All three INA codes provided descriptions specifically related to international terrorism, but they did not adequately describe domestic terrorism. We believe that more specific descriptions of domestic terrorist activities should be developed and applied to domestic terrorist records so that law enforcement officers can respond with better information to such a watch listed individual.

Testing of Individual Database Records

Missing or incomplete terrorist records could have significant consequences because known terrorists may go undetected if they attempt to enter the United States or are stopped by local police for a traffic violation. We reviewed the information contained within the consolidated watch list to determine whether the data was completely and accurately consolidated. Specifically, we selected judgmental samples from the source databases to determine if the unclassified information from those databases was accurately transferred to and displayed in the TSDB 1A and 1B. Our testing also included searching the TSDB 1A and 1B for records of known or suspected terrorists to ensure they were included in the consolidated database.

Missing or Inaccurate FBI Domestic Terrorist Records – We judgmentally selected a sample of 59 records (for 58 individuals) from a universe of 104,116 FBI domestic terrorist records as of August 2004. We traced our sample of records forward to the TSDB 1A and 1B to determine whether each record was included in the consolidated database and whether all pertinent, unclassified information was contained in each TSDB. We identified 8 FBI records (or approximately 13 percent of the sample we reviewed) that were not included in the TSDB 1B. FBI officials informed us that two of these records existed on an updated file that ultimately never was sent from the FBI for inclusion in the TSDB because the primary individual responsible for sending the file was out of the office and nobody filled in to assume that person's duties. The remaining six missing records resulted from technical difficulties in uploading the FBI data into the NCTC database.

Our analysis also revealed that important and relevant information within the 59-sampled FBI records was not always included in the records within the TSDB, and in some instances the information included in the TSDB was incorrect. Specifically, the source FBI database contains a miscellaneous text field that, while not searchable because of its format, can provide important data. For example, the miscellaneous field of one FBI record we reviewed contained data indicating that the subject was not a U.S. citizen, while the TSC record indicated the opposite. Conflicting information can confuse or misinform

screeners and contribute to the misidentification of an innocent person or the inappropriate release or admittance of a dangerous individual.

Missing or Inaccurate NCTC International Terrorist Records – We judgmentally selected a sample of 51 records (all for separate individuals) from a universe of 185,628 NCTC international terrorist records as of August 2004. We traced this sample of records forward to determine if the record was included in the consolidated database and if all pertinent, unclassified information set for inclusion in the TSDB was present.

We identified two records missing from the TSDB 1A that appear to have been the result of record deletion, although no history was maintained in the 1A database to verify this. In addition, 3 records from our sample of 51 were missing from the TSDB 1B. We also found that 12 records in our sample of 51 contained inaccuracies in record content between the information contained within NCTC's database and the information in the TSDB 1A and 1B. These inaccuracies included incorrect information regarding the biographical data of watch listed individuals. TSC officials could not provide an explanation for these inaccuracies.

Inclusion of Known Terrorists in the TSDB – We also performed testing on the TSDB 1A and 1B to determine if publicly known terrorists were included in the consolidated database. We selected a total of 39 names: 14 from news articles, 19 from the FBI's Most Wanted list, and 6 from the Department of State's List of Terrorists under Executive Order 13224. Our analysis found that 38 of the 39 names were included in both versions of the TSDB. The remaining name was included in TSDB 1A but not in TSDB 1B. This name originated from the Department of State and the individual was identified in the 1A database as armed and dangerous. TSC officials did not know why this name was not in the TSDB 1B.

TSC's Management of its 24-hour Call Center

We examined the management of the TSC's call center, which provides law enforcement agencies with around-the-clock access to consolidated information regarding known or suspected terrorists. The demand for expedited response times from the call center results in a fast-paced environment where data quality and system controls are crucial to safeguard the information available on the supporting databases (some of which may be classified), to ensure the accuracy of the data entry into the unclassified systems, and to maximize the quality of communication provided to TSC customers. We evaluated the center's operations and found areas in need of improvement.

As part of our testing, we selected for evaluation a judgmental sample of 30 calls to the call center. For each encounter, we traced the communication

and activities of all parties involved from the time the call was received at the TSC until the final recorded disposition of the encounter. We gathered documentation from the TSC call center, the FBI CT Watch, and the field personnel responsible for performing necessary follow-up on the encounter.

Generally, we found good communication between the TSC and all the agencies involved, including CT Watch and agencies that called the TSC. However, we identified some exceptions where coordination could have been improved. For example, in one case better coordination between agents handling an encounter could have prevented an instance where an individual was permitted to board a domestic flight despite being on the TSA No-Fly list.

We also identified several instances where the information on calls received was not being appropriately entered into the TSC system used to track encounter information, an unclassified system called the Encounter Management database. We found that data was sometimes entered into the wrong fields and at times transposed, resulting in search errors and poor data integrity. Additionally, discrepancies existed between the data available from the TSC and that of the FBI CT Watch. Examples included different times for calls being forwarded and received, different flight times on subjects due to arrive in the United States, and no resolution of the encounter recorded in the TSC's Encounter Management database. We attributed missing resolution detail to the lack of a status field in the Encounter Management database that would track the work flow and determine the calls requiring follow-up action. Although this encounter information does not affect the most important activity within the call center — screening inquiries — it does lessen the value of the information available on historical encounters. This data can be a valuable by-product of the call center activity because it can assist TSC management in evaluating the effectiveness of the organization and is also a potential source of terrorism-related intelligence.

Reliance on Detailees

Due to its rapid start-up and the need for personnel with adjudicated security clearances, the TSC has been heavily dependent upon staff detailed from participating agencies. These detailees generally work at the TSC approximately 60 to 90 days. This rapid personnel turnover increases the amount of training needed and reduces the number of screeners who are completely familiar with their duties.

Officials at the TSC stated that having detailees who can apply their investigative skills to assist callers is important to the mission of the TSC. They said the preferred arrangement would be to have staff assigned from various federal law enforcement and intelligence agencies in increments of 90 days or more. TSC management also stated that current law enforcement experience helps TSC screeners understand what the caller is

experiencing and identify when the information provided presents an investigative concern. However, we found that some detailed staff members came to the TSC directly from their initial law enforcement training or post-military service and had little experience in law enforcement or intelligence work. In addition, the regular rotating of staff hampers the TSC's ability to provide seasoned personnel that have experience as TSC call screeners. Using inexperienced screeners also results in difficulties when relaying information to CT Watch staff. For example, we were informed that special agents at the FBI's CT Watch often ask to speak to a call center shift supervisor because the initial screener has not done an adequate job of conveying the appropriate information.

Training Call Center Staff

We identified several weaknesses in the training of call center personnel. Because some of the call center managers are detailees, the TSC has had difficulty developing and implementing standard oversight procedures. In addition, at times incorrect instructions were provided to call center staff. For example, we were shown a manual that incorrectly directed screeners to search a particular database. Although this was later corrected, it illustrates weaknesses in the management of the call center.

Among other issues, the training provided to call screeners needs to stress the necessity for a thorough search of the supporting system records to ensure that all pertinent information is relayed to the FBI CT Watch. For example, we identified an instance where an individual for whom there was significant derogatory information in the NCTC's database was allowed to enter the country. The individual in question was on the watch list because it was believed that the subject posed a threat as a financial supporter of terrorism, and the individual was being considered for visa revocation. This person was allowed into the United States and the FBI took no follow-up action. Neither the TSC (including State Department officials detailed to the TSC) nor the FBI Counterterrorism Division could explain why no further actions were taken to check the status of the individual's visa revocation. The NCTC's database noted that the individual's visa was revoked three months after this individual was allowed to enter the United States, but there was no indication that this person had subsequently left the country. According to State Department officials at the TSC, the situation described above was an unusual circumstance and does not reflect the manner in which visa revocations are normally handled. While we recognize that many parties did not take proper action to resolve this situation, the TSC is the vital link for making such information available to those who need it.

Other Management Issues in the Call Center

Currently, the call screeners use a manual process to record information from callers and to forward that information to CT Watch. When a call is forwarded or is considered a negative match with no further action required, the call screener enters the data onto a form and then enters it into the Encounter Management database. This redundant data entry is susceptible to transposition errors, missed data, and other data inaccuracies.

In addition, screeners have access to information in a variety of supporting databases. This data may be classified at the Confidential, Secret, Top Secret, or other level. We found at least four instances in which information that was identified as being classified was entered into an unclassified TSC database used to track information about calls received. While this material may contribute to the detail of the encounter, it is important to ensure that controls are in place to prevent entry of classified information into the TSC's unclassified databases.

Further, the TSC does not have an automated system for tracking the amount of time that elapses between when the TSC receives a call, when the call is forwarded to the FBI for further action, when the caller receives specific instructions, and when an encounter is fully resolved and feedback is provided to the FBI and the TSC. We believe that the TSC would benefit from regularly tracking and monitoring calls to ensure that information is being provided to callers in a timely manner and to identify possible process improvements.

Strategic Needs of the TSC

The TSC has made significant progress in consolidating the U.S. government's approach to terrorist screening. In looking to the future, however, we identified several areas requiring action by TSC management to ensure that the organization fully carries out its important mission.

Strategic Planning

The TSC has no formal strategic plan by which to guide its progress, staffing, organizational structure, and future planning. TSC managers have indicated they are working on developing a strategic plan, but no formal document had been developed by the end of our field work. We believe that strategic planning efforts will assist the TSC in addressing the most significant weaknesses that we identified – namely, watch list errors and omissions, deficiencies in the management of the call center, and the immaturity of its information technology environment. A strategic plan would also help the TSC identify which improvements are most critical.

In addition, the TSC Director informed us that because the organization is relatively new, it has not yet established a formal procedure for evaluating the effectiveness of its performance. This kind of self-evaluation is important for ensuring that weaknesses are identified and corrected.

Continuity of Operations Planning

The TSC recently developed a Continuity of Operations Plan, Emergency Action Plan, and Disaster Recovery Plan. Because we did not receive any of these plans until after we had concluded our audit field work, we were unable to assess whether they had been effectively implemented. We were also unable to examine whether the TSC had tested equipment, trained employees, and performed exercises in accordance with the applicable plans.

Based on our reading of the plans, however, we have significant concerns that certain logistical and functional obstacles to successful continuity of operations have not been addressed, including access to the consolidated database at the TSC's back-up location, offsite storage of data, and the existence of alternative systems equipped to run the TSDB software and export the data to supporting agency databases. [SENSITIVE INFORMATION REDACTED]

Information Sharing

The creation of the TSC established a new approach to the sharing of terrorist watch list information. As a result, the TSC has initiated an outreach program that targets various federal agencies to inform them of the TSC's mission and determine what additional screening methods can be implemented. However, the TSC does not currently share information directly with the private sector. The DHS was charged with developing guidelines to accomplish this task, but as of March 2005, no guidelines had been developed.

OIG Conclusion and Recommendations

On December 1, 2003, the TSC began operating as the nation's centralized terrorist screening center, serving as the single point of contact for law enforcement authorities requesting assistance in the identification of individuals with possible ties to terrorism. The TSC's efforts in standing itself up within approximately 75 days of the President's mandate, establishing a 24-hour call center, and implementing a consolidated terrorist watch list within 6 months of its start date is a significant achievement. However, as a new and growing organization, the TSC has experienced many challenges, including difficulties in pulling together fragmented terrorist watch list information, an immature IT environment, and a transitory work force. In an effort to establish the call center and consolidate terrorist watch lists, planning at the TSC has taken a back seat to daily operations.

Our audit found various areas of TSC operations needing improvement. The creation of the consolidated database, a phased approach that continues to evolve, has weaknesses that need to be addressed. Database controls and improved search capabilities are necessary to ensure that watch list data is safeguarded, database history is retained, and call screeners are able to readily identify within the TSDB individuals encountered. Procedures for verifying the completeness and accuracy of records within the TSC database need to be enhanced to ensure that records are included in a timely manner, all record information consolidated into the database is complete and accurate, and measures are taken to ensure any missing, conflicting or duplicate information is identified and resolved on a regular basis. Further, a lack of sufficient training, oversight, and general management of the call screeners has left the activities of the call center vulnerable to procedural errors, poor data entry, and untimely responses to callers.

To assist the TSC in improving its operations, we have provided 40 recommendations in the following areas: database improvements, data accuracy and completeness, call center management, operational planning, coordination between participating agencies, and staffing. The specific recommendations are detailed throughout the report.

TABLE OF CONTENTS

CHAPTER 1: Introduction

Identifying suspected terrorists and keeping them out of the United States is an essential goal of the nation's counterterrorism efforts. However, soon after the terrorist attacks of September 11, 2001, it became apparent that federal agencies were using a variety of systems to track terrorist information. The federal government had no unified database of information to allow law enforcement agencies to undertake a comprehensive and timely check of databases when a suspected terrorist was screened or stopped.[18] In reviewing the events surrounding September 11, the Joint Intelligence Committee Inquiry recommended the creation of a center to coordinate and integrate all terrorist-related watch list systems.[19]

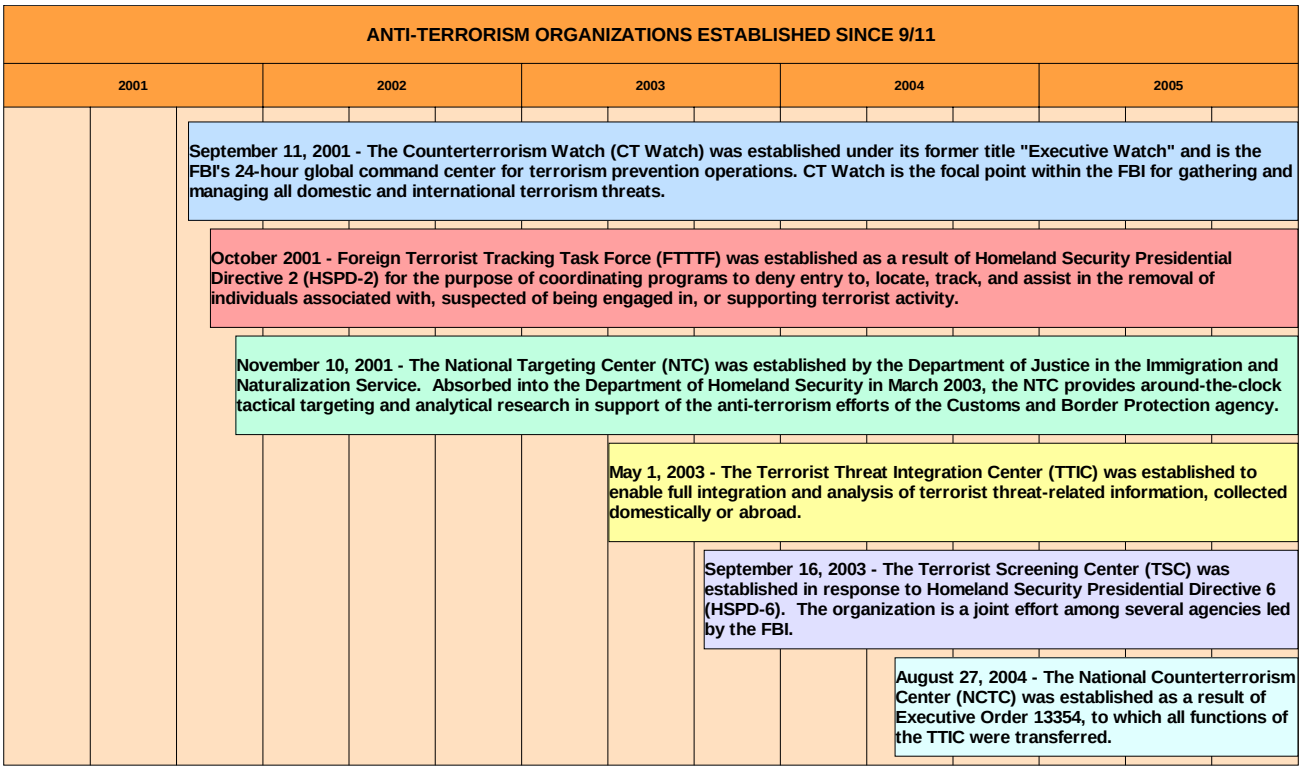
On September 16, 2003, the President signed Homeland Security Presidential Directive-6 (HSPD-6), requiring the Attorney General to establish an organization to "consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes." Specifically, the organization was assigned responsibility for consolidating terrorist watch lists and providing 24-hour, 7-day a week operational support for terrorist screening by federal, state, local, territorial, tribal, and foreign governments, and private sector organizations across the country and around the world.

The resulting Terrorist Screening Center (TSC), a $27 million organization with about 175 staff as of the end of FY 2004, is only one of several organizations established after the September 11 attacks in an attempt to protect the United States from terrorism. The following timeline reflects when these various organizations were created and the stated purpose for each.

---

[18] "Screening" refers to a process that includes, but is not limited to, government officials searching for available information on an individual in various databases. For example, a person may go through a screening process when: 1) applying for a visa at a U.S. Consulate office, 2) attempting to enter the United States through a port of entry, 3) being stopped by a local law enforcement officer for a traffic violation, or 4) attempting to travel on a commercial airline.

[19] *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001 – by the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence* (December 2002).



Source: FBI and DHS websites, HSPD-2 and HSPD-6, NCTC Fact Sheet

Prior Reviews

Two reviews conducted by the Government Accountability Office (GAO) and by the Department of Homeland Security Office of Inspector General (DHS OIG) relate directly to the work of the TSC.

The GAO review, issued on April 15, 2003, reported on the sharing of terrorist watch list information between federal, state, and local agencies.[20] This report pre-dated the creation of the TSC and focused on the importance of sharing terrorist information within the intelligence community and the opportunities for consolidating this information. The GAO concluded that the existing watch lists of various federal agencies needed to be standardized and consolidated, and that the level of federal watch list information sharing was inconsistent with congressional and presidential direction. In its report, the GAO cited 12 watch lists maintained by 9 different agencies that it said were in need of consolidation. These watch lists, the information they contain, who accesses them, and how they are utilized are discussed in detail in Chapter 2.

[20] *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, Government Accountability Office (GAO-03-322, April 2003).

The DHS OIG review focused on the DHS's role in the terrorist watch list consolidation efforts.[21] This report, issued in August 2004, criticized the DHS for not coordinating the consolidation of terrorist watch lists. It opined that DHS oversight and coordination of the overall consolidation efforts could help correct "ad hoc" management of terrorist watch list consolidation. DHS management responded to the OIG report by stating that, because it was just formed, the DHS was not in a position to manage the watch list consolidation effort at the time that HSPD-6 was drafted. The DHS noted that when the TSC was begun, the DHS was less than a year old and was still addressing significant staffing and resource challenges. DHS management noted that the President in HSPD-6 gave authority to the Attorney General to establish an organization for consolidating the government's approach to terrorism screening. The DHS response to the report further stated that the Secretary of Homeland Security and the Under Secretary for Information Analysis and Infrastructure Protection were working diligently to support the Attorney General's efforts, as outlined in HSPD-6.

Audit Approach

The purpose of this audit was to determine whether the TSC: 1) has implemented a viable strategy for accomplishing its mission; 2) is effectively coordinating with participating agencies; and 3) is appropriately managing the terrorist-related information to ensure that a complete, accurate, and current watch list is developed and maintained.

To accomplish our first objective, we examined the TSC's strategic planning outline, management correspondence, applicable legislation, directives, and executed agreements, as well as additional supporting documentation. We reviewed these documents to ensure that we had a thorough knowledge of the creation, vision, mission, establishment, maintenance, and future planning of the TSC. In addition, we conducted numerous interviews with TSC managers and staff members, as well as officials from outside the TSC.

We pursued our second objective by interviewing participating agency representatives and touring facilities to ensure we obtained a detailed understanding of the working relationships, assistance provided, and communication flow during the terrorist screening process.

[21] *DHS Challenges in Consolidating Terrorist Watch List Information,* Department of Homeland Security, Office of Inspector General (OIG-04-31, August 2004).

To fulfill our third objective, we performed testing of the databases maintained by the TSC, including the consolidated watch list. We also reviewed the primary source systems of terrorist-related information. Additionally, we met with officials in various FBI units regarding the role they play in nominating individuals to the consolidated watch list, and we analyzed the paper trail for the inclusion of individuals in the database. Detailed information regarding our audit objectives, scope, and methodology is contained in Appendix I.

In Chapter 2 of the report, we provide background on the terrorist information that existed in watch lists or databases maintained by various agencies, as well as how terrorist screening was performed by these agencies, prior to the establishment of the TSC. This chapter also contains information on the events that led up to the President's mandate in September 2003 to create the TSC. In Chapter 3, we discuss the planning phase of the TSC, including the organization's mission, role, and functions; the efforts made to stand up the organization; and the coordination among various participating agencies.

Chapter 4 contains a description of the TSC's initial operating capability along with details on how the organization functioned during its earliest days. The TSC's efforts to create a consolidated watch list database are detailed in Chapter 5, and a description of the TSC's current structure, activities, and operations is contained in Chapter 6. The results of our testing of the accuracy and completeness of the consolidated watch list are contained in Chapter 7.

In Chapter 8, we examine the activity within the nerve center of the TSC – its screening of the increasing number of inquiries from law enforcement personnel who encounter individuals whose identifying information is included in the consolidated watch list. Chapter 9 contains information on future challenges for the TSC, including the need to develop a strategic plan to guide the organization.

CHAPTER 2: Identifying the Need for a Screening Agency

After the terrorist attacks of September 11, 2001, the federal government reorganized its approach to homeland security and intelligence operations. Prior to September 11, the federal government was using information from multiple databases to attempt to preclude suspected terrorists from obtaining visas or entering the United States illegally and for tracking terrorists within the country. After the September 11 attacks, the President, Congress, and others recognized the problems with such fragmentation and called for the creation of an organization to unify the government's screening efforts.

Terrorist "Watch Lists"

The GAO report mentioned in Chapter 1 identified 12 separate "watch lists" used by the government in various screening venues.[22] According to the GAO report, each of these watch lists was developed in response to the individual agencies' mission as well as its respective legal, cultural, and information technology systems. The GAO found that these separate watch lists contributed to a decentralized and nonstandard effort in the U.S. border security mission.

Further, the GAO reported that many of the lists included redundant, but not identical, data. In addition, policies and procedures governing how the information was shared varied greatly among the federal agencies. Much of the information maintained by the federal agencies was not shared with state and local law enforcement agencies.

The following are summary descriptions for the 12 systems identified by the GAO.

- TIPOFF System – Beginning in 1987, the Department of State's Bureau of Intelligence and Research began keeping watch list (lookout) records on known and suspected international terrorists in its "TIPOFF" system. The Department of State obtained information for lookout records from intelligence community terrorism-related reports, Visa Viper cables generated by consular officers stationed abroad, law

[22] Not all of the databases identified by the GAO are considered to be true "watch lists" by the TSC. Some are databases of information on people of investigative interest (for example, a person in the Warrant Information Network may be an individual with an existing warrant who may have a terrorism nexus).

enforcement agencies, and other sources.[23] This information was stored in the classified TIPOFF system. To operate as a watch list, declassified TIPOFF records were exported to databases used by the State Department's Bureau of Consular Affairs as well as systems accessed by border patrol and immigration agents.

In September 2003, the new Terrorist Threat Integration Center (TTIC) assumed the responsibility for establishing and maintaining a single repository for international terrorist information. As a result, the State Department transferred the TIPOFF system to TTIC as a foundation for the new system.[24]

NCTC plans to replace TIPOFF with a new database – the Terrorist Identities Datamart Environment (TIDE), which is expected to come on line in mid-2005. According to officials at NCTC, TIDE incorporates analysis with the "watch list" component of the TIPOFF database to create a system capable of utilizing watch list data to make analytical associations that identify terrorist threats.

- Violent Gang and Terrorist Organizations File – The FBI's Violent Gang and Terrorist Organizations File (VGTOF), created in October 1995 to track individuals associated with gangs and terrorist organizations, is a component of the National Crime Information Center (NCIC).[25] Each record within the file is identified as either a gang or a terrorist record. The universe of terrorist records in the NCIC/VGTOF file represents

[23] The Visa Viper program is a State Department initiative created after the World Trade Center Bombing in 1993, when the State Department realized that hundreds of cables discussing terrorists had been initiated, but did not necessarily direct an individual to be watch listed. As a result, the Visa Viper program required Consular Affairs posts and other participating agencies to coordinate the submission of cables providing this specific direction on known or suspected terrorists. The program is congressionally mandated, and reports on program activities must be submitted to Congress on a monthly basis.

[24] The TTIC 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. On August 27, 2004, the President signed an Executive Order establishing the National Counterterrorism Center (NCTC) to which all functions and activities of the TTIC were transferred. Regardless of the time period being discussed, all future references to this organization in our report will use the acronym NCTC.

[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 (CJIS), is responsible for managing the NCIC database.

individuals of interest to law enforcement due to suspected or known ties to international or domestic terrorism.

- Interagency Border Inspection System – The Interagency Border Inspection System (IBIS) resides on the DHS's Treasury Enforcement Communications System, or TECS, a large computerized information system containing more than a billion records in 700 tables, designed to identify individuals, businesses, and vehicles suspected of or involved in violation of federal law. TECS is also a communications system permitting message transmittal between law enforcement offices and other federal, state, and local law enforcement agencies. The database provides access to the FBI's NCIC and the National Law Enforcement Telecommunications System (NLETS).[26] The TECS database serves as the principal information system supporting border management and the law enforcement mission of the DHS's U.S. Customs and Border Protection (CBP) and other federal law enforcement agencies.

  CBP personnel located at air, land, and sea ports of entry, as well as law enforcement and regulatory personnel from more than 20 other federal agencies or bureaus, can access IBIS. The IBIS system is used to expedite the clearance process at ports of entry and to keep track of information on suspect individuals, businesses, vehicles, aircraft, and vessels. Therefore, IBIS is considered a watch listing system.

- National Automated Immigration Lookout System – The National Automated Immigration Lookout System (NAILS) was a database created by the former Immigration and Naturalization Service (INS). It contained biographical and case data for aliens who may be inadmissible to the United States or were being sought by officials for other reasons related to immigration and law enforcement. Included in this information were lookouts for individuals associated with terrorism, representing a watch list of individuals that posed a threat to national security.

  Like IBIS, the NAILS database was housed with the TECS system, and the records of each of these systems interfaced with each other. The NAILS database was absorbed into other DHS systems in January 2005.

- Consular Lookout and Support System – The Consular Lookout and Support System (CLASS) is the State Department's tool for vetting foreign individuals applying for visas to the United States. Maintained by the Bureau of Consular Affairs, the CLASS visa database provides

[26] NLETS provides direct access to information from state motor vehicle departments.

information on aliens that is used in the determination of whether visa issuance is appropriate. This database receives information from TIPOFF on individuals associated with or suspected of terrorism and acts as a watch list during the visa issuance process and other processes involving name-checks at State Department Consular Affairs posts throughout the world.

- No-Fly and Selectee Lists – The Transportation Security Administration's (TSA) No-Fly list includes names of individuals that are to be denied transport on commercial flights because they are deemed a threat to civil aviation. The TSA Selectee list includes names of individuals whom air carriers are required to "select" for additional screening prior to permitting them to board an aircraft. Known or suspected terrorists can be submitted for inclusion to either list by an FBI case agent or an NCTC analyst. The lists are disseminated to airlines on a daily basis to be used as a watch list for comparison against passenger manifests for all flights that enter or depart U.S. airspace.

- Integrated Automated Fingerprint Identification System – Maintained by the FBI and operational in July 1999, the Integrated Automated Fingerprint Identification System (IAFIS) is a national fingerprint and criminal history system that provides automated fingerprint and latent search capabilities, electronic image storage, and electronic exchange of fingerprints and responses. According to the FBI, IAFIS is the largest biometric database in the world, containing fingerprints and the corresponding criminal history for more than 47 million subjects.[27]

  The database includes terrorism-related names and fingerprints and therefore is a watch list of sorts; however, individuals included in this database should also be included in primary watch lists such as TIPOFF or VGTOF. IAFIS supports other watch lists by making additional biometric identifying information such as fingerprints available.

- Automated Biometrics Identification System – Initially established by the former INS in 1989, the Automated Biometrics Identification System, or IDENT, contains biometric data including fingerprints and photographs used to identify and track illegal aliens who are apprehended trying to enter the United States. The system is also used to identify apprehended aliens suspected of criminal activity such as alien smuggling, aliens subject to removal for conviction of aggravated felonies, and aliens who have been previously deported. On

[27] Biometrics are discussed in additional detail in Chapter 4.

March 1, 2003, the INS and responsibility for IDENT were transferred to the DHS.

- Warrant Information Network – The United States Marshals Service maintains a Warrant Information Network that contains information on all persons with existing federal warrants.

  The TSC does not consider the information contained within this list to be a terrorist watch list. This information is maintained for the purpose of readily identifying all wanted persons and persons with existing warrants. While used as a source of additional data for terrorist screening, this list provides no independent terrorist watch list function.

- The Department of Defense Top Ten Fugitives (Air Force) – The Defense Department's Fugitive Recovery Program, run by the Air Force Office of Special Investigations, was formally implemented in 1997 to concentrate the Air Force's efforts in retrieving Air Force fugitives.

  Although the TSC has the capability to use this information as an additional source for terrorist screening, this list provides no independent terrorist watch list function. Therefore, the TSC does not consider this list to be a watch list.

- Interpol Terrorism Watch List – In 2002, Interpol established the Interpol Terrorism Watch List, which is available by secure access to Interpol offices and authorized police agencies in its member countries.[28] According to the FBI, the list contained approximately 100 names as of June 2004 and all of the individuals were accounted for on a primary watch list, such as VGTOF or TIPOFF.

While the GAO reported that 9 different federal agencies maintained 12 different lists of terrorist information, as noted above, several are not considered by the TSC to be true watch lists. According to the TSC, the primary watch listing systems were: TIPOFF, NCIC/VGTOF, TECS (and its sub-systems of IBIS and NAILS), CLASS, and the No Fly and Selectee Lists.

[28] The stated mission of Interpol is to provide essential services for the international law enforcement community to optimize the effort to combat crime. The three core services that it provides are: 1) a global police communication system, 2) a range of criminal databases and analytical services, and 3) support for police operations throughout the world. The National Central Bureau of Interpol within the DOJ coordinates with the international organization on behalf of the U.S. government.

Early Discussion of a Consolidated Watch List

The push for a consolidated watch list began after the September 11 attacks. The President's National Strategy for Homeland Security and Congress' inquiry into the September 11, 2001, terrorist attacks both discussed the concept of a consolidated terrorist watch list.

July 2002 National Strategy for Homeland Security

In July 2002, the President issued the National Strategy for Homeland Security, which was designed to create a "comprehensive plan for using America's talents and resources to enhance our protection and reduce our vulnerability to terrorist attacks."[29] This strategy emphasized that no one agency or computer network at the time integrated all available homeland security information. Rather, the information was contained within several federal, state, and local systems, much of which was redundant or supplemental to other watch list data. Terrorist data contained in one database was unlikely to be systematically shared with all levels of government that needed the information. For example, the President's strategy highlighted the importance of consolidating this information to avoid potential errors that could result from agents on the borders and at consular posts not checking information against consistent watch lists. Specifically, the President's strategy stated that "It is crucial to link the vast amounts of knowledge resident within each agency at all levels of government."

The President's strategy identified two primary barriers to an efficient government-wide information system. The first involved the lack of coordination between agencies when acquiring new information technology systems. The strategy stated that while hundreds of new systems were purchased, they were designed to address specific agency needs alone without considering database compatibility among federal, state, and local agencies. This method of networking was described by the President's strategy as an obstruction to efficient collaboration. The second issue involved the cultural differences between agencies and the resulting barriers that prevent their distinct information from being integrated with that of other agencies.

The President's strategy called for the FBI to create a consolidated terrorism watch list that "includes information from a variety of sources and will be fully accessible to all law enforcement officers and the intelligence community." This consolidated watch list would "serve as a central access point for information about individuals of investigative interest," avoiding the

29 Office of Homeland Security, National Strategy for Homeland Security (July 2002).

uncoordinated and ad hoc approach that agencies were taking to minimize terrorist threats within the United States.

The 9/11 Congressional Joint Inquiry

In its review, the 9/11 Congressional Joint Inquiry Committee reported in December 2002 that the U.S. government was not adequately collecting and integrating terrorism-related information from all domestic and foreign sources or appropriately sharing this information among the intelligence and law enforcement communities. The Committee also noted that the intelligence agencies created unclassified products to provide guidance to groups such as private companies, state and local governments, and the public. As a result, the Committee recommended that the U.S. government create a national watch list center to facilitate the development and use of new technologies to help ensure that information about known or suspected terrorists was appropriately collected, declassified, and shared.

GAO Report

As noted in Chapter 1, the GAO examined the federal government's watch list efforts and issued its report in April 2003. Although the GAO did not explicitly recommend that all 12 systems that it identified be consolidated, it reported that there was a need to consider some sort of consolidation effort of terrorism-related information.

CHAPTER 3: Planning Phase of the TSC

On September 16, 2003, the President signed Homeland Security Presidential Directive-6 (HSPD-6), which initiated the creation of the Terrorist Screening Center and the consolidated terrorist watch list.

Establishing the Mission, Role, and Functions of the TSC

Through HSPD-6, the President directed the Attorney General to establish an organization with the mission to "consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes." The goal was to create a unified, sensitive but *unclassified* terrorist watch list, not to replace the existing watch lists maintained by various federal agencies. These agencies were expected to continue gathering and developing terrorist information and to maintain separate systems to fulfill their distinctive missions. In a news release announcing the signing of HSPD-6, the White House announced that the TSC would be operational by December 1, 2003.

To implement HSPD-6, a Memorandum of Understanding (MOU) entitled "Integration and Use of Screening Information to Protect Against Terrorism" was signed on September 16, 2003, by the Attorney General, the Secretary of Homeland Security, the Secretary of State, and the Director of Central Intelligence. The MOU designated the FBI as the agency responsible for administering the TSC. The MOU also described the level of cooperation that would be needed, including the sharing of staff and information from the participating agencies.

The MOU specifically directed the TSC to maintain a continually updated database containing U.S. government terrorist information. This database was expected to be an unclassified subset of the data maintained by federal law enforcement and intelligence agencies. Therefore, the consolidated watch list would be an index of watch listed individuals, and the records would include unclassified identifying information for these individuals.

Former Secretary of Homeland Security Thomas J. Ridge described the role of the TSC as "to make sure we get this information to our agents on the borders and all those who can put it to use on the front lines - to get it there fast."[30] To that end, the TSC was given the responsibility to merge international and domestic terrorist information into one centralized unclassified database and to provide federal, state, and local agencies with the ability to better identify potential terrorists encountered within the

[30] September 16, 2003, News Release: "New Terrorist Screening Center Established," http://www.whitehouse.gov/news/releases/2003/09/print/20030916-8.html

United States and at the borders.[31] The TSC was expected to provide around-the-clock assistance with and access to the information.

Standing-up the TSC

In October 2003, the Attorney General appointed the Director of the TSC, and within one month, two deputy directors were brought on board. An additional deputy director arrived in December 2003. TSC management initially developed working groups with participating agencies to establish an initial planning document detailing how the new organization would function. The TSC designed a process flow chart to illustrate how terrorist information should be received and shared, and ultimately consolidated into an unclassified database.

In order for the TSC to begin operating by December 1, 2003, it was co-located with the Foreign Terrorist Tracking Task Force (FTTTF).[32] The FTTTF provided space, equipment, personnel, and technological and financial support to assist in the creation of the TSC. According to the TSC and the FTTTF, the FTTTF's financial support of the TSC in FY 2004 totaled between $6.5 and $7.8 million.

As TSC management began its efforts to implement HSPD-6 and the MOU, it quickly found that processes related to maintaining a terrorist watch list or responding to an identified terrorist were not formally articulated. As a result, TSC officials began developing procedures and criteria related to: 1) adding or removing terrorist names to or from the individual lists maintained by the participating agencies, 2) providing instructions to law enforcement agencies in the event that a terrorist was identified, and 3) coordinating communication and feedback among the many law enforcement agencies that might be involved.

The TSC planned and assembled its operations center within an existing FTTTF facility. All TSC personnel were required to have appropriate clearances because of the nature of information they would need to research when attempting to identify a person on one of the watch lists. Therefore, TSC staff spent significant time coordinating the necessary security clearance issues during this developmental period.

[31] The TSC's efforts to create such a database are detailed in Chapter 4.

[32] The President established the FTTTF through Homeland Security Presidential Directive-2 as a multi-agency effort led by the Attorney General with assistance from the Secretary of State, the Director of Central Intelligence, and other government officials, as appropriate. The mission of the FTTTF is to ensure that federal agencies coordinate programs to: 1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and 2) locate, detain, prosecute, or deport any such aliens already present in the United States.

In November 2003, the TSC brought an FBI special agent on board as the Chief of Operations. His initial duties were to obtain the software and hardware for the TSC operations and to create the call center logs on which call activity was to be recorded. Additionally, he interviewed personnel who were detailed to the TSC from the different participating agencies in order to match skill levels to the types of duties that needed to be fulfilled.

The TSC developed an initial planning document in November 2003 that consisted of a series of documents detailing the procedures and criteria to be followed. The plan included procedures for how to communicate with various agencies when a suspected terrorist was encountered. The TSC decided early on that the FBI's Counterterrorism Watch (CT Watch) and the DHS's National Targeting Center (NTC) would be involved in the operational response to an encounter with a terrorist. CT Watch is the FBI's 24-hour global command center for terrorism prevention operations, while the DHS's NTC provides around-the-clock tactical targeting and analytical research in support of the anti-terrorism efforts of the Customs and Border Protection agency.

In addition, the TSC identified the end users, or "customers," of its services to include: 1) the Department of State (DOS), which includes the Bureau of Consular Affairs and the visa application and revocation process; 2) the Department of Homeland Security (DHS), and its subcomponents such as the Customs and Border Protection (CBP), Immigration and Customs Enforcement, the Bureau of Citizenship and Immigration Services, and the Transportation Security Administration (TSA); 3) the Department of Justice (DOJ) and its subcomponents such as the FBI and the multi-agency FTTTF; 4) the Department of Defense, including the branches of the U.S. Armed Forces; 5) other federal agencies; 6) state, local, and tribal law enforcement agencies; 7) foreign countries supporting U.S.-led counterterrorism efforts; and 8) industries and infrastructure deemed critical.

The initial planning document stated that personnel detailed from the DOJ, DOS, DHS, and other agencies would comprise the staff at the TSC; however, the document did not specify the number of staff to be provided by the participating agencies. The detailed staff would represent and support their respective Departments, while supporting the functions of the TSC and reporting to the TSC Director. For example, a State Department employee would perform numerous tasks while assigned to the TSC, such as determining which terrorist records should be included in the DOS Consular Lookout and Support System (CLASS) database, examining information related to visa applications and visa holders for terrorist links, coordinating with the State Department's Counterterrorism Office, Bureau of Consular

Affairs, and Bureau of Intelligence and Research to enhance information sharing with foreign governments, and implementing information sharing agreements between the United States and foreign governments.

CHAPTER 4: Initial Operating Capability

On December 1, 2003, the TSC began operating as the primary point of contact for screening individuals with ties to terrorism. While operational, the TSC's capabilities at this time were limited due to its recent establishment. Its primary component was a 24-hour, 7-day a week call center staffed with personnel temporarily assigned to the TSC from participating agencies such as the FBI and the DHS.[33] Although work had begun on developing the first consolidated watch list, it was not ready on December 1 for screening purposes. Instead, the TSC relied on previously existing individual databases or lists to screen persons suspected of having links to terrorism.

When the TSC first became operational, officials established daily briefings that provided a framework for ensuring that TSC staff were focused on priority matters and that on-going or quickly arising issues needing special attention were presented to management. The daily briefings remain an essential management tool at the TSC and, in our opinion, represent a best practice during the infancy of an organization with such an important national security mission. The prior day's activities are discussed in these meetings and a list of action items is maintained. In addition to TSC staff, staff from the FBI's Counterterrorism Division and NCTC regularly attend these meetings.

TSC Call Center

According to TSC officials on-board at the time, by December 1, 2003, the TSC had established a call center staffed with detailees from the various participating agencies. These individuals were experienced in the functions of their home agencies and the related databases used for terrorist screening, which were now available to the TSC in one location.

The call center, co-located with the Foreign Terrorist Tracking Task Force (FTTTF), was initially equipped with computers individually networked to the source watch listing systems. However, access to the individual systems in the call center was limited. Often, agency representatives detailed to the call center were the only individuals at the TSC with the authorization and passwords to use systems owned by their agency. As a result, call center staff relied on each other to fulfill the screening needs of the calls received.

[33] Throughout this report, we refer to this operation as the "call" center. However, inquiries related to some activities, such as visa applications processed through the State Department, are handled through various modes of communication.

Screening Process Prior to the Consolidated Database

TSC officials stated that as of December 1, 2003, the call center was staffed and ready to respond to inquiries from the law enforcement and intelligence communities. While no consolidated database was yet in existence, the TSC and its partner agencies worked together to electronically identify terrorist records within the supporting watch listing systems. As a result, when one of these terrorist records was queried by a front-line law enforcement official, the system would provide instruction to call the TSC. The call center staff recorded on a hard copy form the subject's identifying information, the caller's name, and call-back information including the law enforcement agency's main precinct/headquarters telephone number and evidence to ensure that the caller was a representative of a valid law enforcement agency. The call screener would then initiate a search of each agency database in an effort to determine if the person encountered was a match against any identities within the various databases. Often, this search involved multiple call center staff members because access to the participating agency databases generally was limited to employees from that agency.

The TSC forwarded to the FBI's CT Watch all calls where a positive identity match was made against a record on a watch list, or if the match could not be confirmed or refuted. Once involved, CT Watch was responsible for coordinating directly with the law enforcement officer who initially called the TSC and deciding how the FBI would operationally respond to the encounter. If an immediate law enforcement response was required, CT Watch would deploy nearby FBI agents or coordinate with the Joint Terrorism Task Force (JTTF) within the area of the encounter.[34]

Encounter Tracking

Beginning on the first day of call center operations on December 1, 2003, the TSC began tracking the calls it received as well as the adjudication of the matters. To facilitate this tracking, the TSC maintained a log that included 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 a match against a watch list record (i.e., positive, negative, or inconclusive), and, if appropriate, a notation that the inquiry was forwarded to CT Watch. In addition, TSC staff were responsible for following up to obtain and record data about the

[34] The JTTFs are teams of FBI agents, state and local law enforcement officers, and other federal agents and personnel who work together to investigate and prevent acts of terrorism.

CT Watch response to the call along with any other information about actions taken by law enforcement or additional data about the subject.

Other TSC Efforts

Although the call center was a major portion of the TSC's activity as of December 1, 2003, officials and staff were also in the process of designing the consolidated watch list database required by HSPD-6. These efforts are discussed in detail in Chapter 5. In addition, the TSC was working to establish a process for resolving instances of persons wrongly identified as suspected terrorists and working to educate the law enforcement and intelligence communities about the TSC's mission, role, and functions.

Early Outreach Efforts

In January 2004, the Director of the TSC reported that most calls to the TSC came from the DHS's Customs and Border Protection and were the result of encounters with possible terrorist subjects at the nation's borders. The remaining inquiries came from the Department of State's Bureau of Consular Affairs and state and local police departments.

In these early days, the TSC had not established a formal plan for conducting outreach, but understood the importance of informing other agencies of the service that it could provide in the overall counterterrorism effort. To heighten awareness of the TSC's usefulness to the law enforcement and intelligence communities, the TSC began to give briefings to such organizations as the Department of Defense; the FBI's Basic International Terrorism School in Quantico, Virginia; the New York Police Department; and various federal, state, and local law enforcement agencies gathered together for a conference on Homeland Security. The TSC representatives also articulated the importance of each agency's terrorism-related data and asked that such information be shared in order for the TSC to receive the information for screening purposes.

Establishing a Misidentification Process

Also during this time, TSC officials stated that they were in the process of developing procedures for handling erroneous or outdated information. As of January 2004, the Director reported that several such records had already been identified and were updated or removed. TSC officials said they also discussed creating an "Office of Ombudsman" to handle instances where individuals were incorrectly matched against a watch list record due to similarities of identifying information (known as the misidentification process). However, these processes and procedures were still in their

infancy, and very little progress was made during the TSC's early months. The misidentification process is discussed further in Chapter 8.

Conclusion

As of December 1, 2003, the TSC was up and running and had centralized the location of disparate terrorist watch list information developed by multiple agencies and used in different ways. In January 2004, the TSC Director reported to Congress that as of December 31, 2003, the TSC was able to: 1) make the names and identifying information of known or suspected terrorists accessible to federal, state, and local law enforcement; 2) have a system for properly reviewing whether a known or suspected terrorist should be included in or deleted from additional screening processes; 3) administer a process to ensure that persons who may share a name with a known or suspected terrorist were not unduly inconvenienced in U.S. government screening processes; and 4) implement a system to adjust or delete outdated or incorrect information to prevent problems arising from misidentifications.[35] Many of these accomplishments continued to be works in progress, but the TSC's effort to achieve initial operating capability within about 75 days of the President's mandate to create a screening organization was a significant accomplishment.

[35] Statement of Donna A. Bucella, Director, Terrorist Screening Center, before the National Commission on Terrorist Attacks Upon the United States, January 26, 2004.

CHAPTER 5: The Consolidated Watch List

Throughout the existence of the TSC, its management has focused much effort in developing and deploying technology capable of consolidating the different watch lists into a single database. A major challenge for the TSC was to integrate different types of information in varying formats from the existing systems into a comprehensive index of watch listed individuals. The new system would also ultimately need to facilitate real-time connectivity to end-users and include evolving technology, such as advanced name-search capability and biometric data.

The Memorandum of Understanding executed following the President's mandate to create a terrorist screening organization in HSPD-6 provided direction to the TSC regarding its responsibility to develop a consolidated database. Specifically, the MOU required the TSC to consolidate the government's approach to terrorism screening and to maintain a continuously updated database containing unclassified terrorist information from the FBI and NCTC. The MOU required that the FBI serve as the TSC's source with regard to purely domestic terrorism information, 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. The MOU also required that NCTC serve as the TSC's source of terrorist information, with the exception of the domestic information that the FBI was required to provide. In turn, federal agencies were directed to provide all domestic and international terrorist information in their possession, custody, or control to the FBI and NCTC, as appropriate.

Upon its creation in September 2003, TSC officials and partner agency members formed a working group to define existing database structures and determine the basic functionality and future uses of the consolidated database that they were tasked with creating. During this initial planning process, TSC officials identified several barriers to the timely development of the consolidated database. First, TSC officials stated that there was a shortage of knowledgeable IT professionals with the necessary security clearances to work at TSC. Second, a TSC official did not believe that one contractor had sufficient numbers of qualified employees to complete the full design and implementation of the consolidated database. Third, attempting to hire a single contractor to create the ideal database environment would be cost prohibitive. Finally, because of the critical nature of the project, the TSC faced a compressed deployment schedule. As a result, the TSC divided creation of the consolidated database, which was named the Terrorist Screening Database (TSDB), into three phases: 1) TSDB 1A, 2) TSDB 1B, and 3) Advent TSDB.

TSDB 1A

According to TSC officials, the initial phase of the database, TSDB 1A, was created using proprietary software owned by the contractor. According to TSC officials, this decision was made in an effort to consolidate the watch list information in the most expedient way possible. The TSC understood when entering this contract that it was purchasing a proprietary software application and that all of the contractor's programming would continue to remain the property of the contractor. In addition, any modifications to the program or running sophisticated queries would require the contractor's expertise. The limitations of TSDB 1A, according to TSC officials, would be addressed in the second phase, TSDB 1B.

Between September 2003 and February 2004, TSC staff worked with the contractor to examine the system architecture of the source databases and define the system requirements for the TSDB 1A. This included ensuring that the information that would be received from the participating agency databases, such as individual names and dates of birth, would be compatible with the fields being created for the 1A database.

Although the MOU required the TSC to receive all terrorist information from the FBI and NCTC, at the time of the creation of TSDB 1A the infrastructure for this process was not yet established and the FBI and NCTC were not reliably receiving and inputting terrorist information from other agencies. This resulted in the TSC directly obtaining information from other sources to populate the 1A database.

In February 2004, the TSC began the consolidation of terrorist information by conducting a one-time, manual batch acceptance of data from each of the various supporting systems into the TSDB 1A. This effort included obtaining information directly from the No-Fly and Selectee Lists, as well as from the following systems: TIPOFF, VGTOF, and the Treasury Enforcement Communications System (TECS). By populating the TSDB with information from these five sources, the TSC incorporated information from each of the primary watch listing systems discussed in Chapter 2. As noted in Chapter 2, the remaining systems generally were subsets of information contained in the primary systems or were not actual watch listing systems.

TSC personnel believed that this method of obtaining records was an efficient and effective way of initially populating the TSDB with the most comprehensive universe of terrorist information possible. However, they also recognized that some terrorist watch list records would not be received due to differences in system architectures and participating agency missions, processes, and data requirements. According to the TSC, these obstacles

could not be addressed quickly and in many cases could not be anticipated. However, the time constraints under which the TSC was operating mandated that a consolidated database be developed and populated expeditiously. TSC management has asserted that the organization is still working to resolve obstacles to the receipt of additional data.[36]

TSC management further informed us that neither TSC staff nor the participating agencies reviewed the data prior to its transfer to the TSC because of time constraints and the volume of work involved. Further, because these systems were being relied upon as independent systems, TSC officials believed them to be sufficiently reliable for acceptance.

According to TSC officials, the TSDB 1A began operating on March 12, 2004, and was discontinued on April 1, 2005. The database was manually updated daily using diskettes of new or revised information from the participating agencies. The entire TSDB 1A database was overwritten each day when the new data file was loaded. Given the design of the TSDB 1A database, this overwriting was the only method available to update the information. However, overwriting the data on a daily basis eliminated the ability to view the database in historical context. In addition, the TSDB 1A could not automatically export data to the participating agencies. Rather, the system relied on TSC staff to manually send updated files on diskettes to the supporting systems. The updated information was then uploaded into the databases of the participating agencies. (TSDB 1B, as discussed below, sends direct electronic updates to the agencies.)

TSDB 1A Name-Search Capability

When call screeners at the TSC searched a name in the TSDB 1A, the system used a software application to search on the phonetic code of the last name or the last name with a first name initial, as well as the exact month and day of birth and a plus or minus one in the subject's birth year. The search software recognized when a nickname was being searched and replaced it with the corresponding proper name (e.g., "Bill" would be replaced with "William"). In addition, searches for names beginning with a silent letter, such as "Knight," would result in several corresponding spellings (such as "Night").

TSC officials reported that this search software did not provide consistently good results on names not originating in Europe or the Americas. TSC managers recognized the shortcomings of this search system and attempted to improve search capabilities in subsequent versions of the

[36] We reviewed the TSDB 1A database for accuracy and completeness. The results of our testing are contained in Chapter 7.

database. Name-search capabilities are discussed in further detail in the TSDB 1B and Advent TSDB sections of this Chapter.

TSDB 1B

TSC management opted to use a different contractor for the development of the second phase of the consolidated database – the TSDB 1B. The primary purpose of this phase was to create a system that provided the TSC with more control over the database and its management and to improve connectivity between the TSDB and other databases.

The new contractor created the TSDB 1B using the basic structure of the State Department's TIPOFF system, which has more flexible and comprehensive search capabilities than the TSDB 1A. In creating the 1B database, the TSC obtained batches of records primarily from the FBI and NCTC, in accordance with HSPD-6 and the resulting MOU, which as noted previously required all federal agencies to provide terrorist information to these two agencies.[37]

According to TSC management, the TSDB 1B was originally scheduled for full operational capability, including call screening and exporting of records, by June 2004. Despite it coming online at that time, TSC officials had concerns about the completeness of the records in the database and decided to run the TSDB 1A and 1B in parallel until these concerns could be fully addressed. As noted previously, the TSC stopped using TSDB 1A on April 1, 2005, at which time the 1B database became the single consolidated watch list.[38]

Unlike TSDB 1A, the 1B database can communicate with the participating agencies' IT infrastructures and databases and can provide automatic data exchange, eliminating the need for daily diskette transfers of new and updated information. Because the TSDB 1B system has the capability for automatic data exchange, it has been used since its inception to export records to the databases at the various participating agencies. In

[37] During a query performed on the 1B database, we identified five records that did not originate from the VGTOF or TIPOFF or databases (the systems used by the FBI and NCTC, respectively). TSC staff could not explain the source of these records. Further details of this matter are explained in Chapter 7.

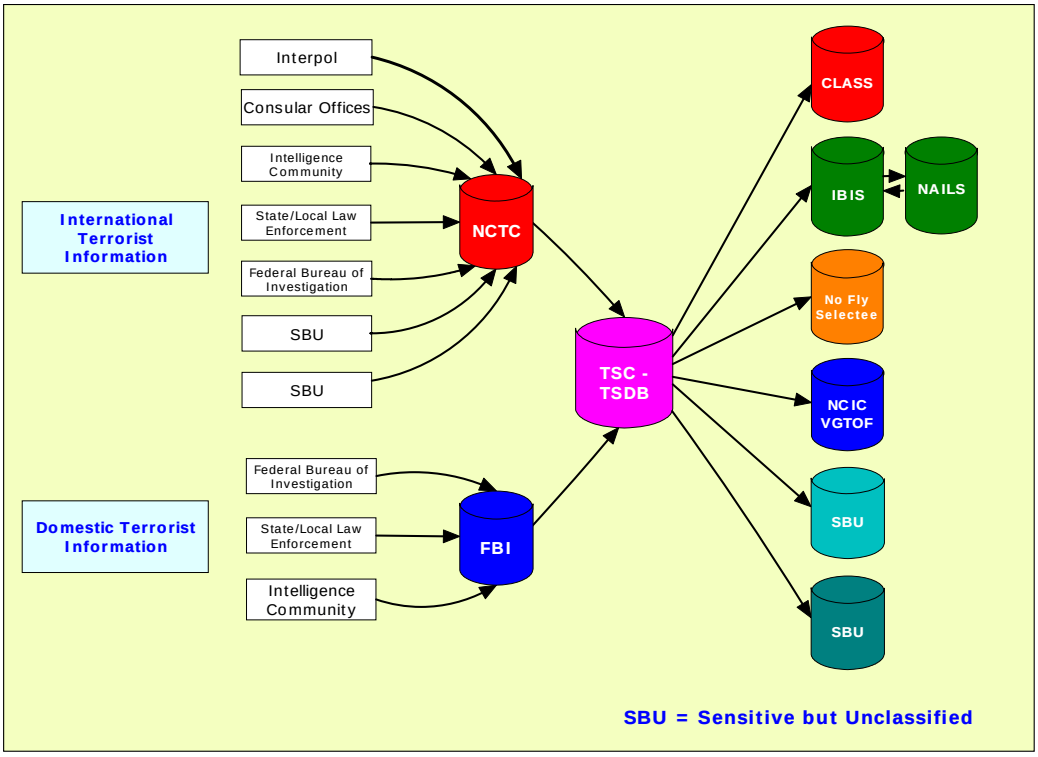
[38] TSC officials explained that the delay in achieving full operational capability of the TSDB 1B resulted in part from technical difficulties related to integrating watch list data in a manner that would ensure supporting agency databases receive in return an appropriate level of detailed information. The delay also resulted from the need to prevent duplicate records from being integrated into the TSDB 1B database. TSC officials explained that there was a shortage of available contractors to work on the project because NCTC was using the same company for its database work.

addition, unlike the TSDB 1A, the 1B system does not overwrite the entire database of records on a daily basis. Instead, the TSDB 1B is updated only with additions, deletions, and modifications to the existing records in the database. Consequently, the system retains a history of all changes that were made to the records. This is a stronger system control that provides the TSC with the advantage of tracing record changes and allows for a greater ability to review data accuracy and reliability.

Data Process Flow

As shown in the following chart, information regarding international terrorism from consular offices, Interpol, the intelligence community, the FBI, state and local law enforcement, and foreign governments is now funneled through NCTC for inclusion in the consolidated watch list. In addition, information regarding purely domestic terrorism from the FBI, state and local law enforcement, and the intelligence community is processed through the FBI for inclusion in the consolidated watch list. The TSC then makes the information from the TSDB available to the appropriate end users, such as border patrol agents, consular offices, and state and local law enforcement. For example, new information regarding an airline hijacker obtained from an overseas consular officer travels to NCTC for vetting. The NCTC then transfers the information on the subject to the TSDB, where the data is distributed to pertinent systems such as CLASS, IBIS, No-Fly, VGTOF, and others.

Domestic and International Terrorist Information Data Flow



Source: TSC Management

TSDB 1B Name-Search Capability

Because the TSDB 1B system architecture is based on the TIPOFF database, the system uses a name-search capability called [SENSITIVE INFORMATION REDACTED] that is more advanced than the 1A system. Specifically, the [SENSITIVE INFORMATION REDACTED] software uses a broader algorithm for searching names that returns query results more precise to all cultures of names within the database. This software has been used by the State Department since the creation of TIPOFF in 1987. According to DOS officials, [SENSITIVE INFORMATION REDACTED] has been an effective tool in the terrorist watch list process.

Advent TSDB and the Future of the Consolidated Database

In the short term, the TSC plans to make improvements to the TSDB 1B that will increase its completeness, functionality, and usability. The database was programmed to contain fields for additional information including: comments, data sources, and biographical information. However, TSC officials did not enable these fields at the time the system initially came on line in June 2004. The TSC has undertaken an initiative called the "wedge project" to enable and populate these fields. In October 2004, the initial database programming for this project was complete. According to the TSC CIO, however, the TSC is not yet receiving much additional information, primarily because of differences in formatting. The CIO stated in December 2004 that the TSC was in formal negotiations with participating agencies as to the format in which the information is to be sent.[39]

The TSC's ultimate goal is to create a database called "Advent TSDB" that will establish real-time connectivity between the TSDB and all supporting agency databases. TSC officials also noted that Advent TSDB will include a full-range of biometric data. This information will improve the screening process by providing additional descriptive data against which to screen encountered individuals.

Connectivity

Real-time connectivity between the TSDB and the supporting agency databases will permit the rapid transfer of information between these systems, increasing the timeliness and completeness of all participating systems' databases while requiring less human involvement. However, most of the participating agencies have different computer operating systems and architecture that may not handle this type of connection. As a result, agencies

[39] For example, the complexion of an individual needs to be recorded in one standard format so the information is searchable.

will need to upgrade their systems to facilitate this capability. While the TSC expects that it will take years to fully implement this plan, the first segment is planned for completion in FY 2005. This first phase will automatically connect NCIC to the TSDB through the Criminal Justice Information Services Division (CJIS), therefore allowing all federal, state, and local law enforcement officials with NCIC access to have immediate, direct, real-time connectivity with TSDB.

Biometrics

The TSC expects that during FY 2005 it also will develop the ability and implement procedures to receive biometric data from NCTC and export that data to NCIC. However, this process is not expected to be fully mature for some time. According to the CIO at the TSC, there is no uniform standard of acceptability for biometric data among the supporting systems. Therefore, only text fields for biometric data are planned to be shared in the first phase. TSC officials stated that graphic files containing some of this information can be made available in the TSDB 1B system; however, this information would not be searchable. In essence, a picture of the biometric information can be stored in the database. TSC officials said that they are awaiting action by other entities to establish the uniform standards and did not know when further progress was anticipated.

Currently, TSDB 1B is an independent system that is not directly connected to the supporting databases. Therefore, in order to access available biometric information, TSC staff must query the source databases, which reside on multiple networks or computer terminals. This may involve searching up to five different systems and switching between classified and unclassified environments. These cumbersome procedures increase the likelihood that biometric information will be missed and adds to the amount of time that TSC staff must take to research available information. The TSC, in conjunction with partner agencies, is currently taking steps to accommodate necessary biometric data in its watch listing efforts.

Name-Search Capability

TSC IT officials have indicated that [SENSITIVE INFORMATION REDACTED] will remain as the TSDB's name-search capability for the foreseeable future. Although the State Department considers this to be a well-operating program, in the long term the TSC hopes to improve upon its name-search capability and is researching other government agencies' experiences with the effectiveness of various programs. For example, the [SENSITIVE INFORMATION REDACTED] developed by [SENSITIVE INFORMATION REDACTED] has been adopted by NCTC for use in its new Terrorist Identities Datamart Environment (TIDE) database. This program provides for the automatic expansion of names to incorporate

phonetic, cultural, and character variations, as well as combinations of these variations. Since one name can be spelled multiple ways, the software manufacturer claims to use search techniques that allow maximum efficiency in query results. While the TSC continues to research the best software for its mission, a TSC official said in October 2004 that the end product probably would be an expansion of the [SENSITIVE INFORMATION REDACTED] software.

Evolution of IT Management

In its relatively short existence, the TSC has experienced numerous changes in its Information Technology (IT) Branch. We found that the management of such an integral part of the terrorist screening process has been deficient. The TSC's IT Branch – staffed with numerous contractors and little consistent management oversight – has not had strong, effective, and focused leadership over the agency's IT functions. In addition, the TSC has experienced significant difficulty in hiring qualified staff with adequate security clearances to perform IT functions.

Prior to May 2004, the TSC's IT Branch was led by acting Program Managers, each of whom was a contractor. In June 2004, the first non-acting, non-contractor Program Manager was brought on board, and he immediately began modifying plans for the next phase of the TSDB. However, the TSC did not hire its first CIO until August 2004.

In June 2004, the TSC established the Systems Architecture Board, which serves as the technical advisory group to the TSC Director, Deputy Directors, and TSDB Project Manager. The group, comprised of IT personnel from the TSC and contractors, is responsible for developing the TSDB system's architecture.

Unfortunately, many major IT decisions were made prior to the arrival of the CIO and the creation of the Systems Architecture Board in June 2004. These include the creation and implementation of TSDB 1A and 1B and other support systems, as well as the establishment of controls and standards for operating and administering these systems. The CIO told us in October 2004 that the TSC has been operating in an immature IT environment since its inception. He explained that systems planning was negatively affected by the need to expeditiously create a consolidated database. He further stated that the IT Branch was understaffed and had not been sufficiently focused on establishing controls to ensure data integrity.

In our meetings with the TSC's CIO, we found that he has an extensive background in both the information technology and intelligence fields. He also has acknowledged the need for active controls and audit trails within

the TSC's databases and manual processes. Such audit trails and controls are important because our review of the current TSC databases found little tracking and retention of historical transactions within the databases, as well as a shortage of human access controls.[40]

Content of the Consolidated Watch List

Each record within the consolidated watch list is designed to contain information about the law enforcement action to be taken when encountering an individual on the watch list. This information is conveyed through a "handling code," which provides insight into the level of threat posed by that individual. Generally, handling codes are expressed on a scale of 1 through 4. These handling codes are described in the following exhibit.

[40] More details on our review of the accuracy and completeness of the database are provided in Chapter 7 of this report.

FBI Handling Codes

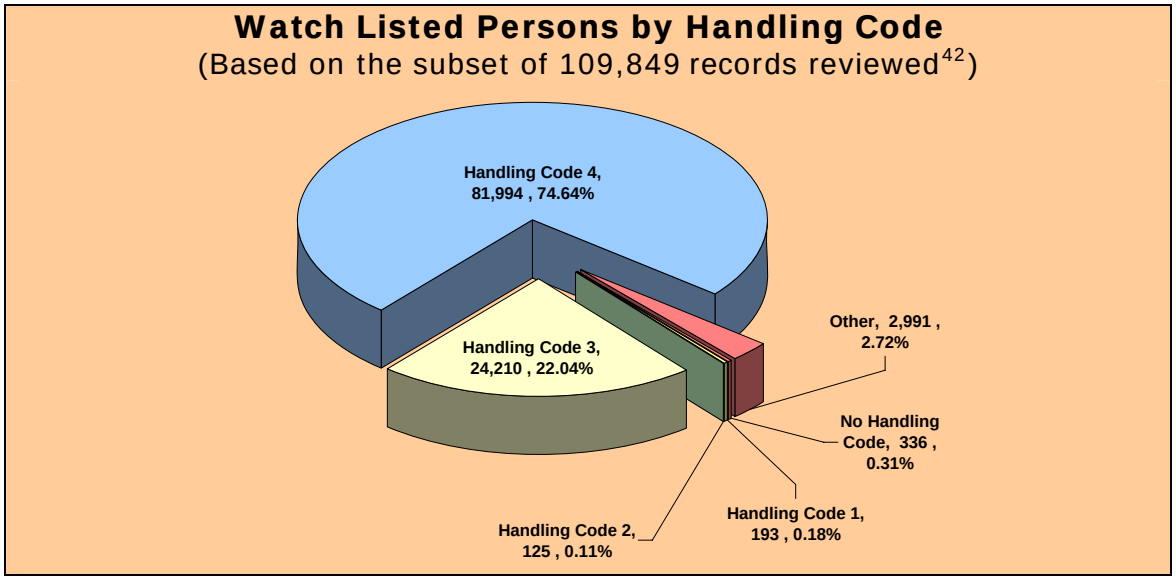
[SENSITIVE INFORMATION REDACTED]

Source: TSC Management

We reviewed a subset of the records in the TSDB 1B to gain an understanding of the characteristics of the individuals on the consolidated watch list. Our review of these records revealed that, as of October 7, 2004, the bulk of the records in the TSDB 1B were designated in handling codes 3 and 4.[41] Specifically, 22 percent of the individuals in our sample were categorized by the FBI as handling code 3. In addition, 75 percent of the

[41] Our sample consisted of the universe of records in the TSDB 1B that were identified for export to the VGTOF database as of October 7, 2004. This universe of 109,849 records represented 53 percent of the 207,553 total records in the TSDB 1B. We selected these records for review in consultation with TSC IT staff.

records in our sample had a handling code 4, the category requiring the lowest possible law enforcement response. Handling codes 1 and 2 were assigned to 193 and 125 records, respectively. Therefore, a total of only 318 records in our sample of 109,849 records were identified at the highest levels. The following chart provides a breakdown of handling codes applied to the subset of TSDB 1B records that we reviewed.



Source: TSC Management

As shown in the preceding chart, we also identified 336 records for which no handling code was assigned. This issue is related to the accuracy and completeness of individual records and is discussed in Chapter 7.

We asked the Director of the TSC about the types of individuals included in the TSC's consolidated watch list. She informed us that, to err on the side of caution, individuals with any degree of a terrorism nexus were included in the TSDB, as long as minimum criteria was met (at least part of the person's name was known plus one other identifying piece of information, such as date of birth). The Director further explained that one of the benefits of watch listing individuals who pose a lower threat was that their movement could be monitored through the screening process and this could provide useful intelligence information to investigators. In addition, she stated that watch listing lower-threat individuals that have associations with higher-threat level terrorists may lead to uncovering the location of higher watch listed individuals.

[42] The "Other" handling codes refer to one record that was transferred to the TSDB 1B from the TIPOFF database with the non-existent handling code 5. The TSC informed us that this record has been corrected. The remaining 2,990 records [SENSITIVE INFORMATION REDACTED].

Conclusion

At this early stage in the TSC's existence, the creation and operation of a single database housing consolidated terrorist information was the most important aspect of its mission. From the outset, TSC management was aware of the obstacles of fully integrating data from myriad, disparate sources as well as the necessity of blending multiple agency processes and data definitions. In response to these challenges, they focused on establishing the best possible database as quickly as possible.

TSC management recognized and we observed weaknesses in the TSC's efforts to accomplish this endeavor, including limitations related to name-search capabilities, availability of historical information, and the use of audit trails within the TSDB databases. However, the TSC successfully integrated different types of information in varying formats from the existing systems into a comprehensive index of watch listed individuals.

Despite providing a consolidated watch list in a compressed timeframe, we identified significant weaknesses related to IT management and planning. The TSC is working to improve its IT management and create a system that facilitates complete real-time connectivity to the end users and includes advanced name-search capability and searchable biometric data.

Recommendations

We recommend that the TSC:

1) Develop a formal IT plan for maturation of the IT environment at the TSC to address: a) IT staffing needs; b) controls to ensure data integrity; c) adequate oversight over IT contracts and contractors, and d) future improvements in the areas of TSDB connectivity, name-search capabilities, acceptance of biometric data, as well as other IT planning issues.

2) Enhance the TSDB to add audit trails to track activity within the database, including historical data and detailed transactions by user, as well as to include enhanced human access controls.

CHAPTER 6: TSC Operations

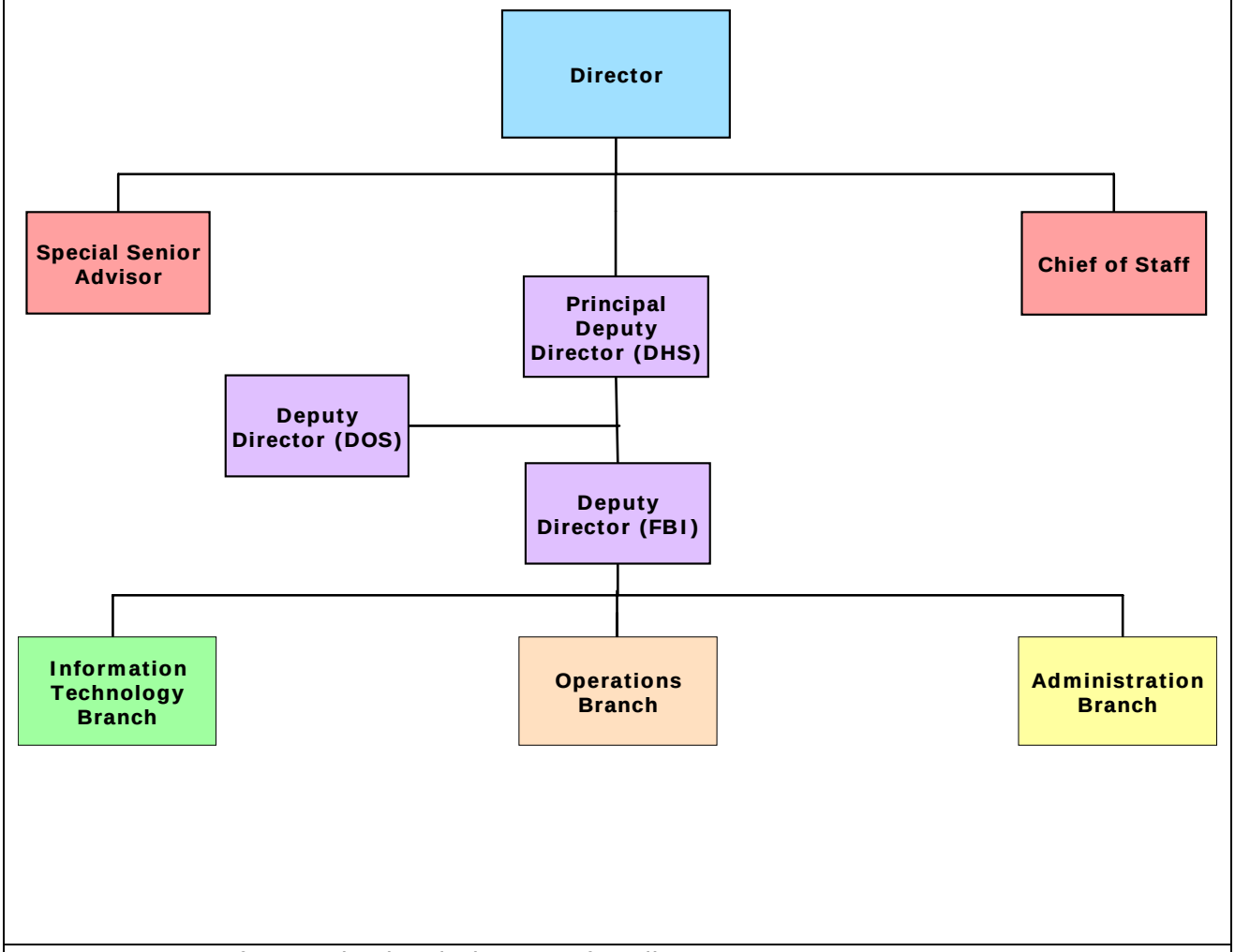
After accomplishing the initial objective of developing and implementing a consolidated watch list database, the TSC has moved into a new phase of its operations. The TSC has established an operating structure and new procedures for its call center. The physical size and activity of the TSC call center has experienced significant growth, and management has implemented procedures for nominating individuals for inclusion in the database, as well as for removing persons from the watch list. Further, the TSC has undertaken measures to increase information sharing and outreach. However, we identified areas in need of improvement; including weaknesses in staffing and the need for enhanced controls over the receipt, acceptance, and accuracy of incoming data.

Structure of the TSC

As of April 2005, the TSC was divided into three major branches: Information Technology, Operations, and Administration. The Information Technology (IT) Branch, headed by a Chief Information Officer (CIO) appointed in August 2004, oversees IT planning and systems architecture, including the design, maintenance, and modification of the TSDB that houses the consolidated watch list information. The Administration Branch handles personnel matters, security and guard services, budgetary issues, and logistics and physical space. The Operations Branch houses the TSC's 24-hour, 7-day a week call center and the Nominations Group, which is responsible for additions, deletions, and modifications to the consolidated watch list.[43] This Branch also handles inquiries, complaints, and comments from the law enforcement community. The Tactical Analysis Group, which is also part of the Operations Branch, performs analysis on encounters with potential terrorists to identify useable intelligence and forwards the information to the necessary parties as rapidly as possible. The general structure of the TSC is illustrated on the following organizational chart.

[43] The nomination process is discussed in further detail later in this chapter.

Terrorist Screening Center Organization

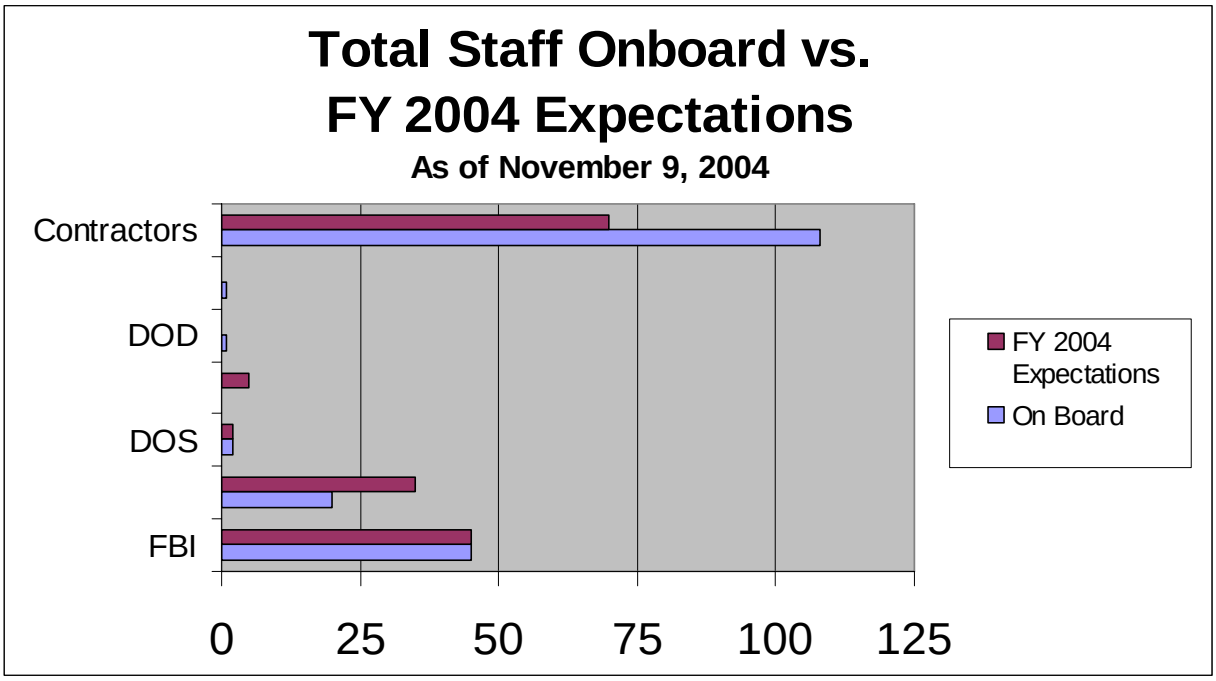


Source: TSC Draft Organizational Chart as of April 2005

Because the TSC is a multi-agency effort, personnel from the DOJ, the DOS, the DHS, the Department of Defense (DOD), and the United States Postal Service (USPS), along with various contractors staff all three branches. The September 2003 MOU executed in response to HSPD-6 required that the Principal Deputy of the TSC be a DHS employee. Neither the MOU nor any formal TSC protocols require other leadership roles, such as Branch or Unit management positions, to include representation from the various participating agencies.

Since its inception, the TSC Director has worked with the heads of the participating agencies to establish the TSC's staffing level and determine the number of detailees from each agency. For fiscal year (FY) 2004, the expected number of personnel at the TSC was 157. As of November 9, 2004,

a total of 177 staff were on board. The expectations are compared to the staff on board in the following exhibit.[44]



Source: TSC Administrative Unit

By the beginning of November 2004, DHS contributions fell 10 staff short of expectations. According to the TSC Director, she has repeatedly asked the DHS to provide additional employees, without success. To make up for the shortfall from the DHS, the TSC hired additional contractors, and as of November 9, 2004, more than half of the TSC personnel (108 of 177 total staff, or 61 percent) were contractors. The FBI is the next largest provider of TSC personnel, with about a quarter of the staff in the organization.

Participating agencies have also provided staff on a Temporary Duty (TDY) basis, with details of 60 to 90 days. In addition, these organizations loaned existing contractors to the TSC, some of whom have since become TSC-paid contractors. A total of 73 percent of the staff on board as of November 2004 were permanent TSC employees or contractors hired by the TSC. This staffing breakdown is displayed in the following table.

[44] We could not compare staffing numbers and expectations for different points in time because the TSC did not track the actual staffing levels. As a result, we compared available information, consisting of the FY 2004 expectations and the November 9, 2004, actual staffing levels. As of March 2005, the FY 2005 expectations had not been finalized.

TSC STAFFING INFORMATION
AS OF NOVEMBER 9, 2004

SOURCE	NUMBER TDY/LOAN	NUMBER PERMANENT TSC	TOTAL
FBI	21	24	45
DHS	13	7	20
DOD	1	0	1
DOS	1	1	2
USPS	0	1	1
Contract[45]	12	96	108
TOTAL	48	129	177

Source: TSC Administrative Unit

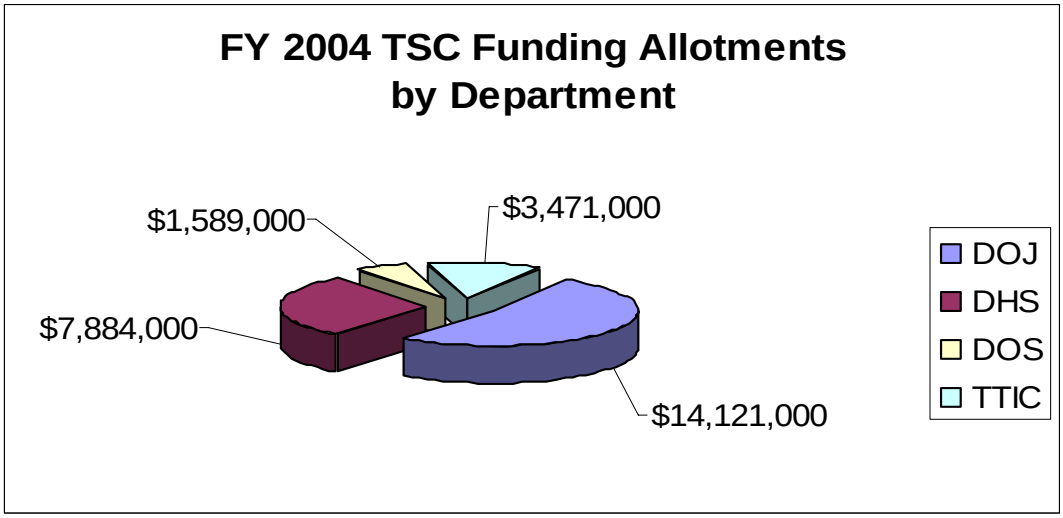
The rotating nature of much of the TSC's staff and the large percentage of contract employees has impacted the TSC's development. For example, the TSC lacks historical knowledge of its own organization. Only one individual, a contractor that was originally on loan from the FBI but whose contract has since been assumed by the TSC, has been with the organization since its creation in September 2003. Only about five additional individuals currently on staff with the TSC were at the organization during its planning phase, including the Director and two of the Deputy Directors. In addition, short TDY periods force the TSC to continually train and orient new personnel.[46]

Funding of the TSC

The TSC was created outside the normal budget process. As a result, no government staff positions were granted to the TSC by the Office of Management and Budget (OMB), and funding for FY 2004 was derived from the Departments of Homeland Security, Justice, and State, as well as NCTC. The FY 2004 OMB allocations for each of these agencies are detailed in the following chart.

[45] The number of contract personnel in the column labeled "Number Permanent TSC" are contractors that are not on loan from other agencies, but instead are paid directly by the TSC.

[46] Further examples of the negative effect of the TDY environment are provided in Chapter 8, Management of the TSC Call Center.



Source: FBI Budget Formulation Office and the TSC Administrative Unit

According to the OMB allocations, the TSC's FY 2004 budget was set at about $27 million. As of September 30, 2004, participating agencies had contributed a total of $27.5 million to the TSC. While the DHS and DOS both contributed the full amount specified by the OMB, NCTC's contribution of $3 million was $471,000 short of its FY 2004 allocation. The FBI provided $15 million to the TSC in FY 2004, almost twice as much as any other participating agency and $879,000 more than the OMB requirement. The following table distinguishes between the amount of funding allotted and the amount provided from each agency for FY 2004.

DEPARTMENT	DOJ/FBI	DHS	DOS	NCTC	TOTAL
Alloted	$14,121,000	$7,884,000	$1,589,000	$3,471,000	$27,065,000
Provided	$15,000,000	$7,884,000	$1,589,000	$3,000,000	$27,473,000

Source: TSC Administrative Unit

According to TSC management, the FY 2004 funding figures were based on conservative estimates of initial operating capability and did not represent a baseline estimate of future TSC needs. Further, the approved FY 2005 budget was $29 million and TSC officials assert that this amount is below normal operating requirements.[47] The TSC has estimated that the total resources required to accomplish the activities outlined in HSPD-6 and the resulting MOU amount to $50 million in funding and a staff size of 267. The TSC also analyzed the resources needed to meet the requirements of new initiatives that would affect the TSC's mission beginning in late FY 2005. According to this analysis, TSC officials believe that the organization will need an initial budget of $142 million and 455 personnel, with recurring costs of

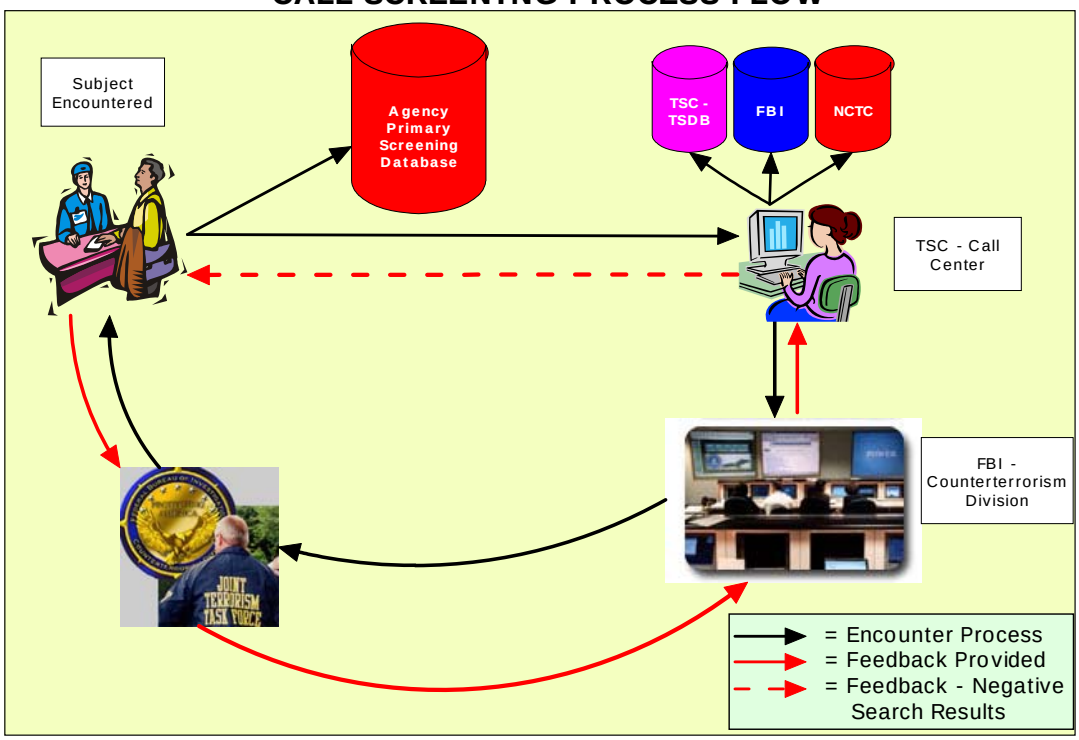
[47] The FY 2005 appropriation for the TSC was incorporated into the FBI's overall appropriation, thus eliminating the need to transfer funds between agencies.

$118 million each successive fiscal year. As of April 2005, Congress was considering an OMB-approved $40 million supplemental appropriation request for FY 2005.

The TSC Call Center

As noted in Chapter 4, on December 1, 2003, the TSC initiated operations in its call center, providing law enforcement agencies with around-the-clock access to consolidated information regarding known or suspected terrorists. The basic tasks performed by call center staff – namely fielding inquiries, researching terrorist information, and facilitating the identification and apprehension of terrorists – remains the same as the functions performed at the point of initial operating capability. However, the creation of the consolidated watch list has allowed TSC screening staff to begin all research with a single database – the TSDB. The general process flow of activity surrounding a possible hit against the TSDB is summarized in the following exhibit.

CALL SCREENING PROCESS FLOW



Source: The Terrorist Screening Center

The first step in the process when a person is encountered domestically or at the border is that the identity of an individual is searched in a law enforcement system such as NCIC or the Interagency Border Inspection System (IBIS). For example, an individual stopped by a police officer for speeding will be queried in NCIC, or an individual attempting to enter the United States at a border crossing is queried in IBIS. Although law

enforcement officials cannot connect directly to the TSDB, the TSC exports the consolidated watch list records to all supporting agency databases eligible to receive the information. If the queried identity appears to match a record in the TSDB, the law enforcement official receives a response to contact the TSC.[48] When the inquiry is received by the TSC, call center staff assist in determining if the encountered individual positively matches the identity of a known or suspected terrorist on the consolidated watch list. First, the screeners search the TSDB to obtain all basic identifying information available. Then, the screeners search supporting agency databases to locate any additional information that may assist in making an identification or provide further detail about the subject, some of which may be classified. For all calls received, the call screeners record details about the inquiry on a Call Intake Form. If the TSC call screener determines that the encountered individual does not match the identity of an individual on the watch list, the caller is immediately informed of the negative results.

If the subject is positively identified or the match attempt is inconclusive, the TSC call screener forwards the Call Intake Form, via facsimile, to the FBI's CT Watch. CT Watch is then responsible for coordinating the law enforcement response to the encounter, including making further attempts to establish positive identity and, if necessary, deploying agents to take appropriate action.

For every inquiry that TSC call screeners refer to CT Watch, the screeners are responsible for obtaining information on the disposition of the encounter, such as whether or not the subject was arrested, questioned, or denied entry into the United States. This information is recorded into an internal TSC database.[49]

In addition to domestic or border encounters, the TSC is involved when foreign individuals apply for a United States visa. According to State Department officials at the TSC, when a person overseas applies for a visa, U.S. government officials search the CLASS database, which receives watch list information from the TSC. If this search reveals a possible identity match with an individual recorded in the TSDB, the official will send the TSC a cable (a secure, electronic communication). A State Department representative at the TSC will review the cable along with information within supporting agency databases to determine if the person requesting a visa is

[48] This description of the process flow reflects the general process for call screening. There can be variances depending on the type of encounter, such as a border inquiry that would require the border patrol agent to first call the Department of Homeland Security's call center (the National Targeting Center), which in turn would contact the TSC.

[49] See Appendix III for detailed information on call center activity.

an individual with ties to terrorism. This information will be used by the U.S. government officials overseas to either issue or deny the visa application.[50]

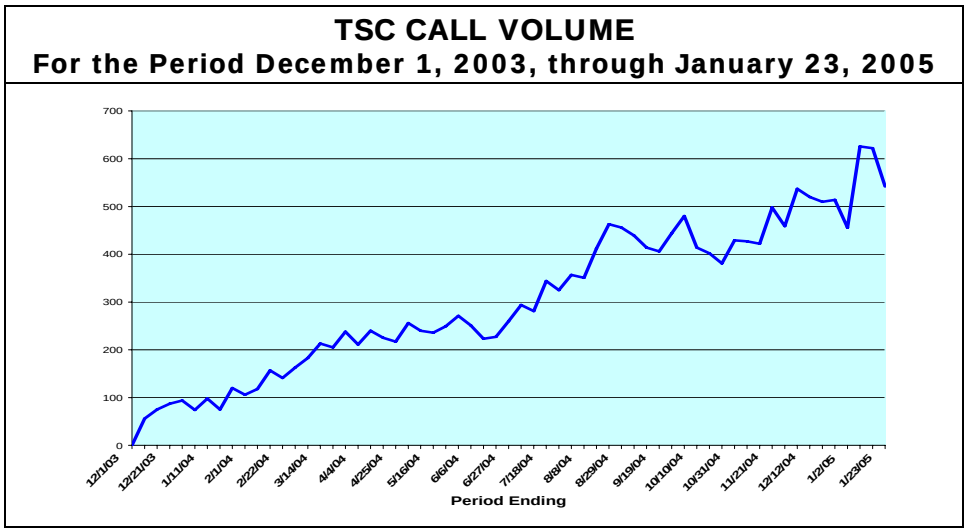
Expanding Use of the TSC

One way to illustrate the development and maturation of the TSC is to examine the increase in activity at its call center. The TSC generates weekly statistical reports detailing the total number of calls received, the origin (e.g., state or local law enforcement or border patrol), the result of the identity determination (i.e., positive, negative, or inconclusive match), the disposition (e.g., arrested or questioned and released). At times during our audit, the reported data contained small mathematical errors. While the reports are now mathematically correct, we believe the TSC should establish controls to ensure that its call data is checked regularly for accuracy.

Based on TSC weekly call reports, as of January 23, 2005, TSC call screeners had responded to 18,534 inquiries from federal, state, and local agencies regarding encounters with known or suspected terrorists. Of these inquiries, the TSC determined in 9,510 instances (51 percent) that the individual encountered was an individual of interest.

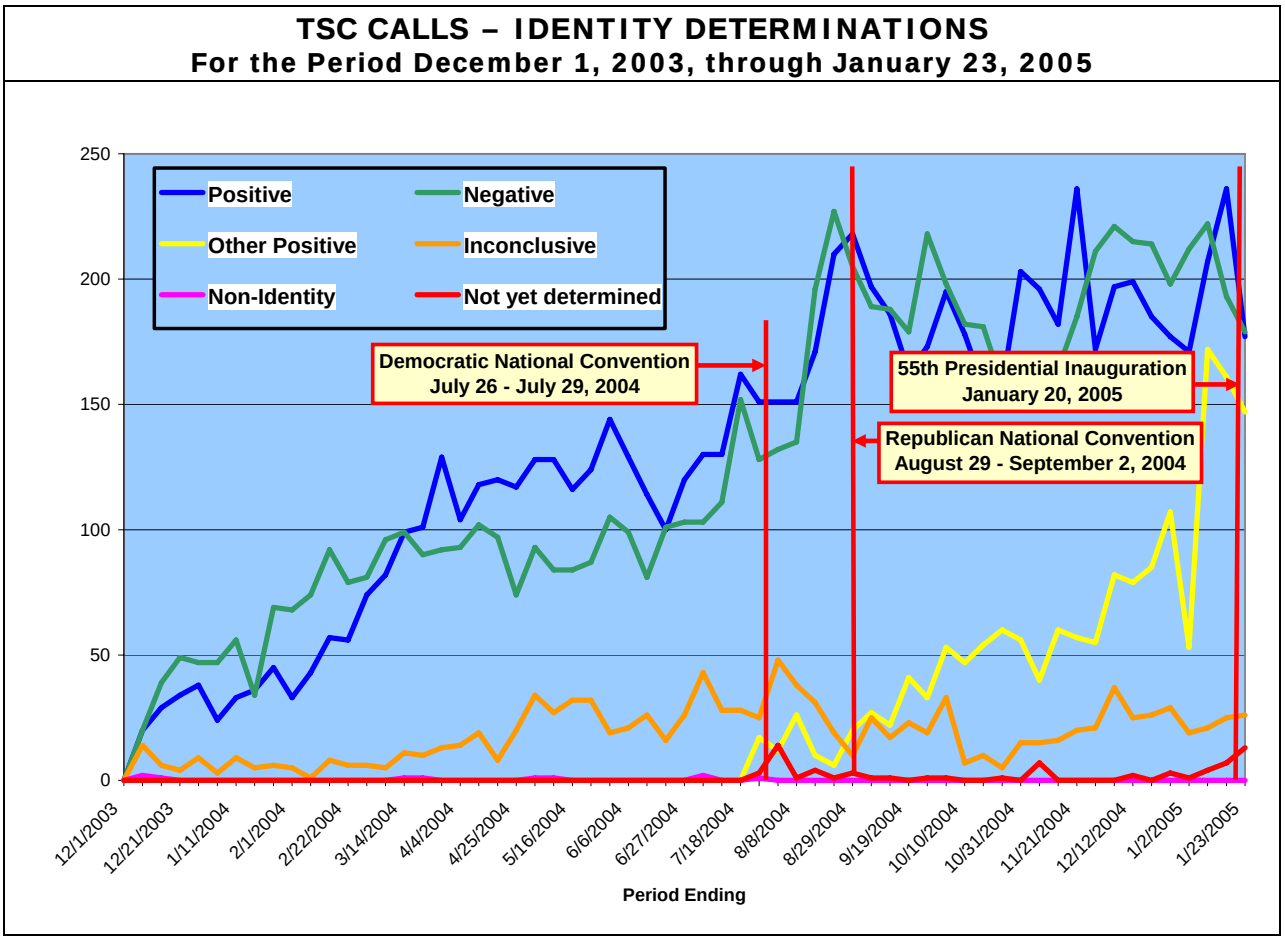
As shown in the following charts, at the start of its call center operations in December 2003, the TSC received approximately 8 to 11 calls per day. For the month of January 2005, the TSC's call volume had reached an average of 85 calls per day. The percentage of calls resulting in a positive identification match was 43 percent for the period of December 2003 through January 2005.

[50] The State Department's visa application review activities represent, in general, a process that existed prior to the creation of the TSC and continues to be conducted by DOS personnel. Our review of TSC activities focused on domestic and border processes and encounters.



Source: TSC Management

This 965 percent growth in call volume from December 2003 to January 2005 is attributable, in part, to the TSC's successful communication and outreach to the law enforcement and intelligence communities. This increase in call volume has been accompanied by an increase in actual positive identity matches. According to the TSC, this increase indicates that the quality and dissemination of information has improved. TSC staff is also aware that major events with national security implications, such as the presidential inauguration, stimulate an increase in call center activity. The breakdown of the identity determinations resulting from calls to the TSC call center is displayed in the following chart.



Source: TSC Management

Nomination Process

When a law enforcement or intelligence agency has identified an individual as a potential terrorist threat to the United States and wants the individual to be added to the consolidated watch list, that person must be "nominated" for inclusion in the TSDB.[51] Nominations occur in two ways – individuals may be added through the Routine Nomination Process, or they may be deemed an immediate threat that requires use of the Emergency/Expedited Nomination Process. The Routine Nomination Process, the most common of the two nomination methods, involves the submission of international or domestic terrorist-related names by government agents to either NCTC or the Terrorist Watch and Warning Unit (TWWU) at the FBI. Staff members review the information and decide whether or not the person is an appropriate candidate for inclusion on the TSC's watch list and whether

[51] The nomination process described here relates to the articulated process for maintaining the TSDB, which is done on a record-by-record basis. As noted in Chapter 5, the 1A and 1B databases were initially populated by accepting universes of records from source databases.

or not sufficient identifying information is available. If so, the information is forwarded to the TSC for inclusion in the consolidated database.

The Emergency Nomination Process is used when there is an imminent threat and a watch list record needs to be quickly created or highlighted. When an imminent threat exists, the requesting agency informs the TSC directly and TSC staff create a record in the TSDB and all supporting databases. If the threat contains a nexus to international terrorism, the TSC creates additional files of all the information gathered on the subject for submission to NCTC and subsequent creation of a record in the TIPOFF system.

At the time of our review, the TSC process for including a name in the TSDB was more of an acceptance than nomination. TSC staff did not review the majority of the records submitted unless an automated error occurred while the records were uploaded to the database. While we recognize that the ultimate decision for nomination into the consolidated database should be done by analysts who have access to originating documentation, the TSC needs to ensure that the information that is placed into the TSDB accurately represents the data that was submitted by the nominating agency. In addition, the TSC should establish controls to ensure that it can trace the origin of the record to the agency that nominated it. When comparing TSDB records to the source information, we identified differences for which the TSC could not provide an adequate explanation. Our testing of the accuracy and completeness of database records is contained in Chapter 7.

To gain a better understanding of the nomination process, we met with the Chief of the Nominations Unit in July 2004 and walked through the process of uploading the daily nominated records into the TSDB. As part of that process, we found that the TSC was using an unclassified, stand-alone system on which to conduct a "dirty word search," that is, a search that seeks to identify classified information within the file and presents it for deletion prior to uploading the file into the unclassified TSDB. This process presents a dilemma if classified information is found on the file because the presence of any classified information on what is supposed to be an unclassified system would result in security issues. Based on our identification of this weakness and subsequent discussions with the CIO, the TSC officially changed the designation of the stand-alone system from unclassified to classified in September 2004.

In addition, we initially found no formal back-up plan for receiving daily nominations and uploading these records into the TSDB. On at least one occasion, the two individuals responsible for performing the upload of records from NCTC and the FBI were both out of the office, and as a result no records were uploaded that day. This type of situation leaves the

database vulnerable to omissions and the screeners with potentially outdated and incomplete information. After we identified this problem, the TSC informed us that it had established a back-up plan under which the responsibilities will be shared by five employees. However, as of November 15, 2004, the TSC had not formalized this plan in writing. As mentioned previously, enhancing the database to automate the daily upload of records nominated for inclusion in the TSDB would avoid the need to rely on such human intervention.

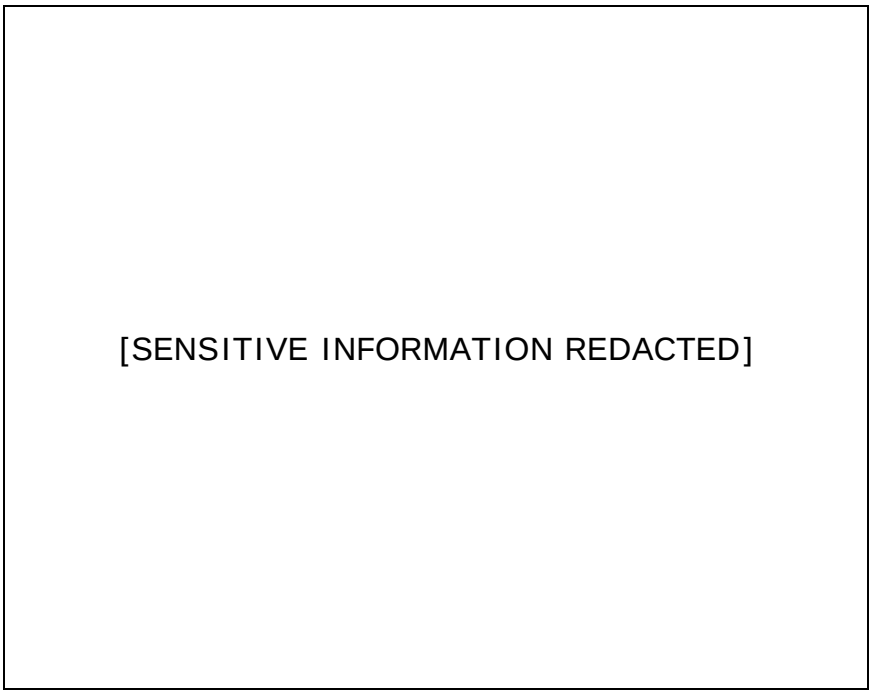
Removal of Names from the Watch Lists

The TSC removes names from the consolidated database and as of October 2004, 3,673 records had been removed from TSDB 1B since its creation in June 2004. Like the nomination process, there are two ways in which these removals are processed, referred to by the TSC as automatic removals and specific removals. Specific removals occur through quality assurance processes and as the result of misidentifications; these are discussed in further detail in Chapter 8. Automatic removals occur when the TSC receives an automated prompt from a supporting system of a participating agency, as described below.

When an international terrorist record is to be removed from the TSDB, the TSC will accept an electronic indicator to delete the record from the daily update file sent by NCTC.[52] When the TSC exports an update file from the TSDB to the participating agencies, the supporting systems that contained the subject record receive a deletion indicator as well, thereby removing the record from all supporting databases.

For example, as shown by the red arrow in the following screen print, the TSDB 1B main screen displays a box next to each database that receives exports of information from the TSC. On each record, these boxes are marked with a "Y" (yes) or "N" (no) depending on whether the database is approved to receive the record. If one of the boxes is left blank, the database defaults to "N." When a source agency such as NCTC deletes a record, it sends the record marked for deletion to the TSC where staff members delete the record from the TSDB. During the daily export of records to participating agencies, the TSDB sends the same type of deletion prompt to the agency databases marked "Y" for receipt of the particular record, thereby removing the record from all supporting databases.

[52] Because NCTC is not a component of the Department of Justice, we did not perform a detailed review of its procedures for removing names from the consolidated watch list.



Source: TSC Nominations Unit

Similar to its role in the nomination process, the TSC does not analyze these deletion requests and relies on the supporting agencies to conduct the necessary analysis that would lead to record deletion. As the owners of the data, the supporting agencies are responsible for making decisions regarding the appropriateness of an individual being watch listed.

When a domestic terrorist record needs to be removed from the TSC database, the appropriate FBI field office sends the TWWU a form that must be completed for any new submissions, provision of supplemental information, or removal requests on persons of a terrorist threat. When the form is received by the TWWU, it is reviewed for completeness and appropriate action. If complete, the form is forwarded to the TSC for removal of the record from the TSDB and all supporting systems.

Foreign Government Information Sharing

Another important aspect of the TSC's operations is the sharing of appropriate information with foreign governments. According to the September 16, 2003, MOU that was signed by the participating agencies to create the TSC and outline its core requirements, the parties were required, to the extent permitted by law, to provide appropriate information about suspected terrorists to foreign governments that cooperate with the United States. [SENSITIVE INFORMATION REDACTED]

Outreach to Additional Departments/Agencies

The TSC represents a new approach to information sharing and coordination among law enforcement, the intelligence community, and international agencies by offering one central point where all known terrorist-related information can be reviewed against the information of an encountered individual. To enhance the effectiveness of the government's efforts for terrorist screening, the TSC communicates with law enforcement agencies in many ways, including: 1) informing law enforcement personnel of the mission, role, and functions of the TSC; 2) educating law enforcement personnel on techniques for handling encountered individuals; and 3) promoting awareness that front-line law enforcement officers often have opportunities for gathering information that may be useful in on-going cases.

The TSC has established an outreach program that targets federal departments and agencies, informing them of the TSC's mission and determining what agency-specific opportunities exist for screening appropriate individuals against the TSC's consolidated watch list. In addition, TSC officials have attended numerous Chiefs of Police conferences and intelligence community gatherings, established booths at the federal law enforcement training center in Quantico, Virginia, and made presentations about its operations to state and local law enforcement agencies. TSC officials informed us that, from December 1, 2003, through June 30, 2004, they briefed approximately 2,000 people in 11 states and the District of Columbia on the efforts and usefulness of the TSC.

TSC officials said they also are working to identify specific organizations and industries that need to be informed of the TSC's role and functions. Officials also said that they have established a plan that includes creation of a website to provide basic information about the agency and the purpose of the consolidated database. Yet, based on our review of the TSC's outreach program, we believe the TSC should develop a more vigorous plan to target and prioritize specific organizations and industries, and establish a timeline to complete these outreach goals. We also believe that any outreach plan should be incorporated into the TSC's strategic plan, once the strategic plan is formally developed.

Private-Sector Information Sharing

According to HPSD-6, the DHS was charged with developing guidelines "to govern the use of such information to support state, local, territorial, and tribal screening processes, and private sector screening processes that have a substantial bearing on homeland security." The TSC has developed procedures for supporting state, local, territorial, and tribal screening

processes using the data contained within the TSC. However, as of October 2004, the DHS had not developed guidelines for private-sector screening or sharing of information.

In a drafted report to Congress dated October 2004, the TSC indicated that regular private-sector screening is anticipated in the future because DHS was finalizing a plan to screen individuals at certain private high-risk infrastructure facilities, such as hazardous material drivers.[53] DHS personnel assigned to the TSC are expected to perform the private-sector screening, but they will not be permitted to directly release identifying information to private organizations. However, as of October 29, 2004, DHS officials had not developed a formal plan for how this would be accomplished.

Conclusion

As a developing organization, the TSC has spent significant time establishing and implementing basic operating procedures. However, as exhibited by the activity in the TSC call center, the use of the TSC and its resources is expanding and management must take action to improve processes in certain areas. For example, the TSC needs to create formal plans for automating the daily upload of records to the TSDB and for implementing the DHS's system for private-sector screening. In addition, the TSC should address staffing issues, including the heavy reliance on contractors and short-term temporary staff.

Recommendations

We recommend that the TSC:

3) Develop staffing protocols to ensure that the TSC remains a multi-agency operation and make further efforts to encourage DHS to provide additional staff.

4) Take steps to increase the number of permanent government personnel and long-term TDY staff employed by the TSC to take advantage of valuable expertise and institutional knowledge and to reduce the necessity of constant orientation and training.

[53] *Terrorist Screening Center: Draft Report to Congress, Pursuant to the Intelligence Authorization Act for Fiscal Year 2004, Section 360* (October 29, 2004). For example, in preparation for the July 2004 Democratic National Convention, the TSC received the names of 18 hazardous material drivers from the Transportation Security Administration for screening.

5) Ensure that the information placed into the TSDB accurately represents the data that was submitted by the nominating agency. In addition, the TSC should establish controls to ensure that it can trace the origin of the record to the nominating agency.

6) Take measures to automate the daily upload of records nominated for inclusion in the TSDB to reduce the need for human intervention.

7) Develop a more vigorous outreach plan that includes specific target organizations and industries, and establish timelines for the completion of outreach goals. Incorporate the plan into the TSC strategic plan, when formally created.

8) Encourage the DHS to finalize guidelines to allow the TSC to begin regular screening for private sector organizations.

CHAPTER 7: Database Accuracy and Completeness

The TSC has successfully created a consolidated database of unclassified watch list information from supporting agency systems. However, the accuracy and completeness of the information contained in the database is as critical as the consolidation effort itself. There is little room for error because a single name omitted from the TSDB could result in a suspected terrorist successfully applying for a visa, being admitted to the United States, or failing to be identified when stopped for a traffic violation.

One of the TSC's primary goals under HSPD-6 was to maintain thorough, accurate, and current information. Although the TSC does not create terrorist-related information, it is responsible for ensuring that all necessary terrorist-related information maintained by NCTC and the FBI is transferred to the TSC and accurately maintained in its consolidated database.

Our review of the accuracy and completeness of the terrorist watch list was divided 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, the fields of information available for screeners to view on the TSDB 1A and 1B screens, and the population of those fields within the databases. We also reviewed the descriptive categories and handling instructions that are applied to each record within the database. Second, we tested individual records within the database for accuracy and completeness. This included reviewing a sample of FBI and NCTC records from the respective agency databases (i.e., VGTOF and TIPOFF) and tracing them forward to the TSDB 1A and 1B to determine if complete and accurate information was carried forward into the TSDBs. Additionally, we reviewed a sample of the forms FBI agents use to nominate individuals for inclusion in the consolidated database, and traced those forms to the TSDB to determine if the individuals were, in fact, included in the database and that the information was accurate. We also checked known terrorist names against the TSDB 1A and 1B to determine whether those individuals were in the database.[54]

Overall Review of the Consolidated Databases

We first reviewed the TSDB 1A and 1B to gain an overall understanding of its contents. This included reviewing the number of records that each database maintained and the structure for each record. In

[54] Where possible, we reviewed both the TSDB 1A and TSDB 1B because, at the time of our testing, both databases were in use at the TSC.

addition, we analyzed the types of categories and handling instructions assigned to individual terrorist records. Our review found several problems, including inconsistent record counts, duplicate records within the consolidated database, limited identifying information shown to screeners on the TSDB 1A and 1B screens, lack of needed fields within the TSDB, and weaknesses related to the instructions for handling encountered individuals as well as the descriptive information related to the type of threat posed by subjects in the database.

Database Record Counts

On October 22, 2004, NCTC officials estimated that there were approximately 170,000 unique individuals who were known to the U.S. government as known or suspected terrorists or as having ties to terrorism. As of January 2005, the TSDB 1A and 1B included a total of 455,002 and 237,615 active records, respectively. Both databases include unique individuals and aliases. Since both databases were maintained and updated simultaneously, theoretically both should have had the same number of records. However, as indicated above, we found a difference of 217,387 records between the two databases in January 2005.

According to TSC officials, this disparity resulted from the immediate need during the earliest days of the TSC to develop a comprehensive database (TSDB 1A) of potentially high-risk suspects. Accepting records directly from numerous databases resulted in duplicate records being imported into the TSDB 1A. Further, TSC officials said the complex task of consolidating large and often incompatible data systems required accepting less than optimal data. For example, in creating the TSDB 1A, the TSC imported records directly from the Treasury Enforcement Communications System (TECS), thereby receiving records that were unique to TECS and were not included in its sub-systems – the Interagency Border Inspection System (IBIS) or the National Automated Immigration Lookout System (NAILS). These unique TECS records were not included in the 1B database because, according to TSC staff, they had not been provided to NCTC and there was significant concern about the quality of the records.

TSC officials informed us in early March 2005 that they had successfully addressed the significant difference in record counts between the TSDB 1A and 1B. They reported that they reduced the difference to about 40,200 records existing in TSDB 1A but not in TSDB 1B. This group of records has undergone initial review and the TSC stated that it consists of 39,000 records awaiting additional vetting by NCTC and 1,200 that will require manual correction at the TSC.

Duplicate Records

The use of unique identifying numbers in a database is an important internal control for minimizing duplicate records. According to TSC officials, both the TSDB 1A and 1B assigned unique identifying numbers for every record added to the databases. Likewise, TIPOFF records, including all aliases, each have a separate unique identifier.

However, the VGTOF database assigns a distinct record number to each *individual* in the database, and known aliases or varying identifying information for the individual are recorded within the original record. When included in the TSDB, a new record is created for every combination of identifying information contained on a VGTOF record. For example, two dates of birth listed on one VGTOF record for an individual would be included in the TSDB as two records – one for each date of birth. As a result, both of these records in the TSDB will show the same VGTOF number, while each will have a unique TSDB record number.

The TSDB should not contain multiple records with the same TIPOFF or TSDB record number; however, it is possible to have multiple records with the same VGTOF number. Further, each record within the TSDB should represent a *unique combination* of identifying information for an individual. For example, an individual who [SENSITIVE INFORMATION REDACTED] would have two records, each with the same [SENSITIVE INFORMATION REDACTED]; however, the [SENSITIVE INFORMATION REDACTED] would be different. The TSDB should not contain multiple records with completely identical identifying information. In addition, because aliases refer to the same individual, the databases to which an individual's record should be exported (e.g., CLASS, IBIS, VGTOF) and the instructions regarding how the individual is to be handled should be the same.

Duplicate records within the TSDB can cause a time-consuming and possibly confusing experience for screeners when researching a specific individual. The call screener can mistakenly rely on one record while a second, more complete record may be ignored. This can result in important information being missed. Also, if update information is transferred for a record in the TSDB 1B that has duplicate entries, then one of the duplicate records may be updated while the other may not. This situation would result in two identical record numbers containing different information.

We attempted to determine whether duplicate records existed within the TSDB 1B.[55] Although we did not identify duplicate TSDB 1B numbers, we did find duplicate records. We found 31 records that had duplicate information in five core identifying fields [SENSITIVE INFORMATION REDACTED]. Of these, 15 records also had duplicate TIPOFF record numbers.

Our review of the duplicate records revealed that six contained different information describing the individuals' association with terrorism. For example, for one set of duplicates one record reflected that the person was "Likely to Engage in Terrorism if Enters in U.S." while the other record reflected that the same individual "Provides Support, Safehouse, Weapons, Funds, ID, etc." An additional 16 records had either conflicting or missing handling instructions. These descriptions and instructions are used by the front-line law enforcement officers to assess and determine the level of threat posed by the individual encountered and help to protect the safety of these officers. Therefore, it is essential that this information be accurate and consistently applied to all records related to one individual.

In addition to the 31 duplicate records, we found 4 records for which the "unique" TIPOFF record number was duplicated, but for which the 5 core fields were not all the same. The TSC could not explain how this occurred.

In our review of the duplicate records, we also identified instances where instructions for which database a record was to be included were omitted, conflicted, or not applied. For example, on multiple occasions records nominated for inclusion on the TSA No-Fly list were not forwarded to that list. However, associated records (such as aliases) that similarly were nominated for the No-Fly list were, in fact, included on the list.

Overall, the TSC could not explain why duplicate records existed in the TSDB 1B. Based upon our observations and analyses, one probable cause for some of the duplicative information was the transfer of the FBI's data on international terrorist records from the VGTOF to NCTC. At the time the TSC established the consolidated database, NCTC was not receiving international terrorist records from the FBI because the agencies had not yet come to agreement on the terms of information sharing. As a result, to implement and maintain the most accurate and comprehensive database of terrorist

[55] We did not perform similar tests for duplication in the TSDB 1A. TSC officials explained that the TSDB 1A was developed by a contractor using proprietary software and the contract had ended by the time of our field work. No one at the TSC had knowledge of the database structure in order to perform our requested queries and significant time would have been required from contractors engaged in other major TSC developments to learn the database structure.

information, TSC officials decided to include international terrorist information directly from the FBI. When the FBI later transferred its international terrorist records to NCTC, the volume of data, coupled with the excessive manpower required to review each record, precluded NCTC from reviewing each record to ensure that it did not forward any duplicate or outdated records to the TSC. TSC officials indicated that they plan to address this issue by manually reviewing and deleting any duplicate records that have been created as a result of this process and updating any outdated information. We believe that the TSC should regularly perform queries of its consolidated watch list database to ensure duplicate records are not being created.

Records with Unidentifiable Sources

Although we had been informed that the TSDB 1B was created with information solely from the FBI and NCTC, we found five records in the database that were not derived from the NCTC or FBI databases. IT contractors at the TSC could not explain why these records were included in the 1B database if they did not come from either of the primary source systems. This is significant because the TSDB is an index of summary information owned by other agencies, and it must be able to identify the source of records in order to obtain necessary supporting information and appropriately assist law enforcement. TSC managers said they would look into this matter, but as of March 2005 had not provided an explanation for this situation.

Descriptive Categories

For each of the international terrorist names included in the two TSC databases, an Immigration and Nationality Act (INA) code is assigned by NCTC that provides a description of how a specific individual is associated with international terrorism. There are 25 different INA codes that can be assigned to each international terrorist record in TIPOFF, but the system includes controls to ensure that only one INA code is assigned; 8 of the codes indicate that the individual should be considered armed and dangerous. This data is subsequently transferred to the TSC for inclusion in the consolidated databases. The following table displays the distribution of records in the TSDB 1B according to the INA code.

Watch List Distribution by INA Code

[SENSITIVE INFORMATION REDACTED]

Source: TSC IT Branch, subset of TSDB 1B records as of October 7, 2004

In reviewing the descriptions of the 25 INA codes, we found that they do not appear to be mutually exclusive and that a suspected terrorist may fit more than one category. The TSDB does not allow for more than one INA code to be applied to each record. Consequently, this restriction may limit the amount of descriptive information available on particular records in the consolidated database.

Records originating from the FBI do not contain INA codes because the categories were developed for the purpose of assigning an identifier to aliens. In an effort to make TSDB record structures consistent for both foreign and domestic records, the TSC directed the FBI to assign one of three possible codes to the data it sent to the TSC. The FBI developed a program that automatically assigns one of the three INA codes to a domestic terrorist record based on the existing handling instructions. This automated process occurs every time new domestic terrorist records are transferred to the TSC. The Director of the TSC explained that the purpose of assigning an

INA code to domestic terrorist records entered into the TSDB 1B was to have a single standardized method for identifying the type of terrorist threat presented by each subject in the database.

In our opinion, the three codes currently being used do not provide an adequate description of domestic terrorist activities. We recognize the TSC's objective of standardizing the use of descriptive codes, but using descriptions more applicable to international terrorist activities to describe domestic terrorist activities diminishes the usefulness of the coding system. Instead, we believe that specific descriptions of domestic terrorist activities should be developed and applied to domestic terrorist records.

Handling Instructions

As noted previously, one of the benefits from the TSC's efforts to develop the TSDB is that the sharing and consolidation of all available watch list information puts law enforcement personnel in a better position to take appropriate action when individuals are identified. The TSC has attempted to provide law enforcement personnel with the necessary handling instructions for individuals whose names appear in the consolidated database. According to TSC officials, all records in the consolidated watch list database should have a handling code assigned.[56] FBI agents nominating a record for inclusion in the VGTOF and other databases assign a handling code based on the information available about the individual, including whether a valid arrest warrant exists or if the person is considered armed and dangerous. For international terrorist records received from NCTC, the TSC assigns a handling code based on the designated INA code, the extent of identifying data available, and any other information that may be related to how the individual should be treated.

Missing Handling Codes

Based on our review, we found that 336 records in a subset of 109,849 did not have a handling code assigned.[57] Of these records, at least 160 of the individuals were described as armed and dangerous, according to the designated INA codes. It is important that the appropriate handling code be assigned to each record so that law enforcement officers are adequately protected.

[56] Handling codes were discussed and defined previously on page 29 of this report.

[57] We did not perform similar tests of the TSDB 1A for the same reasons explained in footnote number 55.

INA Codes vs. Handling Codes

For records in the TSDB 1B, we compared the INA codes to the handling instructions in the database to determine if the two corresponded. In our small sample of VGTOF records, we found several instances where records had handling instructions that did not correspond to the level of threat indicated by the descriptive category. For example, we identified at least 19 instances where records were categorized with INA codes designated as "armed and dangerous" but the records had handling instructions that were applicable for individuals requiring the lowest level of law enforcement response.[58] In addition, we found 12 instances where INA code 5, a designation applied to group members not considered to be armed and dangerous, was applied to handling codes 1 and 2, which require the highest level of safety precautions due to the more significant threat the subjects may present.

We found that the INA codes were misapplied because of a problem with the FBI's programming language used to transfer records from VGTOF to TSDB 1B. For each VGTOF record sent to the TSC for inclusion in the TSDB, the TSC requested that the FBI assign an INA code based on the previously assigned handling code. The TSC's protocol for assigning handling codes to records with pre-existing INA codes stated that if a subject was issued a non-armed and dangerous INA code, then a handling code 4 was to be applied, which is representative of the lowest level of law enforcement response. According to FBI officials, the opposite message was communicated for assigning INA codes to records with pre-existing handling codes. FBI officials stated that they were told to apply an armed and dangerous INA code to records designated handling code 4 and a non-armed and dangerous INA code as a default to all other handling codes. When notified of our concerns, the TSC Quality Assurance staff acknowledged that the wrong INA codes had been applied to the VGTOF records, and the Director of the TSC informed us that she would look into this matter.

The results of this test led us to perform a search on the entire 1B database to determine the general consistency between INA and handling codes. We found at least 31,954 records with INA codes that were categorized as "armed and dangerous" but had handling codes conveying instructions applicable for individuals at the lowest level, which does not require the encountering law enforcement officer to contact the TSC or any other agency. As shown in the following table, the INA codes for some of these records described these individuals as: 1) having engaged in terrorism; 2) likely to engage in terrorism if they enter the United States; 3) hijacker; 4) hostage taker; 5) [SENSITIVE INFORMATION REDACTED]; and 6) user of explosives or firearms.

[58] These 19 records were assigned INA code 7, "Likely to Engage in Terrorism if Enters U.S.," considered to be an armed and dangerous category, but were assigned handling code 4.

HANDLING CODE DISTRIBUTION (Records eligible for export from TSDB 1B to VGTOF as of October 7, 2004)
[SENSITIVE INFORMATION REDACTED]

Source: TSC Information Technology Staff

At the time of our field work, TSC officials could not explain this apparent mismatch, but informed us that they would look into this matter. This situation, which represents a weakness in the database and places front-line law enforcement officers in a vulnerable position, should be addressed as quickly as possible.

Database Record Fields

During our review, we found that records in the TSDB 1A contained different identifying fields than records in the TSDB 1B. The following table compares the available fields for a given record in each database.

SAMPLE OF RECORD FIELDS AVAILABLE IN BOTH THE TSDB 1A AND THE TSDB 1B

[SENSITIVE INFORMATION REDACTED

Source: TSC Management

TSC officials explained that they are working to increase the available fields in the 1B database. As discussed in Chapter 5, TSDB 1B was programmed to include additional information fields, such as specific biographical data, but these fields have not yet been enabled.

In addition, during our testing of the TSDB 1A database, we found that for domestic terrorist records, certain fields of information were all consistently omitted from the screen display even though this data was maintained in the database. Therefore, although the TSDB 1A was capable of displaying eight possible fields of information, as few as three were often displayed. This left the screeners with limited data to make initial determinations of potential matches. TSC IT personnel were previously unaware of the limited screen information and said that the screen interface was not programmed correctly to display all of the information to screeners. The TSC's failure to recognize this shortcoming is another example of the weaknesses in IT management, which were discussed in Chapter 5.

Lack of Needed Fields

In our review of the TSDB 1B, we found that there were no separate fields specifically designated to identify [SENSITIVE INFORMATION REDACTED]. This type of information is important when attempting to verify the identity of an individual. Currently, the [SENSITIVE INFORMATION REDACTED] field in the 1B database is closely related to the [SENSITIVE INFORMATION REDACTED] field. [SENSITIVE INFORMATION REDACTED] We found this use of the [SENSITIVE INFORMATION REDACTED] field for recording the [SENSITIVE INFORMATION REDACTED] of an individual to be inconsistent with the title of the field. The fact that one database field can reflect two very different sets of information makes the field vulnerable to errors. In addition, the information is subject to misinterpretation by screeners who are using the information in the data fields to identify potential terrorists. We believe that this dual usage of the [SENSITIVE INFORMATION REDACTED] field should be corrected with separate fields that specifically identify the [SENSITIVE INFORMATION REDACTED].

Testing of Individual Database Records

We reviewed the information contained in the TSDB 1A and 1B to determine whether the databases were complete, accurate, and properly consolidated. Using formulated queries, names of known or suspected terrorists, and judgmental samples pulled from the two primary supporting databases, we assessed the completeness and accuracy of the information contained within the consolidated database, the timeliness of the information consolidated, and other issues related to the database.

To perform our tests of TSDB 1A and 1B records, we selected judgmental samples from the TIPOFF and VGTOF databases and traced them forward to the consolidated database, verifying whether the unclassified information contained in the source records was accurately transferred to

and displayed in the TSDB 1A and 1B. We also performed testing on nominated additions, modifications, and deletions from the FBI to determine the timeliness of the resultant actions and to assess the completeness and accuracy of the changes made. Further, we searched selected known or suspected terrorist names in the TSDB to ensure they were included in the consolidated database. The results of our findings are discussed below.

VGTOF Trace to the TSDB

To verify the completeness and accuracy of VGTOF records maintained within the TSDB 1A and 1B, we judgmentally selected a sample of 59 records (for 58 individuals) from a universe of 104,116 VGTOF records as of August 2004. Our sample of records was traced forward to the 1A and 1B databases to ensure that each record was included in the consolidated database and that all pertinent, unclassified information intended for inclusion in the TSDB was present. Our analysis found all 59 records contained in the TSDB 1A. However, eight of these records, all for different individuals, were missing from the TSDB 1B. In addition, 5 records in our sample of 59 contained inaccuracies in record content between the information contained within the VGTOF database and information in the TSDB 1B. The omissions and inaccuracies of these records resulted from problems in a number of different areas and are explained in detail in the following sections.

VGTOF File Not Sent to the TSC

On a daily basis, the TSC receives updated files from VGTOF for inclusion in the TSDB 1B. During our testing of the 59 sample records, we identified 2 VGTOF records that were not included in the 1B database. We contacted the FBI's Criminal Justice Information Services (CJIS) Division, who informed us that these records existed on a June 11, 2004, update file that ultimately was never sent to the TSC.[59] CJIS officials said this resulted from a lack of back-up coverage when the individual normally responsible for sending the update file to the TSC was out of the office. Upon closer examination of the update file that was not sent to the TSC, we found that the file contained 12 new records (representing 6 separate persons, 2 of whom were in the records we identified as missing from the database) and 8 modifications to existing records (representing the records of 4 separate persons).

[59] Before August 9, 2004, CJIS was responsible for managing the VGTOF file and for sending the daily update files to the TSC. On August 9, 2004, the TSC became responsible for managing the VGTOF file.

Technological Difficulties with NCTC

As previously discussed, HSPD-6 directed that all terrorist information in the possession of the U.S. government, with the exception of purely domestic terrorist information, must be provided by federal departments and agencies to NCTC for inclusion into its database. The MOU resulting from HSPD-6 called for NCTC to serve as the primary data source for the TSC's consolidated database, with the exception of purely domestic terrorist information that would be provided by the FBI. As a result, NCTC took control of the State Department's TIPOFF database in November 2003 to serve as the central repository for all international terrorist information. However, because the FBI possessed international records prior to the establishment of NCTC, it was necessary for NCTC to obtain this data from the FBI. This data, originally housed in the FBI's VGTOF database, was sent electronically to NCTC for inclusion in the TIPOFF database. The records subsequently would be sent electronically to the TSC for inclusion in the TSDB.

The NCTC experienced a number of technical difficulties in uploading the VGTOF data file into TIPOFF. As a result, the information was delayed from inclusion in the TSDB 1B for approximately one month. We identified a total of 6 records from our sample of 59 that were not included in the TSDB 1B for this reason. A second search for these records a month later found that all but one of the records had been added to the database. One record remained unaccounted for, and the TSC could provide no explanation as to why this record was missing from its database. When we questioned TSC officials about NCTC's difficulties, they expressed little knowledge of the problem. As a receiver of such vital information, the TSC needs to establish procedures to identify potential barriers to the timely receipt of these important terrorist records. We estimate that the NCTC uploading difficulties may have affected a total of 20,000 records, a significant number of records for which the TSC does not have a suitable level of assurance.[60]

Missing or Conflicting VGTOF Data

Our analysis further revealed that important and relevant information within the 59 sampled VGTOF records was not always included on records in the TSDB. In other instances, the information was incorrect. Specifically, VGTOF contains a miscellaneous text field that, while not searchable because of its format, often provides important identifying information that could be

[60] Approximately 20,000 international terrorism records in the VGTOF database were sent from the FBI to NCTC in August 2004 for inclusion in the TIPOFF database. The records then were to be forwarded to the TSC for inclusion in the TSDB in accordance with the MOU.

missed by the TSC or information that conflicts with the TSC record information. One VGTOF record within our sample contained information in the miscellaneous field indicating that the subject was not a U.S. person, while the TSC record indicated that the subject was a U.S. person. Conflicting information such as this can confuse screeners and possibly contribute to the misidentification of an innocent person, or the inappropriate release or admittance of a dangerous individual.

Two additional records within our sample included text in the miscellaneous field identifying the subjects as [SENSITIVE INFORMATION REDACTED]. However, the TSDB 1B records showed the individuals as U.S. persons with no additional information provided. TSC and CJIS officials also attributed this situation to the programming of the TSDB 1B database. As previously reported, the [SENSITIVE INFORMATION REDACTED] field in the TSDB 1B database is closely related to the [SENSITIVE INFORMATION REDACTED] field. The two sample records mentioned above did not contain a [SENSITIVE INFORMATION REDACTED], and therefore should have reflected the individuals as [SENSITIVE INFORMATION REDACTED].

Another sampled VGTOF record identified a [SENSITIVE INFORMATION REDACTED] in the miscellaneous column that was not reflected in the TSDB record. CJIS officials explained to us that [SENSITIVE INFORMATION REDACTED] were erroneously entered into the miscellaneous field instead of the [SENSITIVE INFORMATION REDACTED] field when FBI field agents entered the data directly into VGTOF. As a result, unless the TSC specifically searches the miscellaneous text field, any information that was incorrectly entered into the miscellaneous field will be missed. The TSC's assumption of responsibility for the VGTOF file records in August 2004 should reduce similar data entry errors because FBI field personnel no longer have the ability to directly enter information. However, the TSC will need to ensure that past data entry problems do not limit the amount or quality of data contained within the TSDB records.

One record within our sample of VGTOF records showed text in the miscellaneous field that stated the individual's reported biographical data may not be accurate. TSC screeners may miss such important information unless the TSC establishes procedures to require review of the miscellaneous text field of each VGTOF record in order to identify such potentially useful information.

TSC-Identified VGTOF Errors

We were informed during initial interviews with the TSC Chief of Operations that, upon establishment of the TSC call center, the VGTOF data

was tested for accuracy and was found to possess a 40 percent error rate based on a sample of 20 records. Errors were said to exist mainly in the handling codes, and we were told that NCIC was responsible for fixing the problem. At the time, the VGTOF database contained approximately 15,000 names. While we did not perform this test, we considered this information when we performed our own testing of the VGTOF database to assure that an accurate representation of the information contained in the database was reported. TSC's Chief of Operations at the time of our inquiry informed us that the FBI's Counterterrorism Division had been informed of the problem and the FBI issued an Electronic Communication directing its field offices to immediately "clean-up" the record information.

However, we learned later from the TSC Quality Assurance staff that no follow-up action had been taken by the TSC to ensure the VGTOF data had been corrected. In our opinion, the TSC needs to follow up to ensure that other FBI units have taken the necessary steps to correct erroneous information.

TIPOFF Trace to the TSDB

To determine the completeness and accuracy of TIPOFF records maintained within the TSDB 1A and 1B, we judgmentally selected a sample of 51 records (all separate individuals) from a universe of 185,628 TIPOFF records as of August 2004. Our sample was traced forward to the 1A and 1B databases to ensure that each record was included in the consolidated database and that all pertinent, unclassified information was present. From our analysis, we found that 2 of the 51 records were missing from the TSDB 1A. This appeared to result from record deletion, although as stated previously the 1A database does not maintain an audit trail of changes. In addition, 3 records from our sample of 51 were missing from the TSDB 1B. We also identified that 12 records in our sample contained inconsistent information when compared against the records in TSDB 1A and 1B. The omissions and inaccuracies of these records resulted from a variety of problems that are discussed in the following sections.

TIPOFF Records Missing from TSDB

Our review of the TIPOFF records traced to the consolidated database identified active records in TIPOFF that had been deleted from the TSDB 1B, as well as active TIPOFF records that had never been included in the 1B database. Because the entire contents of TSDB 1A were overwritten on a daily basis, no history was retained in the 1A database to determine if the records deleted from 1B had ever existed within 1A.

TIPOFF records sent to the TSC marked for deletion from the consolidated database often result when an individual no longer is considered a threat to the U.S. government. When a record is sent for deletion, the TSC nominations staff receives a prompt on the electronic NCTC file to delete the record. However, NCTC retains the original record in its system but deactivates the record by excluding it from the TSDB and other supporting systems. Our review of a sample of the TIPOFF records revealed two records that were not in the TSDB 1B but did reflect, through the historical information available, that the records had been included in the 1B database in the past. Each of these records was appropriately denoted as being exempt for inclusion in the TSDB.

Records missing from the TSDB that were active within the TIPOFF database and which had been marked for inclusion in the TSDB require further examination. We identified three such instances of active TIPOFF records that should have been included in the TSDB. In these three instances, the TSDB 1B did not contain a history of the records ever being included in the 1B database. Officials at the TSC informed us that they are unsure of the reason why these TIPOFF records were missing from the TSDB 1B.

To maintain a complete and accurate subset of all terrorism watch list related information, the TSDB must contain all records possessed by the U.S. government related to individuals who may pose any level of terrorist threat. A record not passed to the TSC for inclusion in the database and other supporting systems creates vulnerability should that individual be encountered and contributes to the incomplete status of the TSDB.

Missing or Conflicting TIPOFF Data

Our trace of the TIPOFF records within the TSDB revealed a number of discrepancies in the content of record data within the two databases. Again, we identified errors related to the [SENSITIVE INFORMATION REDACTED] field in the TSDB 1B database being closely related to the [SENSITIVE INFORMATION REDACTED] field. For one record in our sample, [SENSITIVE INFORMATION REDACTED]. However, upon our review of this record in the TSDB 1B database, we identified that [SENSITIVE INFORMATION REDACTED].

We also identified two instances where a TSDB 1A and/or 1B record did not accurately reflect important identifying information contained in the source TIPOFF record. Specifically, one TIPOFF record in our sample showed the particular individual as a male with no listed date of birth who had an INA code 89, “Lost/Stolen Passports.” The related TSDB 1B record showed this individual as a female with a date of birth who had an INA code 5,

"Group Member." The TSDB 1A record for this individual showed the individual with the same date of birth and a description of "FTO Member," short for Foreign Terrorist Organization Member.[61] The second instance mentioned showed a TIPOFF record with an INA code 2, "Any Other Unlawful Activity," while the related TSDB 1B record was applied an INA code 89, "Lost/Stolen Passport." No warning was shown in the 1A database for this record.

Additionally, we found nine instances where no warning was reflected on the TSDB 1A screen for TIPOFF records within our sample. Of those instances, seven records had no handling code either.

Such a large database requires significant controls to ensure that the information contained within the system maintains the highest level of integrity, both in its completeness and accuracy, as well as its ability to provide users with the most current information available. We feel that the TSDBs display several vulnerabilities in controls over data validity and integrity.

TWWU Errors in Record Inclusion

The FBI's Terrorist Watch and Warning Unit (TWWU) receives requests from FBI field agents to include an individual with ties to terrorism into the appropriate federal databases. These requests are provided on nomination forms, which indicate whether the request is an initial submission, a supplement to the initial submission, or a request for removal from the databases. We selected for review nine nomination forms based on TWWU-completed activity and the type of requests made.

From our analysis of this limited number of transactions, we determined that nominations to the consolidated database could be untimely, sometimes resulting in delays of up to 45 days. The delay in entering this information into the consolidated database presents a vulnerability to the screeners in correctly identifying an individual, and contributes to the incompleteness and inaccuracy of the database as a whole. In addition, the TWWU is making errors in the delivery of the nomination forms to the appropriate agency for inclusion into the applicable database. For example, one form was submitted to the TWWU on August 26, 2004, to nominate an individual related to domestic terrorism for inclusion in the VGTOF database. This nomination form was reviewed by the TWWU and, instead of being provided to the TSC for data entry into the VGTOF database, the form was incorrectly provided to NCTC. The NCTC

[61] The 1A database did not include INA codes, but instead included similar descriptive fields called "warnings" and "categories."

mistakenly included this purely domestic matter into the TIPOFF database. On September 9, 2004, the TSC received NCTC's regular electronic file of updated records and uploaded this particular record into the TSDB. On October 1, 2004, the day we identified this error, NCTC sent its regular electronic update file with a deletion prompt for the record. As a result, the record was deleted from the TSDB. At that time, the TSC Nominations Unit staff called the TWWU to request the nomination form so they could appropriately enter the record into the VGTOF database from which they would correctly upload the record into the TSDB. This example shows that these errors can cause a lengthy delay in the inclusion of terrorist records in the TSDB and supporting databases. These mistakes can cause incompleteness in the consolidated database, which can create a security vulnerability.

Inclusion of Known Terrorists in the TSDB

We performed limited testing on the TSDB 1A and 1B to determine if publicly known terrorists were included in the consolidated database. We selected for our review a total of 39 names: 14 from news media accounts, 19 from the FBI's Most Wanted list, and 6 from the DOS' List of Terrorists under Executive Order 13224. We searched both TSDB 1A and TSDB 1B for these 39 names. Our analysis concluded that 37 of the 39 names were in both the TSDB 1A and 1B. Of the two remaining names, one was recorded accurately in the 1A database but contained significant spelling variations in 1B; the other name was included only in TSDB 1A where the individual was identified as armed and dangerous. These latter two names both originated from the DOS' List of Terrorists under Executive Order 13224. TSC officials 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.

Our review of the 39 known terrorist names also revealed that TSDB records for five of the individuals were not marked for export to the appropriate receiving databases. It is critical that the TSC develop strong controls to ensure that each name in the TSDB is appropriately marked for export to the relevant supporting systems so necessary actions are taken if the individual encounters a law enforcement officer. The omission of a watch listed name on any one of the applicable supporting databases could result in a failure to identify and detain a potential terrorist in the United States.[62]

[62] This test was based on our review of the information contained in TSDB records. We did not conduct further testing to determine whether these individuals had been recorded in the supporting databases through different processes.

Conclusion

The TSC maintains information from an array of organizations to fulfill its mandate to maintain a complete, accurate, and thorough consolidated database of terrorist information. Our review of the consolidated watch list identified a variety of issues that contribute to weaknesses in the completeness and accuracy of the data, including variances in the record counts between TSDB 1A and 1B, duplicate records, missing or inappropriate handling instructions or categories, missing records, and inconsistencies in identifying information between TSDB and source records.

The TSC must establish a mechanism for regularly testing the information contained within the consolidated databases. A database containing such vast amounts of information from multiple government agencies cannot be maintained successfully without standard procedures to ensure that the information being received, viewed, and shared is of the utmost reliability.

Recommendations

We recommend that the TSC:

9) Review the 1,200 TSDB 1A records, which may require manual correction, to ensure that these records are included in TSDB 1B, if appropriate.

10) Review and correct the 31 duplicate records identified in the TSDB 1B.

11) Review and correct the four records identified in the TSDB 1B as having duplicate TIPOFF record numbers.

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

13) Ensure that each record in the TSDB 1B can be traced to either the FBI or NCTC database.

14) Establish codes that more accurately describe domestic terrorist activity, replacing the INA codes that are currently applied to domestic terrorist records.

15) Review the INA codes applied to domestic terrorist records to ensure they properly reflect domestic terrorist activity.

16) Assign handling codes to all records within the TSDB that are exported to VGTOF, including the 336 records that we identified as lacking handling codes.

17) Review and correct the inconsistent assignment of low-level handling codes to records with “armed and dangerous” INA codes.

18) Establish in TSDB 1B separate fields to identify [SENSITIVE INFORMATION REDACTED] and [SENSITIVE INFORMATION REDACTED].

19) Enhance the TSDB 1B by ensuring that all available fields of information have been activated and populated as appropriate.

20) Implement automated procedures to ensure records and corresponding data transmitted to and from the TSDB is accurate, consistent, and complete. This should include a review of the eight VGTOF records and the three TIPOFF records that were omitted from the TSDB 1B and the two TIPOFF records omitted from the TSDB 1A.

21) Work with partner agencies to establish data field definitions and consistently apply them within all coordinated databases.

22) In coordination with the supporting agencies, establish procedures to identify and resolve missing and conflicting record information.

23) In coordination with the TWWU, streamline operations to ensure nominations are made to the appropriate system in a timely manner and in accordance with HSPD-6 so that domestic terrorist records are not forwarded to NCTC.

24) Establish procedures to regularly review the Department of State’s List of Terrorists under Executive Order 13224 to ensure individuals are accurately included in the TSDB.

CHAPTER 8: Management of the TSC Call Center

The TSC call center employs call screeners who respond to queries from law enforcement, border, and intelligence agencies 24 hours a day, 7 days a week. As noted in Chapter 6, the TSC call center received an average of 85 calls per day in January 2005. To successfully meet their responsibilities, screeners need access to each supporting agency database in order to thoroughly perform searches and provide the most accurate response to the caller.

The demand for expedited response times promotes a fast-paced environment where high-quality data and effective database controls are crucial to safeguard the information available on the supporting databases, the data entered into the unclassified systems, and the quality of communication provided to TSC customers. As a result, call center staff need quality, on-going training to effectively accomplish their mission.

TSC Access to Databases

The TSC call center contains terminals connected to different agency databases, all of which can be accessed by the call screeners. These databases include TIPOFF, VGTOF, and TECS/IBIS/NAILS. State Department representatives who are co-located in the call center (but do not screen calls) also have access to CLASS, in addition to TIPOFF. The existence of such a large number of classified and unclassified databases in such a close environment underscores the need for strong controls. During the initial operations of the TSC, a limited number of call center staff had access to all of the supporting agency databases because security clearances had not been granted and because agencies had not yet approved additional staff for access to their databases.

Screeners routinely query names against the TSDB to check for any "hits," or matches within the database. They also use another database, called the Encounter Management Application (EMA), to record the details of all incoming calls to the call center, including what information they received from the caller, whether the information resulted in a match against the information in the TSDB, whether the caller was forwarded to CT Watch staff for further action, and the final disposition of the call.

Encounter Management at the TSC

The TSC uses the EMA, an Oracle-based program, to manage the data related to the calls received at the TSC regarding possible terrorism-related encounters. The EMA generates daily status reports of 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 agencies for further review.

The EMA was implemented in July 2004 to replace separate Oracle and Microsoft Access databases previously used by the TSC. Soon after the creation of the original Oracle database, TSC managers realized that the system required specialized programming to generate reports using the data it contained. Without these reports, tracking the various encounters with suspect individuals would have been difficult, and the opportunity to share the data with participating agencies would have been minimal. TSC officials told us that modifying the original Oracle database would have required IT personnel to divert their attention away from creation of the TSDB, which was not a viable option.

As a result, the TSC created a Microsoft Access Encounter Management database containing a duplicate set of the Oracle data, but with the ability to generate reports on daily, weekly, monthly, and cumulative call activity. In addition, this database generated detailed reports on: the calls received by state and local law enforcement; calls related to airline inquiries; the positive, negative, and inconclusive results from calls sorted by category; and reports on how many calls were referred to CT Watch. These standardized reports have been incorporated into the new EMA system.

We obtained a copy of the Microsoft Access Encounter Management database and selected a judgmental sample of 30 encounters occurring within the jurisdiction of the FBI's Chicago Field Office from the inception of the TSC on December 1, 2003, to July 25, 2004. For each encounter, we traced the communication and responsibilities of all parties involved from the time the call was received at the TSC. We gathered documentation from the TSC call center, the FBI's CT Watch, and the JTTF and Airport Liaisons attached to the FBI Chicago Field Office. While we found good communication between the agencies involved, we identified exceptions where coordination between agents handling an encounter could be improved. For example, in one of our sample encounters an individual was permitted to board a domestic flight despite being on the No-Fly list. In this case, CT Watch contacted previous and current case agents, who had conflicting information with regard to whether the individual was a threat to civil aviation. The CT Watch log did not reflect any further activity related to this matter, and the individual was allowed to board the aircraft. The local JTTF had no record of being contacted regarding this encounter.

In addition, we found poor quality controls in the supervision of TSC call screeners and poor data entry into both the Encounter Management

database and the CT Watch Log.[63] Specifically, we identified several instances where the information recorded on hard-copy Call Intake Forms was not appropriately transferred into the Encounter Management database. Examining the information transferred, we found data transposed and entered into wrong fields. Additionally, discrepancies existed between the data recorded by the TSC and that of the FBI's CT Watch. Examples of this include different recorded times of calls being forwarded and received, different flight times on subjects due to arrive in the United States, different contact persons for the applicable cases, and often little or no resolution of the encounter recorded in the TSC's Encounter Management database. We attributed the missing resolution detail to the lack of a status field in the TSC's Encounter Management database that supervisors could use to track the work flow and easily determine calls requiring follow-up action.

Reliance on TDY Staff

Currently, the TSC relies heavily on personnel provided by participating agencies for short periods of time. These individuals generally have a tour of duty lasting approximately 60 to 90 days. This results in rapid personnel turnover that, in turn, significantly increases the amount of training needed and by its nature results in a less experienced screener workforce.

Officials at the TSC stated that rotating staff is important to the mission of the TSC. According to TSC officials, the desired arrangement would be to have staff loaned to the TSC from federal law enforcement and intelligence agencies for 90 or more days to enable them to apply their investigative skills in assisting callers. TSC managers stated that having law enforcement experience helps the screener understand what the caller is experiencing, and helps them identify when the information provided presents an investigative concern. However, we found that some detailed staff members came to the TSC directly from their initial law enforcement training or post-military service and had little experience in law enforcement or intelligence work. In addition, the regular rotating of staff hampers the TSC's ability to provide seasoned personnel that have experience as TSC call screeners. Using inexperienced screeners also results in difficulties when relaying information to CT Watch staff. For example, we were informed that special agents at the FBI's CT Watch often ask to speak to a call center shift supervisor because the initial screener has not done an adequate job of conveying the appropriate information.

[63] The CT Watch Log is an electronic file maintained by personnel in the FBI CT Watch Unit to record the activity of the unit in response to inquiries and requests for operational support. Because positive and inconclusive hits against the TSDB are forwarded to the CT Watch, its log contains information regarding the interaction between this unit and the TSC call center.

Training Call Center Staff

As previously discussed, training within the call center is a critical issue due to the constant turnover of non-permanent personnel. The TSC needs to repeatedly conduct clear and thorough training in order to ensure that calls are properly handled, database access is contained to appropriate use only, and data entry is completed securely.

During the course of our field work, we identified weaknesses in the training of call center personnel. First, because some of the call center managers are also on short-term loan from other agencies, the TSC has experienced difficulty in establishing a consistent, well-managed training program with centralized oversight. In addition, we found that call center employees received sporadic and, at times, inaccurate training. For example, a call center manager we interviewed was unable to identify specific individuals tasked with providing training to all employees for each call center shift. Further, call center management was unable to provide assurances that screeners, while receiving training regarding the TSDB 1B system when it became operational, were told that they should continue using the TSDB 1A database for primary call screening. Training in this regard was important because the 1B database was still considered to be in a preliminary status and the TSDB 1A remained the primary call center database until the TSC discontinued it in April 2005. Based on our observation, TSC staff updated the training manual to specify the primary screening database.

The training provided to call screeners also needs to address the necessity of thoroughly searching the supporting system records in order to ensure that all pertinent information is relayed to the FBI's CT Watch for follow-up action. During the course of our review, we identified an encounter with an individual for which significant derogatory information existed in the TIPOFF database. Our review of the TSC Encounter Management database and the CT Watch Log showed no indication that this important information contained in the TIPOFF database was relayed to CT Watch for consideration and action. The individual in question was on the watch list because of concerns that the individual was a financial supporter of terrorism and was being considered for visa revocation based on the derogatory information. However, the individual was allowed to enter the United States, and the FBI took no follow-up action. Neither the State Department, TSC, nor CT Watch could provide adequate explanation as to why no further actions were taken to check the status of the individual's visa revocation or to contact the FBI for further review. Department of State representatives at the TSC informed us that the initial visa revocation packet

was lost. However, when the packet was resubmitted three months after the encounter, the subject's visa was revoked within one week.

According to State Department officials at the TSC, the situation described above was an unusual circumstance and does not reflect the manner in which visa revocations are normally handled. While we recognize that many parties were remiss in not taking proper action to resolve this situation, the TSC is the primary organization with responsibility to identify such information and make it available to those who need it.

Timeliness of Response

Timeliness is critical when law enforcement encounters an individual, possibly a terrorist suspect, on the side of the road or when a plane is about to land in the United States and a potentially dangerous individual is on board. Neither the TSC nor CT Watch maintain records on the time that elapses between the key events of an encounter — for example, when the TSC receives a call; when the call is forwarded to CT Watch; and the amount of time before instructions are provided to the caller, the call is resolved, and feedback is provided. A CT Watch official estimated that the response time, in general, has decreased from an average of about 45 minutes per traffic stop to approximately 20 minutes.

During our review of the Encounter Management database, we found that on many occasions more than an hour elapsed between the time a call was received in the TSC's call center and the time the call was referred to CT Watch for further action. Additionally, we found that calls had been received prior to a plane landing in the United States, but no contact was made with CT Watch or DHS's National Targeting Center until after the individual had been allowed to depart the aircraft. It is critical to ensure that no unnecessary delay occurs on any encounter.

We understand that the number of actions and queries the call screeners are required to perform affects the amount of time needed to resolve a call. However, we believe the TSC would benefit greatly from regularly tracking and monitoring these times to ensure that call screeners are responding to callers in a timely and useful fashion. Such tracking could also identify process improvements that can be implemented to save precious time.

Data Entry Problems

Currently, call screeners use a manual Call Intake Form to record the information provided by a caller and then forward that information to CT Watch. When a call is forwarded to CT Watch or is considered a negative match with no further action required, the call screener enters the data from

the form into the unclassified Encounter Management database. This redundant data entry is susceptible to transposition errors, missed data, and data inaccuracies. TSC managers informed us that they are taking steps to automate this process so manual Call Intake Forms will not be necessary.

Security Issues

When call screeners identify useful information in a supporting system, that information may be classified at the Confidential, Secret, Top Secret, or other level, depending on the source database for the information. This supporting material, while helpful, may inadvertently make its way into the TSC's unclassified databases and it is important to ensure that proper controls are in place to prevent this from happening.

We identified an incident where a classified portion of the CT Watch Log, which was appropriately marked, was copied verbatim by a TSC call screener into the unclassified Encounter Management database resolution. According to DOJ regulations, classified information must be appropriately marked and those markings must be carried forward to any newly created documents.

Upon our discovery of this incident, we immediately discussed our concerns with TSC officials, who informed us that classified material had been entered into the unclassified TSC Encounter Management database on at least three prior occasions. While the paragraph we identified ultimately was downgraded to unclassified by the FBI Security Complaints Division, the prior incidents all involved information that was ultimately decided to be classified as national security information. According to the information available, the corrective measures taken were limited to removing specific pieces of classified information from the database. Even with the frequency of such events occurring, TSC staff did not conduct a search for any additional classified information. None of the TSC officials available could provide complete information about these prior security incidents, including how they were first identified, because many of the individuals involved were assigned to the TSC on a temporary basis and were no longer detailed there. In our discussions with TSC managers about these issues, the officials expressed the need for a full-time security officer to replace the current individual detailed from the FBI.

Duplication of Efforts

It is evident from our review that certain functions in the encounter management process are causing a duplication of efforts. Upon the referral of an encountered individual for further review, CT Watch routinely re-checks all databases previously searched by the TSC call screener.

CT Watch officials stated that this was necessary because of incomplete searches and inaccuracies in the data recorded by TSC call screeners in the early days of the TSC's existence. Because the result of these errors could ultimately result in an incorrect identity match, CT Watch saw the need to ensure the information was correct. While this appears to have been a necessary procedure to follow in order to ensure accurate information was provided to the caller, CT Watch officials have recently indicated that the quality of information they receive from the TSC call screeners has greatly improved and their current checks rarely reveal inaccuracies. However, all databases continue to be re-searched by CT Watch. This increases the amount of time CT Watch call screeners spend working on a particular encounter, and could potentially cause a time delay for the caller in the field. Upon the initial deployment of real-time connectivity to the TSDB, it would be advantageous to reduce the amount of duplication between the TSC and CT Watch call center procedures.

In addition to the duplication of efforts within the FBI, we identified further duplication between the TSC and the DHS. The NTC is the CBP's 24-hour, 7-day a week call center that provides operational support of the CBP's anti-terrorism efforts. Primarily staffed with personnel from within the DHS, the NTC assists both the TSC and CT Watch in the identification and apprehension of persons named within the TSDB. When an inspector or agent on the border queries the IBIS database (thereby also querying NCIC) on a particular encounter with an individual, they receive a response back informing them to call the NTC if the name of the individual is on the terrorist watch list. The NTC then calls the TSC to initiate the full screening process. TSC searches the individual in accordance with its customary procedures and passes any positive or inconclusive search results to CT Watch for further action. CT Watch then contacts NTC, which in turn contacts the agent on the border. We believe that this process results in a duplication of efforts and the efficiency of the process thereby suffers.

Misidentification Process

When a person has been encountered and call screeners find that the individual has mistakenly been identified as a hit against the consolidated watch list, the incident (or misidentification) is documented, reviewed by management, and provided to the TSC's Quality Assurance team for further action. The Quality Assurance team is to review the information and coordinate with the agency that nominated the record for inclusion in the database to determine what actions are needed to resolve the misidentification, including the possibility of removing a name from the TSDB.

According to TSC officials, the organization has recently established a process to accept referrals from other agencies of complaints or inquiries from individuals who are having difficulty in a screening process that may be related to the consolidated terrorist watch list. According to this process, the TSC Quality Assurance staff researches each individual case to determine if the individual is a misidentified person – that is, an individual who is mistaken for a watch listed person but is not actually a known or suspected terrorist. TSC managers reported that they are working with each screening agency to develop procedures for the various screening processes to help misidentified persons.

However, we found that these processes had not been articulated in a formal, written document clearly defining the protocols to be followed by TSC staff when addressing misidentification issues. Because of the serious impact of possible misidentifications, we believe the TSC should formally articulate procedures for handling misidentifications and train its staff on the proper way to manage these occurrences.

Conclusion

Screeners in the TSC call center respond to queries from law enforcement, border, and intelligence agencies 24 hours a day, 7 days a week. These screeners access multiple systems and a wide array of data and have direct responsibility for providing accurate information to front-line officers expeditiously. However, management of the call center and its staff is in need of improvement. It is essential that the TSC provide adequate training to these individuals and we feel that the execution of this function has been lacking. We observed instances in which TSC call center staff did not relay important information to CT Watch or other responding law enforcement agents. In addition, call center staff appear to be insufficiently trained in the proper handling of classified national security information and entry of information into the TSC Encounter Management database.

Recommendations

We recommend that the TSC:

25) Establish supervisory controls to ensure that the work of call center personnel is reviewed on a regular basis for completeness, accuracy, and timeliness.

26) Establish protocols for the proper entry and review of data into the Encounter Management database.

27) Develop an automated method for flagging records in the Encounter Management database that require follow-up actions, and establish procedures to complete the necessary follow-up conducted within a reasonable period of time.

28) Establish regular training for call center screeners to keep them informed of the proper approach to screening subjects in the database and providing information to CT Watch, as well as for the entry of appropriate data into the unclassified database.

29) Establish and implement an automated system for tracking the amount of time that elapses between the key events of an encounter, such as when the TSC receives a call, when the call is forwarded to CT Watch, the amount of time before instructions are provided to the caller, and the amount of time before a call is resolved and feedback is provided.

30) Establish an automated method for the entry of call data and the sharing of such data with CT Watch to eliminate the redundancy of recording call information on the Call Intake Form and in the Encounter Management database, and to reduce the time it takes for CT Watch to receive the data and initiate further actions necessary.

31) Assign a full-time security officer to handle security requirements and provide TSC staff guidance and training on the proper handling of national security information.

32) Review all records in the Encounter Management database for classified data within the unclassified system and develop a process for regularly checking the work of the call screeners to ensure that classified information is not entered into the unclassified system.

33) Develop a method for recording and reporting security breaches.

34) Work with partner agencies such as CT Watch and DHS's NTC to reduce possible redundancies and duplications of effort.

35) Strengthen procedures for handling misidentifications and articulate in a formal written document the protocol supporting such procedures, as well as provide training to staff on the proper way to manage misidentifications.

CHAPTER 9: Future of the TSC

The TSC has made significant progress in consolidating the U.S. government's approach to terrorist screening. Most importantly, it has created a database that has been used to integrate terrorist information that previously existed in myriad systems and formats and established an around-the-clock call center to assist in ascertaining the identity of encountered individuals. However, the TSC must build on its initial accomplishments and address the areas of weakness that we have identified, including the efficiency, accuracy, and completeness of its database and the management of its call center activities. TSC managers must also ensure that the organization is adequately planning for future improvements to its operations.

Evaluating the Effectiveness of the TSC

The Director of the TSC informed us that because the TSC is relatively new, it has not yet established a formal procedure to evaluate the organization's overall effectiveness. Such procedures are important to ensure the TSC is as helpful as possible to assist law enforcement in the identification of potential terrorists. In April 2004, the TSC Director began to informally track the successes of the TSDB, as well as the "holes" in operations and communications identified by TSC staff. As of October 2004, however, the tracking process had not yet been formalized.

Strategic Planning

As of March 2005, the TSC had no formal strategic plan by which to guide its progress, staffing, organizational structure, and future planning. A strategic plan should provide a road map for an organization to achieve its strategic goals and objectives. This formal document also should provide the strategies and methods for evaluating the performance of an organization. TSC managers have indicated that they are working to develop a strategic plan from the outline that was conceived at the inception of the organization. However, while they appear to understand the importance of creating such a plan, they told us they do not view its creation as a high priority or an essential task at this point in time.

We believe that strategic planning efforts would assist the TSC in addressing the most significant weaknesses that we identified – namely, the watch list errors and omissions, deficiencies in the management of the call center, and the immaturity of the agency's information technology environment and controls. In performing the tasks that are necessary to develop a comprehensive strategic plan, TSC managers should identify the

need for personnel, experience, and skill sets necessary to staff, train, and manage the various TSC units in order to fulfill the goals and objectives of the organization. The identification of the knowledge, skills, and abilities that staff members need to perform the necessary functions within the TSC may also lead to the recruitment of different types of employees from different sources. With a strong strategy in place for the various units of the organization, TSC managers should identify the controls necessary to ensure data is protected, procedures are established and followed, and personnel are adequately trained. A well-defined strategic plan would help TSC managers prioritize what must be accomplished.

Continuity of Operations Plan/Emergency Action Plan for the TSC

We obtained and reviewed the TSC's Continuity of Operations Plan (COOP), its Emergency Action Plan, and the Disaster Recovery Plan it created using Federal Emergency Management Agency (FEMA) and Department of Justice guidance. The TSC-developed COOP, dated August 10, 2004, provides guidance and legal authority to TSC employees to facilitate a timely and effective response, relocation, resumption, recovery, and restoration of essential operations in the event of a crisis. According to the COOP, the plan offers a set of "pre-defined and flexible procedures to be used before and after a crisis to reduce ad-hoc reactions, loss of information, duplication of efforts, and prolonged disruption of mission critical services to the intelligence and law enforcement community."

Our review of the COOP indicates that the plan provides a broad, comprehensive framework that identifies key officials and units within the TSC, including roles and responsibilities; defines orders of succession and delegations of authority; delineates essential functions and activities; establishes a methodical plan for the orderly transition of functions including key operations, as well as realistic timeframes and benchmarks; determines both the mission critical data and systems necessary for effective operations; and specifies alternate operating facilities. Based on the COOP, individual departments within the TSC (such as information technology), establish and maintain their own plans, procedures, and records in support of continued operations.

With an effective date of October 25, 2004, the TSC's Emergency Action Plan (EAP) provides specific direction regarding the protection of Communication Security material and other classified material, the evacuation of personnel, and the actions to be taken in various emergency situations. The TSC's Disaster Recovery Plan (DRP), dated August 10, 2004, states that it was derived from both the COOP and the EAP. Further, the COOP and EAP were designed to include all necessary components of a DRP.

Because we did not receive the TSC's COOP, EAP, and DRP until December 2004, after we had concluded our field work, we were unable to verify if the TSC had tested the equipment, trained the employees, and performed exercises in accordance with FEMA guidelines. However, based on our field work, we have significant concerns whether certain logistical and functional obstacles have been addressed.

First, the FBI CT Watch serves as the back-up facility for the TSC but does not have access to the consolidated terrorist information database. Second, while we have been told that the TSC regularly backs up the database information onto removable media and stores the data off-site to allow for the recovery of information, none of the TSC officials we asked knew where this storage site was located. Third, we are unaware of any off-site systems that are equipped to run the TSDB software and connect to the end-user databases for data export should the TSC main facility be crippled or destroyed. Finally, according to TSC managers, [SENSITIVE INFORMATION REDACTED].

Database Classification

Given the security concerns we identified during our audit (such as the entry of classified information into the unclassified Encounter Management database), officials at the TSC have discussed the desire to move the Encounter Management database to a classified network. This would allow call screeners to enter classified information detailing the events of an encounter into the Encounter Management database. While call screeners would need to continue to ensure information entered is not classified at a level higher than that of the network used, this move would most likely allow for information in the CT Watch Log to be included in the language of the encounter detail. This would provide the TSC with the stronger security controls that are needed because of the high turnover of TSC detailees and the weak training program that leaves data entry vulnerable.

Officials at the TSC have also discussed the possibility of moving the TSDB to a network capable of recording material on a Law Enforcement Sensitive, Confidential, Secret, Top Secret, or other level, and transferring only appropriate material to other agencies at the applicable level of classification. For example, state and local law enforcement officials who query the NCIC database now only receive information classified as Law Enforcement Sensitive, since state and local police officers do not carry the appropriate clearances for information classified at higher levels. A classified TSC network would also allow, for example, the TSC to include in its database information of a higher classification level provided by NCTC to

better identify subjects during the screening process. This information would remain on the higher classification level of the database and would not be disseminated to the majority of the TSDB users, such as local law enforcement.

Considering the problems we identified in the TSC's handling of classified information, we believe that the TSC should proceed cautiously with regard to the classification level of the network housing the TSDB and its plans to change the classification level of the TSDB as a whole. The creators of the TSC, through the September 2003 Memorandum of Understanding, clearly designated that the consolidated watch list was to be a sensitive, but unclassified subset of the available terrorist information. In addition, the MOU highlighted the importance of sharing information with all appropriate users.

A New Direction

Since the completion of our field work, at least two developments have occurred that will impact the operations of the TSC. Although we were unable to perform detailed audit work in each of the areas, the TSC has asserted that it is developing procedures to address these two matters, which are discussed below.

Issuance of HSPD-11

On August 27, 2004, the President signed Homeland Security Presidential Directive-11 (HSPD-11) entitled, "Comprehensive Terrorist-Related Screening Procedures." The new HSPD-11 supplements HSPD-6 and calls for greater participation from a variety of federal agencies in the development of "…comprehensive, coordinated, systematic terrorist-related screening procedures and capabilities…." The new directive calls for many enhancements to the current screening process, including but not limited to the elimination of any duplicative terrorist screening systems and the enhancement of information flow between the various screening programs.

Secure Flight

One of the recommendations of the National Commission on Terrorist Attacks upon the United States (9/11 Commission) stated that the federal government should assume responsibility for checking airline passengers' names against expanded "no-fly" and "automatic selectee" lists. Presently, this function is performed by individual airlines. In response to the 9/11 Commission's recommendations, the DHS proposed to expand its airline screening program to include both international and domestic flights.

Currently, only international flights are regularly pre-screened. As a result, the DHS is developing a next-generation system of domestic airline passenger pre-screening called "Secure Flight." This new system will compare passenger name record information against the information contained in the TSDB.

In partnership with other agencies, the TSC is working to expand its capacity to accommodate the anticipated workload associated with inquiries related to the approximately 1.7 million passengers who travel on domestic flights each day. The TSC anticipates needing significant additional resources to carry out this new responsibility. The TSC's FY 2006 budget includes a request for a $75 million increase for the TSC's efforts related to implementing the DHS's Secure Flight program. Congress has asked and we intend to conduct an audit of the TSC's plans for Secure Flight.

Conclusion

The TSC has continued to improve to its consolidated database, outreach performance, and overall development. However, prioritizing efforts to develop a formalized strategic planning document is an important step for the TSC to identify areas in need of stronger controls, enhance staffing qualifications and placement, and plan for the necessary systems and procedures that will enable the TSC to attain its goals and objectives. TSC officials also have begun preparing for disaster recovery and emergency situations, but enhancements are necessary to ensure that the TSC is prepared for these undertakings should they ever need to be set in motion. In addition, as a newly established organization, the TSC has the opportunity to enhance its performance by measuring its effectiveness as a centralized screening and coordinating center for managing terrorism-related encounters. By doing this, the TSC will more efficiently identify the successes of the organization while understanding where the weaknesses lie and the importance of resolving such matters.

Recommendations

We recommend that the TSC:

36) Develop a formal process for evaluating the effectiveness of the TSC.

37) Develop a formal, comprehensive strategic plan to establish the framework necessary for accomplishing the mission, goals, and objectives of the organization.

38) Enhance the COOP and EAP to: a) include preparations for access to the consolidated terrorist information database at the established back-up site, b) identify a location for the storage of database back-

up disks in preparation for the loss of database information should a power surge or disaster occur, c) establish an off-site system that is equipped to run the TSDB software as well as connect to the end-user databases for data export, and d) ensure that proper safeguards are in place for the security and temperature control of the TSC.

39) Ensure that the COOP and EAP are fully implemented including employee training, equipment testing, and plan exercising.

40) Consider the transfer of the Encounter Management database to a classified network capable of maintaining the database at the various classification levels.

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit of the Terrorist Screening Center (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's internal control structure as a whole. However, we noted certain matters involving internal 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 internal control structure that, in our judgment, could adversely affect the TSC's ability to effectively organize a coordinated approach to terrorist screening. We identified weaknesses in: 1) information technology oversight and review, 2) data accuracy and completeness, 3) staffing/hiring of personnel, 4) training provided to call center staff; 5) management of the call center, and 6) strategic planning. These issues are discussed within the body of this report.

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

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

We have audited the FBI's Terrorist Screening Center. In connection with the audit, as required by the 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 Terrorist Screening Center is the responsibility of the TSC's management.

Our audit included examining, on a test basis, evidence about laws and regulations. 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 watch list identified weaknesses related to the accuracy and completeness of the data. This condition is fully discussed in Chapter 7. The requirements for an accurate and complete watch list are contained in HSPD-6.

In addition, while performing our audit, we identified an issue regarding the TSC's compliance with 28 CFR Part 17, sections 17.25 (a), 17.26 (b) and (c). We identified instances where information denoted to be classified at the Secret level was entered into an unclassified database located on an unclassified network, and the original classification marking for the Secret data was not retained. We notified the FBI Security Complaints Division and TSC Management of these instances. This condition is fully discussed in Chapter 8 of this report.

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.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

Audit Objectives

The objectives of the audit were to determine whether the Terrorist Screening Center (TSC): 1) has implemented a viable strategy for accomplishing its mission; 2) is effectively coordinating with participating agencies; and 3) is appropriately managing terrorist-related information to ensure that a complete, accurate, and current watch list is developed and maintained.

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 September 16, 2003, through April 2005.

To accomplish our objectives, we conducted work primarily at the TSC, located in the Washington, D.C., metropolitan area and interviewed contractors and representatives from various participating Departments working within the Operations Branch, Information Technology Branch, Administration Branch, TSC Call Center, Customer Service Unit, Nominations Unit, and other support areas. Additionally, we visited other federal law enforcement agencies whose work related to TSC operations, such as the Terrorist Threat Integration Center, or NCTC. We also held interviews with the Director of the FBI's Foreign Terrorist Tracking Task Force, as well as FBI officials at FBI Headquarters from the Counterterrorism Watch (CT Watch); Budget Formulation and Presentation Unit; and the Executive Assistant Director and Deputy Assistant Director of the Counterterrorism Division. We visited the Chicago FBI Field Office and held meetings with the Assistant Special Agent in Charge and agents from the Chicago Joint Terrorism Task Force (JTTF).

We performed various tests of the Violent Gang and Terrorist Organization File (VGTOF), the State Department's TIPOFF system, the Terrorist Screening Database (TSDB) and the Oracle and Access Encounter Management databases used by the TSC. (The results of our testing are presented in Chapters 7 and 8 of this report.) We performed queries on the TSDB 1B as a whole to assist in verifying the integrity of the database information for the purposes of our audit objectives only. We did not test the integrity of the database from an Information Systems perspective, and

do not opine on the system infrastructure as a whole. Specifically, we performed multiple queries on the consolidated database using the most restrictive definition of a duplicate record – all five identifying fields identical. We did not test other combinations. We also performed queries on the quantity of data in the TSDB 1B and the sources from which it was obtained. In addition, we queried the total number of records without a handling code applied, and the total number of records within each handling and INA code.

We performed a detailed analysis of the electronic VGTOF file we received from CJIS, as well as on the Access file we received on the encounter management information. On the VGTOF file, we reviewed the quality and quantity of data being provided to the TSC, the accuracy of the data entry performed by the field offices, and the application of handling codes. On the Access file, we reviewed the completeness, accuracy, and timeliness of data entry and call response, the quality of feedback recorded in the database, encounters by location, and the number of resolutions overturned by CT Watch.

We also conducted testing of a limited number of records in the database and the encounters that have taken place. Although our sample was small, we consider even one error to be significant because of the potential impact that one missing record or one inefficient encounter could have on counterterrorism activities. We selected a judgmental sample of 59 records from the VGTOF database based on the handling codes assigned, and 51 records from the TIPOFF database based on the INA Codes assigned, and traced them forward to determine if those names existed within the TSDB, and whether the information on such persons was accurate. Appropriate follow-up was conducted on names not included in the TSDB and inaccuracies in the information reviewed. In addition, we selected a number of terrorists and terrorist aliases recently acknowledged by the FBI, the DOS, and various press releases to determine if the TSDB contained records for these individuals.

Further, we selected a judgmental sample of ten positive, ten negative, and ten inconclusive hits from the Encounter Management database that originated in Chicago and traced them through the encounter process to CT Watch and the deployment of the Chicago JTTF, identifying what communication was then fed back to CT Watch and the TSC. Negative hits were reviewed to determine the timeliness and adequacy of the call resolution.

Finally, we reviewed legislative material regarding the creation, establishment, and maintenance of the TSC, as well as manuals, policies and procedures, memorandum, correspondence, and electronic communications

related to the TSC. We also reviewed and collected various records and documents as needed, including financial documents, strategic planning documents, workload data, position descriptions, prior audit reports, and reports to Congress

ACRONYMS USED THROUGHOUT THE REPORT

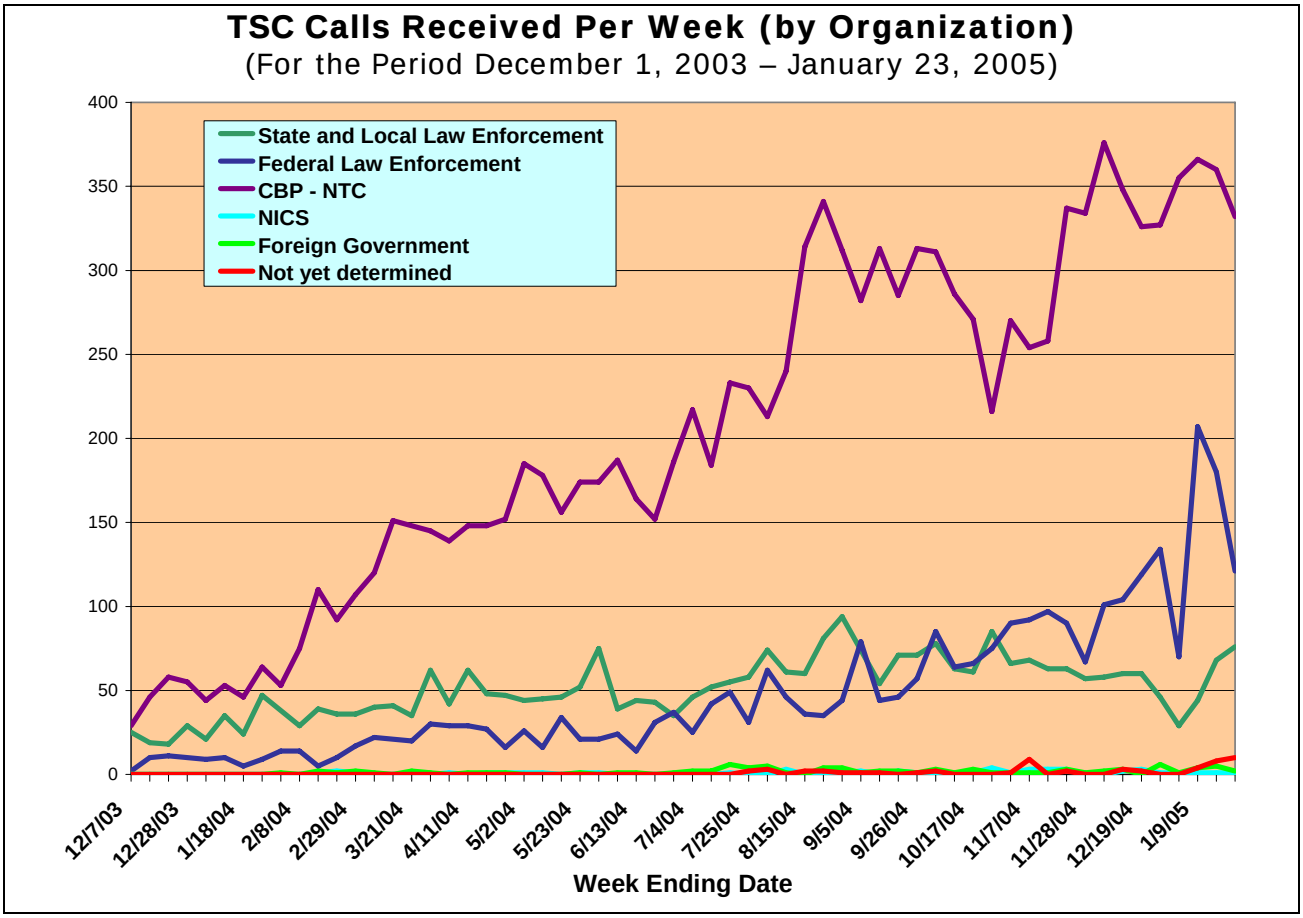
ACS	Automated Case Support
CBP	Customs and Border Protection
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services Division
CLASS	Consular Lookout and Support System
COOP	Continuity of Operations Plan
CT Watch	FBI Counterterrorism Watch
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
DRP	Disaster Recovery Plan
EAP	Emergency Action Plan
EMA	Encounter Management Application
FBI	Federal Bureau of Investigation
FTTTF	Foreign Terrorist Tracking Task Force
GAO	Government Accountability Office
IAFIS	Integrated Automated Fingerprint Identification System
IBIS	Interagency Border Inspection System
INA Code	Immigration and Nationality Act Code
IT	Information Technology
JTTF	Joint Terrorism Task Force
	[SENSITIVE INFORMATION REDACTED]
MOU	Memorandum of Understanding

NAILS	National Automated Immigration Lookout System
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NICS	National Instant Criminal Background Check System
NLETS	National Law Enforcement Telecommunication System
NTC	National Targeting Center
NYSIIS	New York State Identification and Intelligence System
OIG	Office of the Inspector General
OMB	Office of Management and Budget
	[SENSITIVE INFORMATION REDACTED]
TDY	Temporary Duty
TECS	Treasury Enforcement Customs System
TIDE	Terrorist Identities Datamart Environment
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TTIC	Terrorist Threat Integration Center
	[SENSITIVE INFORMATION REDACTED]
TWWU	Terrorist Watch and Warning Unit
USPS	United States Postal Service
VGTOF	Violent Gang and Terrorist Organizations File

TSC CALL STATISTICS

TSC Call Volume Progression[64]

As discussed in the body of this report, the TSC receives calls on a daily basis from state and local law enforcement, federal law enforcement, customs agents and border inspectors, private arms dealers (through NCIC), and foreign governments. The chart below indicates the call trends for each of these organizations since the stand-up of the TSC.



Source: TSC Management

As shown in the preceding exhibit, most of the calls received by call screeners at the TSC are derived from the CBP. In fact, these calls equaled 67 percent of the total calls received between December 1, 2003, and January 23, 2005. As of December 7, 2003, the total calls per week from the CBP totaled 29. This number increased to 221 calls per week by July 25, 2004, a 662 percent increase in the TSC's call volume from the CBP per week. By January 23, 2005, the total number of calls per week from the CBP totaled 332,

[64] These call figures were provided by TSC management. On many occasions, the numbers do not add up to equal the totals shown. We did not attempt to verify the numbers provided. We recommend in the body of our report (Chapter 6) that the TSC input controls to ensure these numbers are regularly checked for accuracy.

an overall increase of 1,045 percent. These numbers reflect the impact of potential terrorist encounters at U.S. borders and airports, and show the importance of establishing a mutual protocol between the CBP and the FBI for handling these encounters (this subject is discussed further in Chapter 7 of the report).

The state and local law enforcement agency (LEA) calls represent 17 percent of the total calls received by the TSC between December 1, 2003, and January 23, 2005. Second in call volume to the CBP, the state and local calls increased by 204 percent during this time period, from 25 calls per week in December 2003 to 76 calls per week in January 2005. This increase indicates TSC's success at communicating the purpose and importance of the TSC in encounter process to the officers on patrol. This increase in state and local calls is necessary for the TSC to effectively manage all terrorist encounters, and would be expected to continue increasing as the TSC conducts further outreach to the population of state and local law enforcement.

Total Calls By Organization *(December 1, 2003, through January 23, 2005)*	
State and Local LEA	**3,092**
Federal LEA	**2,902**
CBP – NTC	**12,343**
NICS	**47**
Foreign Government	**89**
Not Yet Determined	**54**
Total[65]	**18,534**

While calls from federal law enforcement agents totaled 16 percent of the total calls received during this period, the call volume per week from federal law enforcement increased by 5,950 percent, ranging from 2 calls per week in December 2003, to 121 calls per week by January 2005. This is a significant increase in the use of the TSC as a screening center for terrorist encounters by federal law enforcement agents and amplifies the need for such an organization to centralize anti-terrorism efforts.

The TSC also receives calls resulting from individuals accessing the National Instant Criminal Background Check System (NICS). The NICS is the FBI's database that checks available records on persons who may be disqualified from receiving firearms. Established as a result of the Brady Handgun Violence Prevention Act (Brady Act) of 1993, Public Law 103-159, the system allows for Federal Firearms Licensees to retrieve, via telephone or electronic communications, immediate information as to whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law. According to the NICS 2001/2002 Operational Report, as of December

[65] As previously stated, these call figures were provided by TSC management. In this table, the numbers do not add up to equal the total shown. We did not attempt to verify the numbers provided.

31, 2002, the NICS Section of the FBI had denied a total of 281,883 firearm transfers to prohibited individuals and estimates that the approximate total number of denials is in excess of 563,000 since the inception of the NICS.

Calls resulting from inquiries in the NICS database are few. These calls range between 0 and 1 per week at the TSC. As of January 23, 2005, TSC call screeners had received a total of 47 calls in response to NICS inquiries. However, the significance of each call received at the TSC from counterterrorism activities is great.

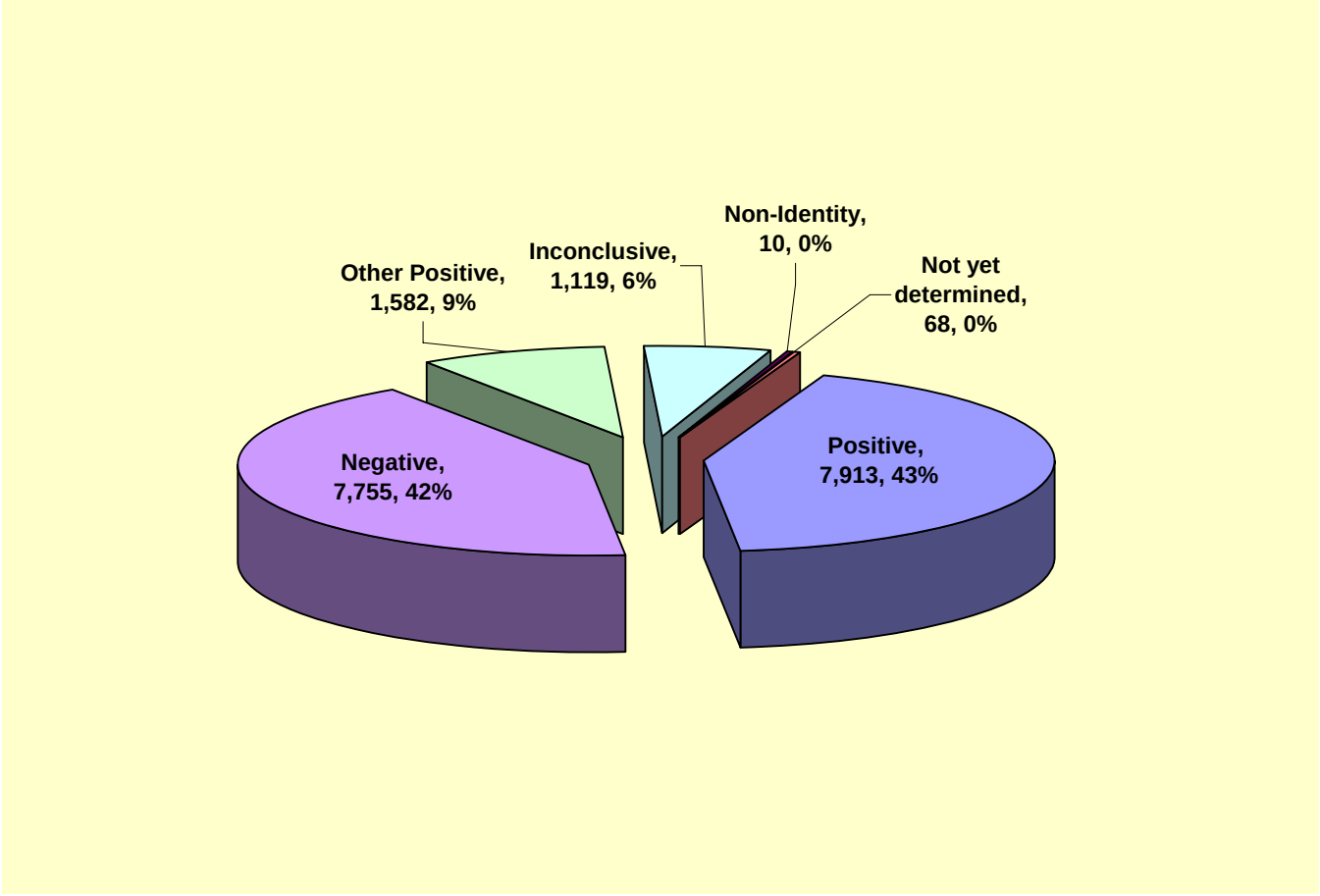
Between December 1, 2003, and January 23, 2005, a total of 89 calls resulted from foreign government inquiries on persons of interest. This resulted in less than one percent of the 18,534 total calls received by the TSC during this period. The origin of a total of 54 calls had not yet been determined as of January 23, 2005.

Call Resolution

Of the calls received by TSC call screeners since December 1, 2003, approximately 43 percent resulted in positive identity matches in the TSDB, requiring the calls to be forwarded to CT Watch for further action (see Chapter 6 for a description of the encounter process). Of the remaining calls, six percent resulted in inconclusive hits, for which the TSC was unable to determine whether the encountered individual was on a watch list. These calls are also forwarded to CT Watch for further research for a conclusive identification. During this period, a total of 9,284 calls were forwarded to CT Watch for further review.

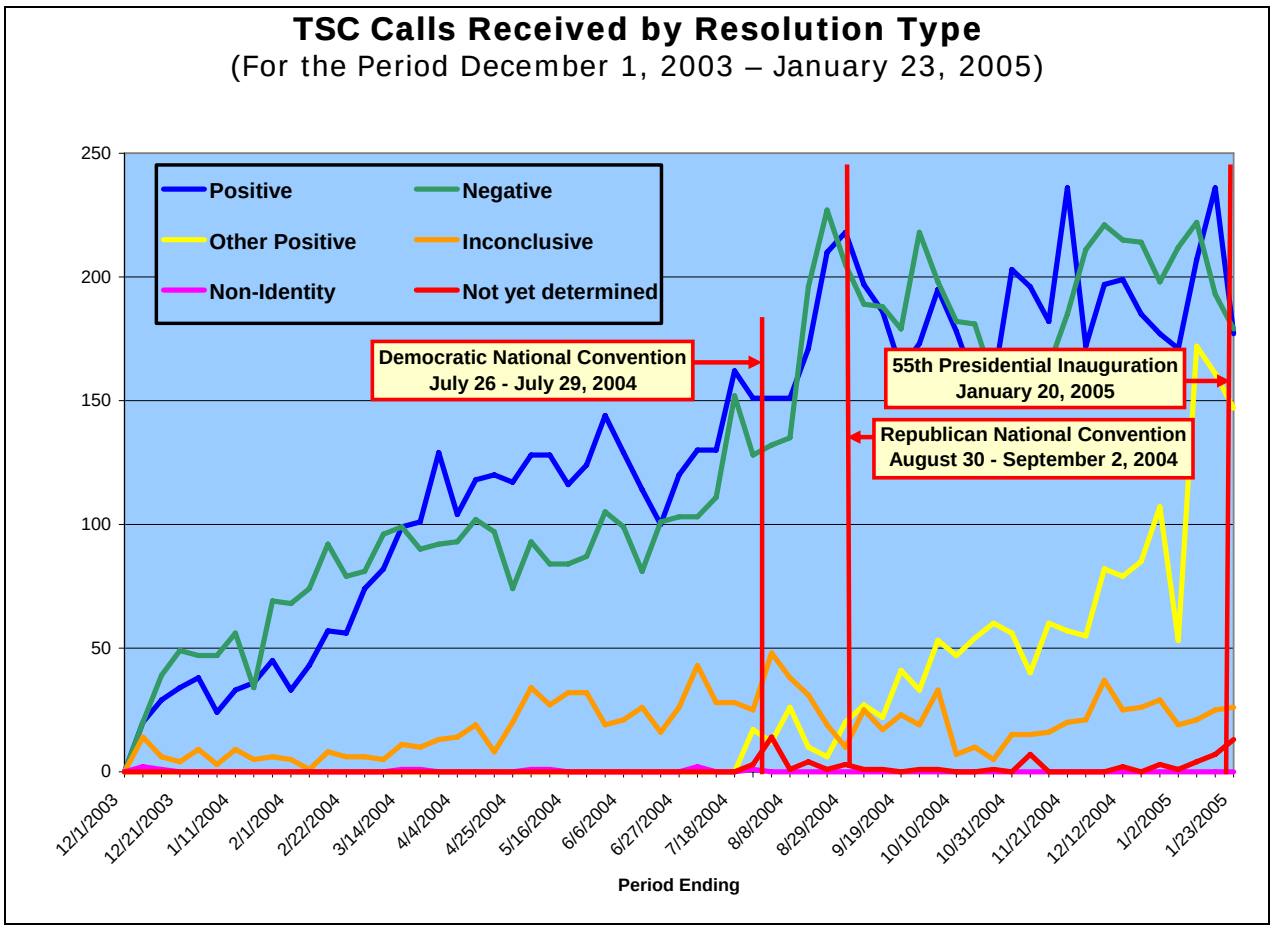
Negative hits, or searches in the database that identified no terrorist match, accounted for 42 percent of the total calls received. Ten of the total calls were classified as “Non-Identity,” or the result of a hit occurring where an individual is not present for identification. An example of this would be when a law enforcement officer comes across an abandoned car and runs the license plate number in the NCIC database. If the license plate is referenced in the database in relation to a suspected terrorist/terrorist supporter, the plate would result in a “Non-Identity” hit. The below chart displays the total number of positive, negative, inconclusive, and non-identity hits that occurred as a result of calls to the TSC between December 1, 2003, and January 23, 2005.

TSC Calls Received by Resolution Type
(For the Period December 1, 2003 – January 23, 2005)



Source: TSC Management

In addition, the TSC has experienced sporadic increases in call volume during events with a high national profile. As shown in the following exhibit, call volumes and corresponding positive and negative identity matches appear to increase during the Democratic National Convention, Republican National Convention and the Presidential Inauguration.



Source: TSC Management

Calls by Handling Codes

As discussed in Chapter 5, a handling code is to be assigned to every record within the TSDB. FBI agents nominating a record for inclusion in the VGTOF and supporting databases assign a handling code based on the information available about the individual. These handling codes provide instructions to law enforcement. The TSC received a relatively small number of calls related to handling codes 1 and 2, and a significant call volume in handling codes 3 and 4. [SENSITIVE INFORMATION REDACTED]

TERRORIST SCREENING CENTER RESPONSE

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

June 8, 2005

Ms. Carol Taraszka
Regional Audit Manager
Office of the Inspector General
Chicago Regional Audit Office
U.S. Department of Justice
Suite 3510A
500 W. Madison Street
Chicago, Illinois 60661

Dear Ms. Taraszka:

Re: RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL'S AUDIT OF THE TERRORIST SCREENING CENTER

The Federal Bureau of Investigation has prepared appropriate responses to the recommendations contained in your report captioned above. The classification and sensitivity reviews were completed and are enclosed with this letter.

Please contact either myself or Robin Dinerman of my staff should you have any questions. Ms. Dinerman may be reached on (202) 324-6389.

Sincerely yours,

Charlene B. Thornton

Charlene B. Thornton
Assistant Director
Inspection Division

Enclosures (2)

THE TERRORIST SCREENING CENTER DRAFT AUDIT REPORT

Terrorist Screening Center Response

The United States (US) Department of Justice (DOJ) Office of the Inspector General (OIG) conducted an audit of the Terrorist Screening Center (TSC) in 2004. The purpose of that audit was to determine whether the TSC: 1) has implemented a viable strategy for accomplishing its mission; 2) is effectively coordinating with participating agencies; and 3) is appropriately managing the terrorist-related information to ensure that a complete, accurate and current watch list is developed and maintained. On April 18, 2005, the TSC received a copy of the draft audit report for the purpose of providing comments on the recommendations and a sensitivity review. A separate response was required for each of the reviews, due to the DOJ/OIG within two weeks from April 18, 2005.

For its response to the recommendations, the TSC was requested to provide: a statement that the TSC either agrees or disagrees with each recommendation; if the TSC agrees, a description of actions completed and planned including dates when corrective action will be achieved; if the TSC disagrees that the recommendations can be implemented, a description of alternate corrective action for the DOJ/OIG's consideration. What follows below is the TSC response to those recommendations.

Executive Summary

First and foremost, the DOJ/IG began their audit within the first five months of the TSC initial operation and concluded several months later. Before TSC's inception, no agency or organization was responsible for consolidating the names and identities of both domestic and international terrorists. Furthermore, no agency was responsible for coordinating the Government's approach to terrorism screening. Since the initial days of the DOJ/OIG audit, and continuing several months after the on-site audit was concluded, the TSC maintains an accelerated pace of growth and evolution to building and refining a singular, unique and precedent setting agency which consolidates the Government's approach to terrorism screening. In the seventeen months of operation, the TSC has made significant strides.[66] Most notably, since December 1, 2003, on a routine and daily basis, the officer on the street, the inspector and the border, and the consular officer at the embassy all have access to same updated list of known and suspected terrorist maintained by the United States Government.

[66] The DOJ/OIG onsite audit was conducted from April of 2004 through November of 2004. The Comptroller General, in his testimony before the Committee on Government Reform, House of Representatives, August 3, 2004 noted, "At the same time, some successes have occurred during the past two years that address process and technology concerns. For example, the Terrorist Screening Center, created under Homeland Security Presidential Directive 6 is intended to help in the consolidation of the federal government's approach to terrorism screening. This center has taken a number of steps to address various organizational, technological, integration, and other challenges, and it may serve as a model for other needed intra- and interorganizational efforts."

Because the TSC mission cuts across traditional boundaries between law enforcement, national security and homeland defense, the TSC embraces the uniqueness and expertise of the multi-agency participation. The distinct and exceptional proficiency, the culture of best practices and the wealth of contacts developed over years of law enforcement service that are brought together by personnel assigned to the TSC enable the TSC as an entity to break through long standing and difficult Government barriers as well as stovepipe operations which in turn fosters and encourages outstanding communication among the various agencies within the US which interact with the TSC.

It is noted that a tremendous amount of the DOJ/OIG audit is devoted to discussion of the Terrorist Screening Database (TSDB) 1A and 1B. The creation of TSDB 1A and 1B were part of a phased approach to developing a database which had never existed before in the history of the United States Government, that would meet the criteria outlined in Homeland Security Presidential Directive (HSPD) – 6, that is one that would maintain critical data to the defense of the United States that is thorough, accurate and current. As a part of that phased approach, there is no longer a TSDB 1A and 1B, but only TSDB. As such, much of the report is no longer relevant in the TSC's rapidly developing approach to consolidating the Government's approach to terrorism screening.

As part of the responsibility to maintain critical data that is thorough, accurate and current, the TSC has taken a large responsibility as mandated in HSPD-6. However, the responsibility is not the TSC's alone. HSPD-6 clearly calls for the participation of every relevant Government agency. HSPD-6 requires the heads of executive departments and agencies to the extent permitted by law to provide all appropriate Terrorist Information in their possession, and conduct screening at all appropriate opportunities.

Also, while privacy issues and redress procedures remain an integral part of TSC operations, the TSC will not establish an Office of the Ombudsmen for redress issues. The ombudsman function will be at the nominating agency level. Each agency that has nominated an individual for inclusion in the TSDB will ultimately be responsible for authorizing the continued inclusion or exclusion from the TSDB. The TSC's will establish a Redress office to coordinate and facilitate that process among and between Federal agencies in the most efficient and effective manner.

The TSC has expended maximum effort to ensure it provides excellent service to its customer base, the law enforcement population that encounters terrorists on a daily basis. In pursuit of that excellence, the TSC maintains a high standard of response to inquiry on terrorist identification. The TSC now averages a ten minute response time to those individuals who have encountered a known or suspected terrorist. This maximizes not only efficiency of operations, but provides an extra layer of safety to the law enforcement community.

In the Draft Audit Report, the DOJ/OIG made 40 recommendations to the TSC. Of the 40 recommendations, the TSC had already implemented 38. In addition, of the 38, 17 were in process prior to the completion of the DOJ/OIG audit of the TSC and were initiated

independently of the DOJ/OIG audit as a natural process of growth and maturity associated with a start-up operation that was not yet one year old. Of the remaining 21, all are expected to be fully implemented by the end of FY 2005. There were two recommendations with which the TSC did not agree and appropriate explanations are provided.

In summary, the TSC has: 1) implemented a viable strategy for accomplishing its mission; 2) effectively coordinated with participating agencies; and 3) is appropriately managing the terrorist-related information to ensure that a complete, accurate and current watch list is developed and maintained.

Background

The TSC was signed into existence by the President of the US on September 16, 2003. The mission of the TSC, understood by all participants, was to devote all available resources to prevent terrorist acts against the US through the consolidation of the government's approach to terrorist screening. The mission of preventing terrorist acts in the US defined every decision made in the initial year of operation and will continue to do so. As such, the focus of the TSC, with limited resources, staffing and funding, has been primarily related to the efficacy of operations first. All time, resources, and materials, as a matter of consequence, had to be devoted to ensuring that the TSC could perform effective screening of terrorists against a consolidated database of terrorist identifiers in the US, at its borders, and outside the US where appropriate. Every other aspect of operations was subordinated to this main focus. However, no aspect of appropriate screening operations was ignored or subverted; it simply maintained a lower priority than the actual support of operations to prevent terrorism against the US.

The team that initiated the start-up of the TSC was assembled and reported to the TSC, under the direction of TSC Director Donna A. Bucella in late October of 2003. Due to the urgency of the mission, the TSC was organized within 33 days of the initial team's formation and reporting dates. As a result of the deadline under which the TSC was mandated to be operational, it was understood by all parties associated with this task and mission that the TSC would operate within an initial operational capability (IOC) for a minimum of a year as the TSC invested what time and resources were available to design an appropriate information technology architecture, business processes to support that architecture and mission, as well as a plan to respond to the totality of requirements outlined in HSPD - 6 and its Memorandum of Understanding (MOU). During this year, the TSC, according to this concept, incrementally developed the areas in priority order that would assist the mission first and administrative concerns second.

The TSC was created in an out of cycle budget environment. As a result, the TSC did not have the opportunity to participate in the budget process initially, nor did it have the background to give a true estimate of normal operating requirements. Funding for the first fiscal year (FY) was reallocated from participating agencies' FY 2004 budgets. No personnel were granted to the TSC to stand up or operate it. Because the budget formulation process leads the execution phase of the budget process by two and one half years, the TSC was not able to have sufficient input into a budget cycle based on normative operational environment requirements until January of

2005, for the FY 2007 budget process, with the exception of a supplemental request for FY 2005 and an enhancement request for FY 2006. The first year that the TSC will have any opportunity to be granted personnel from the budget process is FY 2006, and it only addresses Federal Bureau of Investigation (FBI) personnel, not any of the other agencies since the budget is being requested through the FBI.

It is important to note that the TSC is a new concept and is a living and growing environment that is constantly evolving to meet emerging threats and requirements within the framework of its governing documents, HSPD-6, the MOU, and Addendum A. The TSC immediately developed an initial planning document and supporting Process Flows in November of 2003. These underlying support structures have formed the basis and the standard from which all evolutionary changes have been made to the TSC when it has been faced with new challenges, mandates, and unexpected events that impact the TSC's ability to prevent terrorist acts against the US. The TSC will never reach a stasis point where it has "arrived," or where it will not need to improve. To adopt that approach and mentality would be to concede defeat to the terrorists who will never stop trying to conquer the US, its allies, and the principles on which they were founded.

The DOJ/OIG formal on-site portion of the audit was concluded in November of 2004 less than one year after the TSC established initial operating capability. In this first year of operation, the TSC has accomplished significant achievements in the furtherance of defending the US from terrorist acts as it continues to improve, evolve and change to stay ahead of the expertise level and creativity of the terrorists who perpetuate that activity. Some of these milestones are detailed below:

Visa Revocation: The TSC initiated a Visa Revocation Project to identify known terrorists that may have entered the US on a valid visa, but were unknown to the FBI. This project was expanded to include any terrorist in the Terrorist Screening Database (TSDB) that may have entered the US, including through the visa waiver program. The TSC is vetting the entire TSDB against the Department of State's (DOS's) Consular Lookout and Support System (CLASS). In those instances where the location is unknown, the National Joint Terrorism Task Force (NJTTF) is coordinating efforts to locate them by setting out leads to JTTFs in the field. TSC is compiling a complete historical background on each of these subjects and providing the results to the NJTTF.

No Fly List: In 2004, after the DOJ/IG formal on-site portion of the audit was concluded, the White House Homeland Security Council (HSC) approved new criteria for inclusion of names on the No Fly and Selectee lists used for screening passengers on commercial airlines. The TSC identified the names of international and domestic terrorist subjects and prepared a spreadsheet detailing their current status on the lists. These lists contained over 7,000 names. The FBI JTTF case agent responsible for each terrorist subject on the list re-evaluated their No Fly/Selectee status. The review and re-evaluation was based on the new criteria and case agents changed the

subject's No Fly/Selectee status as appropriate. This effort ensured that with regard to all FBI subjects, their No Fly/Selectee status is consistent with the most recent criteria.

Associates Project: The Associates Project was developed to identify possible associates of known or suspected terrorists. During their normal course of duties, law enforcement officers, DOS officials and Border Agents encounter known or suspected terrorists in the TSDB from querying their case management systems during an encounter. These encounters provide valuable information which includes who the known or suspected terrorist is with at the time of the encounter. These encounters with possible associates will be documented and provided to the office of origin for appropriate action.

[SENSITIVE INFORMATION REDACTED]

Self Inspection Audit: The Director of the TSC directed and documented a self inspection of the entire TSC operation in December 2004. The main purpose of this self inspection was to ensure the TSC was meeting all of its mandates as detailed in HSPD-6.

Quality Assurance: TSC is in the process of conducting a manual review of every record listed in the TSDB. The results for each review will be documented and will ensure that there is adequate derogatory information to justify the inclusion of each subject as a known or suspected terrorist in the TSDB. In addition, TSC is modifying its nominations procedures to ensure that such a review also occurs at the outset for all new and modified nominations to the TSDB.

Liaison: The TSC Watch Commanders implemented a policy in which they meet on a monthly basis with Watch Commanders from the National Targeting Center (NTC) and Supervisory staff from TSOU/TSC Operations. TSC Call Center personnel interact hourly on a 24/7 basis with NTC and TSOU staff and these monthly meetings have proven invaluable in streamlining TSC's daily interactions with these two partner agencies.

Tactical Analytical Group: The Tactical Analysis Unit (TAU) was formed in May of 2004 and provides intelligence analysis for the TSC and documents the conducted analysis in a daily report which is distributed to the intelligence community and TSC's customers. TAU produces a daily report each work day. This report summarizes the TSC's positive encounters for the prior day. The Intelligence Cell within TAU summarizes the type of encounter, what occurred, and what action was taken. The report notes the subject's affiliation with any groups and a summary of the derogatory information available on the individual. Maps depicting the encounters and locations are also included in the report. The report is issued in two basic versions, International Terrorist only and International + Domestic Terrorist. The reports are disseminated by email to TSC's customers in the FBI, Department of Homeland Security (DHS), Transportation Security Administration (TSA), Central Intelligence Agency (CIA), DOS, National Counterterrorism Center (NCTC), Defense Intelligence Agency (DIA), Counterintelligence Field Activity (CIFA), Federal Air Marshals (FAMs) and the HSC at the White House. The principal analysis conducted by TAU is event based, not threat based. TAU maintains situational awareness of

domestic and world events and does not issue threat based analysis products. TAU has the additional responsibility of conducting analytical briefings for TSC Executive Management and groups that have a particular interest in TSC's analytical process or products. This information has never been previously created nor shared within the US Government.

HSPD-6 and Cooperation with Foreign Governments: The President on April 19, 2005, signed a proposal TSC co-authored with DOS on the U.S. government's strategy to boost cooperation with foreign governments in screening individuals for terrorism, a proposal required by HSPD-6. TSC has the lead on the U.S. side in negotiations with the G-8 nations (UK, Canada, France, Italy, Germany, Japan, and Russia) to establish a mechanism to exchange terrorist screening information. The proposal has DOS and TSC as the two key entities in establishing new relationships with foreign governments for the sharing of terrorist screening information. During the first year of operations:

- The DOS and TSC established a pilot program with the United Kingdom (UK) to exchange terrorist screening information. This test is likely the first of its kind between governments. This project has become a prime pillar of the work of DHS's US/UK Joint Contact Group, and garnered support and attention from high-level members of the Group. The results of the pilot revealed ways in which we can mutually strengthen our screening efforts.
- DOS and TSC are leading negotiations with **other** G-8 nations (UK, Canada, France, Italy, Germany, Japan, and Russia) to establish a mechanism to exchange terrorist screening information; the TSC designed the questionnaire to elicit information from foreign governments about their screening protocols, applicable laws, etc.

DOS Support: In addition to the cooperation with Foreign Governments, the DOS has also:

- Established performance measurements for the processing of visa applications and visa revocations and ensured they were followed. All visa revocation screening is promptly completed (zero tolerance for backlog) and visa application screening averages 3 days.
- Implemented expeditious nomination procedures. Now, new and urgent terrorist identities can be placed in CLASS 24/7.
- Improved frequency of exports. Exports of TSDB data to CLASS have increased from weekly to daily. Exports to certain foreign countries have increased from once a month to either once or twice a week.

System Engineering: TSC was provided initial information technology (IT) support by partner organizations. Over the course of the year, TSC has added system engineering capability, designed and implemented development, test, and training environments, and initiated participation in the FBI Enterprise Architecture development effort.

Application Development: In March 2004, an initial prototype system of the TSDB was deployed and populated with the terrorist identities from the watchlists identified by the General

Accounting Office. In June 2004, a sensitive but unclassified (SBU) version of the TIPOFF system was deployed at TSC and updates began to flow from the Terrorist Threat Integration Center (TTIC), which is now called the National Counterterrorism Center (NCTC).

Development was completed for the upgraded operational system (TSDB 1.1) in October 2004. This delivery increases the number of fields in the database to accommodate new types of identification data. TSDB Versions 1.1.1 through 1.1.4 were implemented to fix problems and improve data flow. Version 1.1.5, due to be installed in May 2005, will restore inter-system updating of TSDB to CLASS by correcting problems created in December 2004 when changes to CLASS by DOS rendered data modifications and deletes inoperable.

Re-design of TSDB to version 2.0 is being accomplished in stages by gradually incorporating capabilities developed to prepare for NCTC's implementation of the Terrorist Identities Datamart Environment (TIDE) program which will require TSC to stop using its TIPOFF-based TSDB. Database compatibility with TIDE will exist when TIDE becomes operational in 2005. TSDB's end-user interface will be re-designed to be TIDE-compatible, and access to additional fields of data cited in Addendum A to HSPD-6 will provided by December 2005.

The Encounter Management Application (EMA) was developed as a prototype and has been in production since July 2004. EMA supports the Call Center by tracking call-in encounters by law enforcement personnel; it also supports intelligence gathering and reporting.

IT Operations: [SENSITIVE INFORMATION REDACTED]

For SBU connectivity, each of the partner agencies has brought its system into TSC space and used those paths to pass data to and from the home systems. Purely unclassified connectivity is provided by the Techtrack system.

Project Management Office: The Project Management Office (PMO) was established in August 2004. PMO coordinates schedules for IT projects across the TSC in order to support effective operational capabilities and to improve this capability over time. The PMO does not directly manage projects, but fills a staff role in support of project managers. The PMO provides support for project initiation, portfolio management, master scheduling, project reporting, and weekly reviews.

The PMO also administers the TSC Configuration Control Board (CCB). The CCB is the entry point of new projects into the IT portfolio of TSC. It requires project initiators to explain and justify new initiatives. Existing projects that need to be re-baselined (redefined and/or re-launched) must justify the action and receive approval from the CCB. Members of the PMO support Special Projects as needed in concert with members from other segments of TSC.

Data Management Office: Given the goal of increasing TSC data accuracy, currency, and thoroughness while maintaining security, the CIO created a Data Management Office (DMO) in

March of 2005. The mission of the DMO is to create tools that help our substantive data owners increase the quality of TSC data.

The DMO is supporting the following activities: moving data from one security level or system to another; creating tools to monitor data as it arrives and moves to screening locations; creating reports to analyze data in TSDB and related systems; answering technical questions through analysis if database content; measuring the accuracy, currency, and thoroughness of screening data.

Legal Unit: The TSC established a Legal Unit in June of 2004, and to date they have:

- Prepared a non-disclosure agreement for the TSA-TSC MOU;
- Assisted DOS Deputy with drafting a letter of exchange for the U.S./U.K. pilot project and with reviewing Business Plan for US-UK data exchange;
- Assisted DOS Deputy in drafting a document to grant C-175 Circular Authority to DOS/TSC to enter into agreements with foreign governments on terrorist screening information sharing
- Assisted in drafting agreements regarding Non-Governmental Recipients of U.S. government funds, as per guidance from the National Security Council
- [SENSITIVE INFORMATION REDACTED]
- Constructed and executed an MOU with TSA for the Secure Flight test phase;
- Assisted the DOS with responses for two separate G-8 questionnaires;
- Completed a compilation of information from TSC staff necessary to finalize the Privacy Impact Assessment;
- Obtained call recording information from CJIS for comparison purposes for the TSC call recording project;
- Trained TSC employees on search parameters for TSC search of documents pursuant to a FOIA request received by FBI Headquarters (HQ) regarding the Secure Flight initiative and completed a search for documents and provided to the FBI's FOIA Unit for processing.

Training Highlights/Accomplishments:

- The TSC hired a Training Coordinator on December 1, 2004 and established formalized orientation to all TSC employees.

- Training needs were identified through the use of questionnaires and employee interviews. The results of the questionnaires clearly demonstrated the need for TSC Call Center training to be the number one priority.

- A 20 plus hour training syllabus was developed for TSC Call Center personnel.

- A training manual that incorporates the above information was created. This document is constantly evolving and is critiqued by the trainees as to relevancy and need.

- A regular schedule of "Information Presentations" that are designed to heighten the awareness of all employees in certain topic areas was instituted.

Privacy/Redress: An attorney from the TSA was hired to serve as TSC's first Privacy Officer in January 2005. Her role is to coordinate all matters related to privacy and redress. Since her hire, the Privacy Officer has been working toward the completion of key privacy compliance documents, including the Privacy Act notice and Privacy Impact Assessment. In late January, the Privacy Officer established a formal process to track and respond to all redress inquiries referred to TSC by other agencies. The TSC is also working to develop a consolidated government approach to helping individuals who are repeatedly misidentified during a U.S. government screening process.

The Privacy Officer also modified the Configuration Control Board process to require program managers to conduct an analysis of the privacy impact of any proposed new or modified IT project. The Privacy Officer will also regularly attend CCB meetings.

With this as a short summary background, the TSC offers the following in response to the DOJ/OIG Draft Audit of the TSC:

Recommendation #1:

That the TSC develop a formal IT plan for maturation of the IT environment at the TSC to address: a) IT staffing needs; b) controls to ensure data integrity; c) adequate oversight over IT contracts and contractors, and d) future improvements in the areas of TSDB connectivity, name-search capabilities, acceptance of biometric data, as well as other IT planning issues.

Response:

The TSC agrees with this recommendation, but has operated according to this recommendation since its inception.

a) The TSC developed an initial formal staffing plan in January of 2004. Due to the TSC's creation in an out of cycle budget environment, the FBI provided the majority of the TSC's permanent and temporary staffing. Within this initial plan, the TSC detailed IT staffing requirements from all participating agencies and contract employees. That staffing plan and the organization chart that it was initially derived from are included as TSC Response Exhibits (TSCREs) #1 and #2. The TSC used this initial staffing plan until it became apparent that the TSC's requirements would exceed its proposed staff. As a result, beginning in August of 2004, the TSC began work on a Master Staffing Plan, of which the IT staffing was an integral portion. This Master Staffing Plan was published via an electronic communication (EC) to the Director of

the FBI and other entities as of October 29, 2004 (TSCRE #3). The MSP is a living document that is updated as requirements dictate. Attached is the most current version of the MSP (TSCRE #4).

b) As part of its ongoing Strategic Planning, the TSC has developed three separate software products that will have a tremendous impact on the ability of the TSDB to add audit trails within the database, including historical data and detailed transactions by user, which will enhance human access controls. The first is the Nomination form Project, which is part of the TSDB v1.4 Project described below. The Nomination form is a manual form that is used by the FBI to nominate terrorists for inclusion in the TSDB through submission of the form to the FBI's Terrorist Watch and Warning Unit (TWWU). The Nomination form project automates that process and creates built-in audit capability. The Nomination form will require user login for traceability, it will track date, time, and the username of the last update made to any nomination. The Nomination form Project of the TSDB version 1.4 is scheduled for implementation in May of 2005. The second part of the TSDB v1.4 Project provides for web-based transaction processing of TSDB updates to NCIC's VGTOF file according to NCIC's protocol. It means that adds, modifications, and deletes to VGTOF will occur in real time with TSDB updates at TSC. Version 1.4 is scheduled to be operational at TSC on May 13, 2005. The third is TSDB v1.5, which will allow TSC to ingest data from NCTC's TIDE system (which is designed to replace TIPOFF) while maintaining TSC operations using TSDB. The TSDB 1.5 is currently installed at TSC's Independent Verification and Validation (IV & V) test lab while undergoing acceptance testing, but is dependent upon the NCTC's new TIDE software coming online and completing a rigorous testing phase. That is estimated to be finalized in July of 2005. NCTC advises TSC that they plan to make TIDE operational following a second round of NCTC/TSC acceptance testing scheduled for the week of May 9, 2005. TSC expects more testing will be necessary before TIDE is "hardened" sufficiently to replace TIPOFF. Either way, TSC will be able to receive TIDE exports and continue operating TSDB whenever TIDE is activated.

c) The TSC has four contracts which support IT, three of which are funded by the TSC through the FBI budget process. All contract work activity is reviewed by the TSC CIO, a 20 year IT professional renowned for his IT accomplishments at the Department of Defense. The first IT contract is a large personnel contract with an 8a contractor. This contract provides not only IT personnel but also Administrative and Operational personnel. This contract has a direct program contact at the company level, an on-site Program Manager (PM) located at the TSC, a Contracting Officer (CO) from the Department of the Interior, and an onsite FBI Contracting Officer's Technical Representative (COTR). The COTR maintains daily contact with the on-site PM. There are government employees who oversee the work of all the IT contract employees on the 8a contract.

The second contract is a software development contract. This contract has a direct program contact at the company level, an on-site program manager who splits time at the TSC and the software development offsite (the overwhelming majority of these employees are located offsite), an FBI CO, an onsite FBI COTR, and a FBI software development (SD) IT PM. The

FBI COTR has weekly meetings with the contract PM, and the FBI SD IT PM to provide appropriate direction to and control over the contract company with reference to current project work for the TSC. The FBI SD IT PM has daily contact with all the SD contract project teams. The SD contract has strict project plans, schedules and milestones that are reviewed regularly by the TSC COTR, Executive Management and IT government staff. Furthermore, the primary focus of the SD contract is the development of the TSDB. The TSC made a tactical decision to develop the TSDB on an incremental basis. As such, the TSC has been able to implement robust processes for requirements analysis and promulgation, development, testing, integration, and production that have greatly increased effectiveness of the TSC under tightly controlled circumstances.

The third contract is with a Federally Funded Research and Development Center. This contract provides the TSC with a secondary layer of control over its IT contracts. Experienced IT professionals from this contract have been integrated into the project management oversight to provide further safeguards from fraud, waste and abuse.

Finally, the DHS has provided the TSC with one contract IT employee for infrastructure support. This employee comes under the direct oversight and control of a 19 year FBI employee with 14 years of IT experience.

The TSC believes it has had and continues to exercise substantial and sufficient control over its IT contracts and personnel.

d) As noted above, the TSC made a tactical decision to develop the TSDB in an incremental fashion. This decision was made to ensure the TSC always maintained the ability, from its first day of operation, to provide an effective accomplishment of its mission. Incremental development ensures that systems are always functional with full available capacity as improvements are made gradually. As such, the IT management team, in association with the Executive Management of the TSC, has planned for multiple releases associated with the TSDB. In its Strategic Plan, the TSC has, from its inception, planned increased connectivity, search capabilities, and development of new capability derived from constant review of the TSC mission, function and requirements. Fruits of this planning have been evident with various releases of the TSDB since June of 2004, and continue with releases of TSDB 1.4 and 1.5 later in 2005.

The TSC notes that the DOJ/OIG Draft Audit references through most of the report that the TSDB was divided in two parts. This report was drafted based on observations made during the infancy stages of the TSC and there is one TSDB now.

Recommendation #2:

Enhance the TSDB to add audit trails to track activity within the database, including historical data and detailed transactions by user, as well as to include enhanced human access controls.

Response:

The TSC agrees with this recommendation and has been developing requirements and software to address this recommendation since November of 2004.

As noted in response to recommendation #1(b), as part of its ongoing Strategic Planning, the TSC has developed three separate software products that will have a tremendous impact on the ability of the TSDB to add audit trails within the database, including historical data and detailed transactions by user, which will enhance human access controls. The first is the Nomination form Project, which is part of the TSDB 1.4 Project, and was initiated November 8, 2004. The Nomination form is currently a manual form that is used by the FBI to nominate terrorists for inclusion in the TSDB through submission of the form to the FBI's Terrorist Watch and Warning Unit (TWWU). The Nomination form project automates that process and creates built in audit capability. The Nomination form will require user login for traceability, it will track date, time, and the username of the last update made to any nomination**.** The Nomination form Project of the TSDB 1.4 is scheduled for implementation in May of 2005. (TSCRE #5) The second is the National Crime Information Center (NCIC) Query Project portion of TSDB 1.4 which was initiated on December 13, 2004. (TSCRE #6) In this project, among other increased capability, the NCIC Query portion of TSDB 1.4 will allow for automated tracking of system transactions between the TSDB and NCIC. The NCIC Query TSDB 1.4 is scheduled for implementation in May of 2005. The third is TSDB 1.5, which was initiated December 15, 2004. (TSCRE #7) The TSDB 1.5 requires a transactional audit history of information flow from the NCTC and the TSDB. The TSDB 1.5 is currently in Independent Verification and Validation (IV & V) testing, but is dependent upon the NCTC's new TIDE software coming online and completing a rigorous testing phase.

Recommendation #3:

Develop staffing protocols to ensure that the TSC remains a multi-agency operation and make further efforts to encourage DHS to provide additional staff.

Response:

The TSC agrees with this recommendation and has operated according to this recommendation since its inception.

As noted in the response to recommendation #1, the TSC has been working from an initial staffing document authorization since January of 2004 (TSCRE #1 & #2), which was updated to the MSP as of October 29, 2004 (TSCRE #3 & #4). The MSP is a living document that is updated as requirements dictate. This document is the staffing protocol that governs the staffing of the TSC to include the levels of participation from other agencies.

With particular respect to the DHS, the Principal Deputy Director (PDD) of the TSC and Human Resources Specialist (HRS) of the TSC have periodically met with DHS's Chief Human Capital Officer, to further communication regarding staffing initiatives. To date, position classification actions have been completed for nine DHS positions and vacancy announcements have been drafted. The DHS has been unable to advertise these announcements due to Funded Staffing Level restrictions for FY 2005, since no participating agency was granted personnel to stand up or operate the TSC.

With these restrictions in place, the DHS prepared a memorandum under the signature of Susan Richmond, Chief of Staff for Janet Hale, Under Secretary for Management, requesting agencies that report to the Secretary of Homeland Security to provide staff positions to the TSC on a non-reimbursable basis for the remainder of FY 2005. (TSCRE #8) Further, each agency is responsible for keeping their assigned positions filled with detailees in future years on a non-reimbursable basis until such time as permanent positions are created and funded. Listed below are the positions the DHS will staff and by which agency the positions will be staffed:

BORDER AND TRANSPORTATION SECURITY (2 positions, 0 filled)

1. Management Analyst-Correspondence
2. Policy Analyst

CUSTOMS AND BORDER PROTECTION (6 positions, 1 filled)

1. Center Operations Specialist (2)
2. CBP Inspector (2)
3. Public Affairs Specialist
4. Management Assistant

CITIZENSHIP AND IMMIGRATION SERVICES (1 position, 0 filled)

1. Executive Secretary

EMERGENCY PREPAREDNESS AND RESPONSE (1 position, 0 filled)

1. Facilities Management Specialist

FAMS SERVICE (1 position, 0 filled)

1. Center Operations Technician

INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION (7 positions, 6 filled)

1. Principal Deputy Director

2. Management Analyst
3. Data Analysis Specialist (4)
4. Nominations Supervisor

ICE (4 positions, 1 filled)
1. Center Operations Specialist (2)
2. Center Operations Technician
3. ICE Representative/Agent

OFFICE OF GENERAL COUNSEL (1 position, 0 filled)
1. Attorney-Advisor

TSA (8 positions, 8 filled)
1. Director
2. Center Operations Technician
3. Privacy Specialist
4. TSA Representative (4)
5. Deputy Administrative Officer

US COAST GUARD (6 positions, 3 filled)
1. Center Operations Specialist (4)
2. Congressional Affairs Specialist
3. Budget Analyst

UNDER SECRETARY FOR MANAGEMENT (1 position, 0 filled)
1. Management Analyst-Statistics

US SECRET SERVICE (2 positions, 2 filled)
1. Center Operations Specialist (2)

Recommendation #4:

Take steps to increase the number of permanent government personnel and long term TDY staff employed by the TSC to take advantage of valuable expertise and institutional knowledge and to reduce the necessity of constant orientation and training.

Response:

The TSC agrees with this recommendation and has operated according to this recommendation since its inception.

The TSC has taken aggressive steps to increase the number of permanent and long term TDY personnel and further reduce the need for orientation and training. Due to the unique TSC

mission, at the time of the creation of the TSC, there had, obviously, been no position descriptions created, no vacancy announcements developed, and no postings advertised to fill permanent positions for the TSC. With respect to the FBI and contract hires, beginning in January of 2004, the TSC developed a full complement of position descriptions at multiple grade levels, created vacancy announcements and posted all positions. The TSC then conducted career boards according to merit promotion principles, screening hundreds of applicants, interviewing where appropriate, and making selections for each position, finally working with each candidate to obtain background data to facilitate appropriate investigations for the purpose of obtaining a Top Secret/Secure Compartmentalized Information clearance. The typical hiring time process for the FBI from the date of background initiation can take up to one year. With the initial process to develop the positions and select the candidates, the process can easily take over 18 months.

Even with these constraints, by the time of the end of the DOJ/IG audit, the TSC had a remarkable 73% of permanent staff on board in approximately 10 months. Since November 9, 2004, the TSC has advertised 13 Supervisory Special Agent (SSA) FBI positions. Of those positions advertised, three closed with no applicants applying for the vacancy, five are currently open and will close on April 29, 2005, one is pending with the Executive Development and Selection Program (EDSP) Section to be posted, and a local career board was conducted on March 28, 2005 for four SSA positions and recommendations were forwarded to the EDSP Section for final selection. To better meet the demands of the TSC, management reorganized its SSA positions during December 2004 (TSCRE #9) and April 2005 (TSCRE #10) to more evenly distribute assigned projects and responsibilities managed by the TSC and to capture individuals at the highest level possible that possess appropriate competencies. Through these reorganizations, two additional GS 15 SSA positions were established.

Since November 9, 2004, the TSC has increased its permanent FBI staff by five, with an additional four pending approval of a successful background investigation to complete the hiring process. Two professional support positions are currently posted and three posting requests are pending with the Staffing Unit. During November 2004, the FBI advertised a critically needed Policy Development Officer position. A local career board was conducted in December 2004 and a conditional job offer was made in early January 2005. The offer was accepted; however, the applicant later rescinded her acceptance of the position.

During December 2004, the TSC requested an increase in funded staffing level to support the permanent establishment of Intelligence Analyst positions (TSCRE #11). TSC continues to receive an increasing number of calls for identification as to whether the person encountered is a positive or negative identity match to a known or suspected terrorist. To provide adequate analysis, the TSC proposed that 28 Intelligence Analyst positions be established and added to the TSC staffing level. These positions would be supported and staffed by the following components: 6 FBI; 6 DHS; 4 DOD; and 12 from the Intelligence Community. The request for FBI personnel is pending with the Office of Intelligence for approval. A follow-up communication was prepared on January 14, 2005 (TSCRE #12), requesting the Office of

Intelligence detail six Intelligence Analysts to the TSC for a period of 90 days to augment the TSC's analytical staff until such time as the TSC could be sufficiently staffed with permanent Intelligence Analysts. Unfortunately due to a shortage of Intelligence Analysts within the FBI this request will not be filled until May of 2005.

On March 29-30, 2005, the HRS attended an OPM-sponsored job fair to recruit Presidential Management Fellows (PMF). The government-wide PMF Program is designed to attract outstanding young men and women from diverse academic disciplines to federal service. Prior to the job fair, the TSC reviewed hundreds of resumes. The TSC interviewed seven PMFs and provided three conditional job offers. Unfortunately, all offers were declined. On April 6, 2005, the TSC requested to hire 19 professional support positions over the current FBI funded staffing level to meet the increased workload associated with the Secure Flight program (TSCRE #13), which is scheduled to begin in August 19, 2005.

The DHS and its reporting agencies have contributed to the TSC employee complement by providing nine long-term TDY staff members since November 9, 2005. Refer to Recommendation #4 for further details regarding DHS's future staffing initiatives to support the TSC.

To further enhance multi agency operations and take advantage of valuable expertise, the TSC set forth a formal request on December 10, 2004 (TSCRE #14) to detail a military officer for a one year non-reimbursable tour of duty, with a possible extension, in conjunction with force protection in order to support the Global War on Terrorism. This employee maintains a Top Secret Clearance and recently received his pre-polygraph interview in order to receive indoctrination for SI/TK/G and HCS. It is anticipated that this employee will report to the TSC in 6/2005.

In addition, 16 contract employees have reported since November 9, 2004 to support the mission of the TSC. The TSC continues to interview viable candidates for various positions within the center and has three in background awaiting hire (TSCRE #15).

The TSC has also recently mandated that all temporary duty (TDY) employees report to the TSC for a minimum of 90 days to minimize the need for constant orientation and training. However, as of January 2005, the TSC also now has a robust training program that provides the TDY personnel with appropriate skills sets at a much higher rate than was possible in the past. As such, the potential negative effects on the TSC operations are essentially mitigated.

In summary, the TSC has always recognized the need for permanent or long term expertise skill levels and has aggressively pursued that goal since its inception.

Recommendation #5:

Ensure that the information placed into the TSDB accurately represents the data that was submitted by the nominating agency. In addition, the TSC should establish controls to ensure that it can trace the origin of the record to the nominating agency.

Response:

The TSC agrees with this recommendation and has taken appropriate action to address this matter beginning in November of 2004.

As previously noted, the TSDB 1.4 and 1.5 requirements phase were implemented in November and December of 2004. A substantial portion of these requirements addresses the need to ensure the TSDB accurately represents the data that was submitted by the nominating agency, and establish controls to ensure it can trace the origin back to the nominating agency. There are three important software development projects associated with the TSDB 1.4 and TSDB 1.5 that address these requirements. The first is the Nomination form Project (TSCRE #5), which is part of the TSDB 1.4 Project, initiated November 8, 2004. The Nomination form is currently a manual form that is used by the FBI to nominate terrorists for inclusion in the TSDB through submission of the form to the FBI's Terrorist Watch and Warning Unit (TWWU). The Nomination form project automates that process and creates built in audit capability. The Nomination form will require user login for traceability, it will track date, time, and the username of the last update made to any nomination. The Nomination form Project of the TSDB 1.4 is scheduled for implementation in May of 2005. The second is the National Crime Information Center (NCIC) Query Project portion of TSDB 1.4 which was initiated on December 13, 2004 (TSCRE #6). In this project, among other increased capability, the NCIC Query portion of TSDB 1.4 will allow for automated tracking of system transactions between the TSDB and NCIC. The NCIC Query TSDB 1.4 is scheduled for implementation in May of 2005.-

The third is TSDB 1.5, which was initiated on December 15, 2004 (TSCRE #16). The TSDB 1.5 requires a transactional audit history of information flow from the NCTC and the TSDB. The TSDB 1.5 requires the NCTC to pass message identification (ID), Nomination ID, Nomination Type, TIDE ID, and TIDE Alias Group ID, all of which are mandatory. All of these fields are used to trace the origin of individual records back to the nominating agency. Furthermore, TSDB enforces over 35 business rules in the receipt of data between NCTC and the TSDB. This helps ensure the accuracy of the data from the nominating agency as it applies specific system checks in accordance with the NCTC – TSC data agreement outlined in the Interface Control Document. The TSDB 1.5 is currently in Independent Verification and Validation (IV & V) testing, but is dependent upon the NCTC's new TIDE software coming online and completing a rigorous testing phase.

Finally, a major Quality Assurance (QA) effort (see response #10) is under way in TSC to ensure that records of highest priority for correction are addressed by a record-by-record search. This

QA effort will verify the data of historical TSDB data and allow new data quality to be controlled through the automated processes in TSDB 1.4 and 1.5.

Recommendation #6:

Take measures to automate the daily upload of records nominated for inclusion in the TSDB to reduce the need for human intervention.

Response:

The TSC agrees with the recommendation and has taken steps to implement it since December of 2004.

As noted above in responses to recommendations #2 and #5, when implemented as part of the TIDE project, TSC's TSDB 1.5 (TSCRE #16) will enforce more than 35 business rules to validate that data received from NCTC complies with legal and negotiated restrictions on data relationships. Examples of rules include changing exports of a record when a US person is inappropriately targeted for a foreign country's watch list, and when a person is placed on both the No Fly and Selectee lists. Current policy calls for visual examination of the individual record during ingest.

The real issue with timely and quality ingest relates to the multiple levels of security involved. The Intelligence Community (IC) has been working for years to develop a trusted guard to provide a network connection to move data from top secret to the sensitive but unclassified (SBU) level. Until this capability is available through the IC, TSC must live with significant delays in data arrival from NCTC, and poor data quality.

Recommendation #7:

Develop a more vigorous outreach plan that includes specific target organizations and industries, and establish timelines for the completion of outreach goals. Incorporate the plan into the TSC strategic plan, when formally created.

Response:

The TSC agrees with this recommendation and has complied with this recommendation since the inception of the TSC.

The TSC has had as part of its ongoing Strategic Planning, a clear structure and process for outreach from the TSC. To date, a TSC Video was developed and sent to law enforcement agencies all over the U.S. A TSC Brochure tri-fold (TSCRE #17) was developed and is used in every presentation opportunity to distribute to law enforcement officials all over the US. The TSC has written articles on the TSC and had them published in *The CJIS Link* (October 2004)

(TSCRE #18) and *Crime & Justice International* (March/April 2005) (TSCRE #19). Both have resulted in a number of calls to the TSC seeking additional information. The TSC also has a new DVD in production that will be completed in June 2005 for dissemination to law enforcement agencies all over the US and outside the US.

The TSC regularly trains FBI National Academy classes which are comprised of elite law enforcement officials from all over the world. The TSC participates in conferences for District Attorneys, US Attorneys, Task Forces, State-wide law enforcement conferences, Regional law enforcement conferences, National law enforcement conferences, and Department of Defense legal conferences. Through the use of targeted on-line searching, substantive law enforcement organizations have been located in all the states, and most have been contacted to explore the possibilities of speaking at conventions, conferences, or training sessions in an effort to touch all levels of law enforcement. In addition, thanks to the diverse sources of the TSC workforce, leads have been provided and used for conferences initiated by their agencies. As of April 20, 2005, presentations have been, or are scheduled to be, made in 27 states and the District of Columbia. Presentations outside the US have been made in Ottawa, Ontario, Canada, and London, United Kingdom (TSCRE #20).

For the future, the TSC has initiated a plan to ensure TSC presentations will be made in all 50 states. The TSC will also be involved in training Legal Attaches in all FBI Legats in the next year. The TSC will also be developing a website in for the FBI's Law Enforcement Online (LEO) system to host a TSC informational web site. As the LEO system is available to anyone involved in law enforcement, the TSC will post the Outreach schedule, and provide a forum for those who visit the website to contact the TSC to schedule other outreach opportunities.

As with other areas of operation of the TSC, there will never be a time when the TSC has completed its outreach goals. There will always be the need for not only initial training to every law enforcement component that interacts with the TSC, but also refresher training as the TSC continues to evolve. As such, the TSC will constantly review and revise it outreach goals on an annual basis in conjunction with its annual reviews of the Strategic Plan.

Recommendation #8:

Encourage the DHS to finalize guidelines to allow the TSC to begin regular screening for private sector organizations.

Response:

The TSC concurs with this recommendation and has complied with this recommendation as part of its mission under HSPD-6.

TSC initiated several meetings between DHS headquarters and its component agencies over the last six months in furtherance of this objective (TSCRE #21). DHS recognizes their

responsibility for this initiative and will focus on the critical infrastructure industries first. Per HSPD-6, the TSC is dependent upon the DHS to initiate and lead in this effort. To date, no current schedule exists for rolling out this effort, but the TSC is fully cognizant of its complementary role to the DHS in this effort and is fully engaged in giving encouragement to the process.

Recommendation #9:

Review the 1,200 TSDB 1A records that may require manual correction to ensure that these records are included in TSDB 1B, if appropriate.

Response:

The TSC agrees with this recommendation and has completed this task.

The TSDB was consolidated into one database on April 1, 2005. During the course of this consolidation, TSC identified approximately 1,200 records in the former TSDB 1A that needed to be examined for duplication and added to the official TSDB (previously referred to as TSDB 1B). On March 16, 2005, the TSC sent 1,183 TSDB 1A records to the NCTC for analysis and ingestion back into the TSC TSDB as necessary. On April 20, 2005, based on the NCTC record analysis, 1,131 former TSDB 1A records were transferred to the TSDB, with 52 duplicates identified that were not transferred (TSCRE #22). This task is fully completed.

Recommendation #10:

Review and correct the 31 duplicate records identified in the TSDB 1B.

Response:

The TSC agrees with this recommendation and has taken steps to complete it.

In the Draft Audit Report, the OIG has identified these 31 records as being part of a larger set of records associated with a large number of potentially duplicate records created with the transfer of the FBI's international terrorism records from the VGTOF to the NCTC. The TSC was aware of this issue previously and had independently conducted analysis to determine the source of these records. Through the analysis conducted at the TSC, this mass export of the FBI's international terrorism records to the NCTC was identified as occurring on August 3, 2004. In an effort to address the duplicate records and other QA issues with the TSDB, the TSC initiated a complete record-by-record review of the entire TSDB. With this process initiated in April, 2005, the TSC will review every record in the TSDB to identify and correct the duplicate record issue (TSCRE #23, #24).

Since the August 3, 2004, VGTOF records appear to be the cause of duplicate records, the TSDB QA review will begin with the review of approximately 18,500 records that resulted from this VGTOF transfer of records to the NCTC. The review is estimated to be complete by July of 2005. It is important to note, that although there are duplicate records present in the TSDB, this has not reduced the efficacy of the TSC screening processes.

Recommendation #11:

Review and correct the four records identified in the TSDB 1B as having duplicate TIPOFF record numbers.

Response:

The TSC agrees with this recommendation and has taken steps to complete it.

In the Draft Audit Report, the Inspector General has identified these four records as being part of a larger set of records associated with a large number of potentially duplicate records created with the transfer of the FBI's international terrorism records from the VGTOF to the NCTC. The TSC was aware of this issue previously and had independently conducted analysis to determine the source of these records. Through the analysis conducted at the TSC, this mass export of the FBI's international terrorism records to the NCTC was identified as occurring on August 3, 2004. In an effort to address the duplicate records and other QA issues with the TSDB, the TSC initiated a complete record-by-record review of the entire TSDB. With this process initiated in April, 2005, the TSC will review every record in the TSDB to identify and correct the duplicate record issue. (TSCRE #23, #24)

Since the August 3, 2004, VGTOF records appear to be the cause of duplicate records, the TSDB QA review will begin with the review of approximately 18,500 records that resulted from this VGTOF transfer of records to the NCTC. The review is estimated to be complete by July of 2005. It is important to note, that although there are duplicate records present in the TSDB, this has not reduced the efficacy of the TSC screening processes.

Recommendation #12:

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

Response:

The TSC agrees with this recommendation and has taken steps to complete it.

The Data Management Office (DMO) at the TSC was created in March of 2005 with the mission of creating tools that help increase the quality of TSC data. The DMO is creating structured

query language (SQL) and small-scale database tools to empower QA effectiveness. In addition, TSC is modifying the TSDB 1.5 software to accept the entire TSDB as a batch file. This will apply all of the TSC business rules envisioned for future ingests from the TIDE system against the existing stock of TIPOFF records. (TSCRE #24)

Recommendation #13:

Ensure that each record in the TSDB 1B can be traced to either the FBI or NCTC databases.

Response:

The TSC agrees with this recommendation and has taken appropriate steps to implement it.

In April 2005, this issue was discussed with the Branch Chief, Terrorist Identities Group, NCTC. He has agreed to provide the source of each record in the TSDB, since his computer database at the NCTC tracks the agency that provided all international terrorist information. This will also be captured in TSDB 1.5. (TSCRE #7)

The TSC Nominations Unit is responsible for inputting all Domestic Terrorism records in the TSDB and therefore will track this information.

Recommendation #14:

Establish codes that more accurately describe domestic terrorist activity, replacing the INA codes that are currently applied to domestic terrorist records.

Response:

The TSC agrees with this recommendation and has taken steps to implement it.

When the TIPOFF program resided at the DOS and the Immigration and Naturalization Service was placing TIPOFF lookouts in its database, the INA code was linked to the Immigration and Nationality Act as a reference for possible inadmissibility charges. Since the start of NCTC and TSC relations, however, the INA code has been used as a means to categorize the derogatory information associated with a subject. This code has been used regardless of citizenship or whether the subject is associated with international or domestic terrorism. The INA code is required for export to IBIS, the database operated by the U.S. Bureau of Customs and Border Protection. It should be noted however that INA codes are pre-9/11 screening tools. The INA code is but one factor in determining whether or not a person is a threat.

In October 2004, it was requested that three new INA codes be established for the sole purpose of describing domestic terrorist activity (TSCRE #25). These INA codes will be scheduled in a future release of TSDB.

Recommendation #15:

Review the INA codes applied to domestic terrorist records to ensure they properly reflect domestic terrorist activity.

Response:

The TSC agrees with this recommendation and has taken steps to implement it.

This issue will be addressed with the creation of three new INA codes, which were requested in October, 2004, to be established for the sole purpose of describing domestic terrorist activity (TSCRE #25). This should be scheduled in a future release of TSDB.

It will also be addressed with the previously referenced record by record review of the TSDB to include an examination of the INA codes for each record.

The INA code originated from the Immigration and Nationality Act as a reference for possible inadmissibility charges. Since the start of NCTC (formerly known as the Terrorist Threat Integration Center- TTIC) and TSC relations, however, the INA code has been used as a means to categorize the derogatory information associated with a subject. This code has been used regardless of citizenship or whether the subject is associated with international or domestic terrorism. The INA code is required for export to IBIS, the database operated by the US Bureau of Customs and Border Protection.

Recommendation #16:

Assign handling codes to all records within the TSDB that are exported to VGTOF, including the 336 records that we identified as lacking handling codes.

Response:

The TSC agrees with this recommendation and is taking steps to complete it.

The 336 records identified have been addressed. Also, as previously noted, in April of 2005 the TSC initiated a massive QA review of the entire TSDB. This review is being completed with the use of a form with multiple questions (TSCRE #23). The accuracy of the TSDB handling code (HC) issue will be addressed with question eight in the record-by-record review of the TSDB. Question eight states "Do all linked and unlinked TSDB records have the same VGTOF Handling code? (If no, explain discrepancies in the comments field.)." This question will

identify and correct all records that do not have an HC, as well as identifying and correcting conflicting HCs in linked records.

TSC has identified part of this issue because HCs for the DT subject records (with valid HCs) that were exported from VGTOF into the TSDB on October 9, 2004, inadvertently omitted placement of the HC into the VGTOF Export Eligibility HC box. This oversight was rectified in late-2004. In addition, there were approximately 60 subject records in VGTOF that did not contain a valid SubGroup (SGP), e.g., HC. These records were not previously entered by or reviewed by the TSC since they were pre-existing records from 2002. Upon the creation of HCs, the Criminal Justice Information Services (CJIS) Division coordinated the change of old/obsolete SGP data, (e.g., 'CNFDRT KNGT AMERICA*RLNC'), to the newly created HC data. These records were identified by the CJIS Division as not having responded to the CJIS's change request, and were modified appropriately by the TSC.

Recommendation #17:

Review and correct the inconsistent assignment of low-threat handling codes to records with “armed and dangerous” INA codes.

Response:

The TSC does not agree with this recommendation because there is no link with VGTOF Handling Codes (HCs) used to inform state and local law enforcement officers with the TIPOFF INA Codes used to classify the type of known or suspected terrorists.

The following information should serve to further clarify this for the DOJ/OIG. None of the four existing HCs are considered “low-threat.” In fact, HCs are not associated with threat levels. HCs provide instruction as to when the person is encountered, what action should occur. However, different thresholds must be met prior to the issuance of a particular HC to any IT or DT subject.

[SENSITIVE INFORMATION REDACTED]

All other subjects are reviewed and assigned a HC based on: a) the Case Agent's recommendation (or VGTOF Nomination Team recommendation for non-FBI IT subjects); and b) the quantity and quality of the biographical/identifying data submitted by the Case Agent (or NCTC, for non-FBI IT subjects). The lack or absence of quality biographical/identifying data would warrant consideration that the subject be placed into a HC4 status, rather than a HC3 status, depending on the HC recommendation submitted by the Case Agent. If a clear photograph or useful biographical/identifying data is not provided, attempts to efficiently and accurately conclude a positive or negative hit will be hampered. HC3 is where the majority of the persons are categorized.

The assignment of INA Codes is a means to quickly label the type of derogatory that exists for a subject. The "armed & dangerous" designation is an old carry over from when the TIPOFF program shared records with the Immigration and Naturalization Service (INS). The INS designated certain INA Codes, linked at that time to possible inadmissibility charges, to the Interagency Border Information System's "A&D designator." NCTC merely uses the INA Codes to categorize the derogatory information compiled on a particular person and label that person by assigning an INA Code. **While the INA Code assigned to a subject record is examined, it is a factor, but not a primary consideration in the review and assignment of a HC**.

Lastly, it should be noted that HCs are not assigned to subjects "according to the level of threat the individual poses," as is cited throughout the DOJ/OIG Audit Report. [SENSITIVE INFORMATION REDACTED]

Enclosures/Supporting Documentation:

-VGTOF Nomination Protocol (dated 02/25/2005) (TSCRE #26)

Recommendation #18:

Establish in TSDB 1B separate fields to identify [SENSITIVE INFORMATION REDACTED] and [SENSITIVE INFORMATION REDACTED].

Response:

The TSC agrees with this recommendation and this is complete.

In October of 2004, the TSDB Wedge Project was placed in production. This project was specifically designed to address all fields in TIPOFF that could be exported from the NCTC, but could not be held in the TSDB. Of these fields, [SENSITIVE INFORMATION REDACTED] and [SENSITIVE INFORMATION REDACTED] were included. As such, this item has been completed since August of 2004. (TSCRE #27)

Recommendation #19:

Enhance the TSDB 1B by ensuring that available all fields of information have been activated and populated as appropriate.

Response:

The TSC agrees with this recommendation and has completed this action.

Per recommendation #18, and the response to that question, the TSDB Wedge Project was completed in August of 2004. All appropriate fields have been activated and populated as

appropriate. The only fields not activated and populated to date are those associated with the TIDE implementation, which will export all Addendum A material, and will occur later in 2005. (TSCRE #27B)

Recommendation #20:

Implement automated procedures to ensure records and corresponding data transmitted to and from the TSDB is accurate, consistent, and complete. This should include a review of the eight VGTOF records and the three TIPOFF records that were omitted from the TSDB 1B and the two TIPOFF records omitted from the TSDB 1A.

Response:

The TSC agrees with this recommendation and has taken steps to complete this action.

The previously referenced record by record QA review of the TSDB (TSCRE #23, #24), initiated in April, 2005, will address "the eight VGTOF records and the three TIPOFF records" that were not in TSDB 1B. This review is expected to be complete in June of 2005. It is also noted that there is no longer a TSDB 1A and TSDB 1B, but only a TSDB.

For information to be "accurate, consistent and complete," the TSC relies on the input from the nominating agencies. It should be noted that all Intelligence Community and law enforcement agencies are reviewing all of their record. Quality assurance is a shared responsibility and does not belong to the TSC alone.

With regards to automated procedures to ensure "accurate, consistent, and complete" data transmission to and from TSDB, TSDB 1.5 will help to ensure data integrity with built-in protections and buffers. When implemented as part of the TIDE project, TSC's TSDB 1.5 will enforce more than 35 business rules to validate that data received from NCTC complies with legal and negotiated restrictions on data relationships. Examples of rules include changing exports of a record when a US person is inappropriately targeted for a foreign country's watch list, and when a person is placed on both the No Fly and Selectee lists. Current policy calls for visual examination of individual record during ingest.

The real issue with timely and quality ingest relates to the multiple levels of security involved. The IC has been working for years to develop a trusted guard to provide a network connection to move data from top secret to the SBU level. Until this capability is available through the IC, TSC must live with significant delays in data arrival from NCTC, and poor data quality.

Recommendation #21:

Work with partner agencies to establish data field definitions and consistently apply them within all coordinated databases.

Response:

The TSC agrees with this recommendation and has taken steps to implement it, and will be the first and only entity to date interacting with the IC to use the new standard.

The Terrorist Watch Person Data Exchange Standard (TWPDES) was adopted by the IC Metadata Working Group (ICMWG) and incorporated into the data flow from NCTC to TSC. TWPDES is being integrated with the Justice Global Information Sharing XML 3.0 standard, but will remain a named subset of data. With the implementation of TSDB 1.4 in May of 2005, the TSC will be the first entity to use this standard in any interaction with the IC. (TSCRE #'s 5, 7, & 28)

Recommendation #22:

In coordination with the supporting agencies, establish procedures to identify and resolve missing and conflicting record information.

Response:

The TSC agrees with this recommendation and has had procedures to identify and resolve missing and conflicting record information since its inception.

To date, the TSC has completed a review of and corrected approximately 18,744 records. These records include 854 referrals from the EMA since May, 2004; 1,132 records transferred from the old TSDB 1A database to the current TSDB in April, 2005; about 6,000 VGTOF records reviewed and reconciled since April, 2004; about 1,800 Chechen Suicide Bomber records applied to the appropriate No Fly/Selectee list in September, 2004; about 50 INA records reviewed in January, 2005; 1,408 No Fly/Selectee records for possible duplication in December, 2004; and the March/April, 2005 review of over 7,500 FBI cases to apply the new White House No Fly/Selectee criteria.

The Nominations Unit at TSC has weekly meetings with NCTC and regular telephonic contact with the Terrorist Watch and Warning Unit, FBI Counterterrorism Division (CTD); TSOU, CTD; the NTC, Customs and Border Patrol, DHS; TSA, DHS; and NCTC to resolve missing and conflicting records. In addition to this liaison, the record-by-record review of the TSDB will identify and correct missing and conflicting records.

The Nominations Unit has a QA component that provides the following procedures for handling TSDB discrepancies:

Current Procedures for handling QA Matters at the TSC: Daily Call Center Reports are submitted to QA. Pages needing Quality Assurance Review (QAR) are tagged for QA. Copies

of tagged pages are duplicated and subsequently logged onto a separate spreadsheet. Copies are maintained in folders in date order until resolved and then archived alphabetically. Call Center Reports are analyzed to determine the type of matter needing resolution. The appropriate databases are queried and contact is made with appropriate sources to verify/resolve each QA matter. All measures taken to resolve each QA matter are logged onto a separate activity log for statistical purposes.

Computer Modifications requested to manage QA matters: QA worked with an FFRDC (June/July 2004) to document requirements to modify TSC's existing Encounter Management Database. Additional meetings transpired April 2005. The modifications will allow QA Matters to be submitted to QA personnel electronically. A separate QA screen will be established and fields added to better monitor, track and quantify QA Matters. The following are computer requirements discussed and requested:

- Ensure ability to view information previously entered by Call Center.
- Create a separate QA screen.
- Add field to reflect date received in QA.
- Add pick list to reflect type of QA matter to be resolved.
- Add field to reflect actions taken to resolve QA matter, Points of Contact (POCs), telephone numbers, calls, emails, etc.
- Add field to reflect final resolution.
- Add field to reflect date of final resolution.
- Ensure ability to query by name.
- Ensure ability to query by Service Request Number (SRN).
- Ensure ability to run reports (a) Pending QA matters alphabetically; by SRN; and for a specific time frame (b) Closed QA matters alphabetically; by SRN; and for a specific time frame (c) All inclusive (pending or closed) for a specific time frame.

Types of QA matters received: QA receives a variety of matters to research and resolve. Although there is no limit or way to predict the types of matters QA will encounter in the future most received to date have fallen into specific categories as listed below:

- Review of Violent Gang and Terrorist Organizations File (VGTOF) records to verify existence; coordinate removal; or to resolve errors or discrepancies.

- Coordinate with Customs and Border Patrol (CBP) the review of Treasury Enforcement Communications System (TECS) records to verify existence; removal; or correction of errors or discrepancies.

- Coordinate with TSA the review of NO FLY records to verify existence; removal; or correction of errors or discrepancies.

- Coordinate with TSA the review of SELECTEE records to verify existence; removal; or correction of errors or discrepancies.

- Review of NCTC TIPOFF records to verify existence and status of records; coordinate through NCTC the possible entry or removal from exports and/or archiving of records if warranted.

- Review of TSDB records to verify existence of records; or to coordinate with TSC the entry, removal or correction of records.

- Ensure NICS inquiries logged properly for statistical purposes.

Current procedures for resolving QA matters: The following are newly established procedures for resolving the aforementioned QA matters. Each QA matter is unique in nature therefore the below are simply guidelines:

- VGTOF records: Upon receipt the TSC Call Center sheet is reviewed to determine the type of matter needing resolution. The QA matter is subsequently logged onto a spreadsheet for tracking purposes. QA queries NCIC for current VGTOF status. QA queries the FBI's matter tracking system, ACS, for all references to subject. QA coordinates with record owner (ORI/FBI case agent) the entry, removal or correction of the VGTOF entry via telephone and email. The TSC is ORI for all VGTOF entries and initiates the modifications when warranted. Electronic Communications (ECs) are generated when necessary. All VGTOF modifications are confirmed by a subsequent query of NCIC/VGTOF records. Upon verification the QA matter is closed and archived. All subjects removed from VGTOF are logged onto a spreadsheet for statistical purposes. The names of all International Terrorist subjects removed from VGTOF are forwarded to NCTC for review and archiving if warranted.

- TECS Records: Upon receipt the TSC Call Center sheet is reviewed to determine the type of matter needing resolution. The QA matter is then logged onto a spreadsheet for tracking purposes. QA contacts TSC's CBP representative for a copy of the TECS record. In addition CBP provides the email address of record owner. QA reviews the TECS record. Contact is made with the appropriate authority, FBI, ICE or CBP for record modification if warranted. The matter is closed subsequent to contact with the record archived.

- NO FLY Records: Upon receipt the Call Center sheet is reviewed to determine the type of matter needing resolution. The matter is subsequently logged onto a spreadsheet for tracking purposes receipt. All QA matters pertaining to the review and modification of NO FLY records are forwarded to TSC's TSA representative(s) for review and action. Upon receipt of final resolution from TSA the QA matter is closed and archived.

- SELECTEE Records: Upon receipt the Call Center sheet is reviewed to distinguish the type of matter needing resolution. The matter is logged onto a spreadsheet for tracking purposes. All QA matters pertaining to the review and modification of SELECTEE records are forwarded to TSC's TSA representative(s) for review and action. Upon receipt of final resolution from TSA the QA matter is closed and archived.

- TIPOFF Records: Upon receipt the Call Center sheet is reviewed to discern the type of matter needing resolution. The QA matter is subsequently logged onto a spreadsheet for tracking purposes. QA queries TIPOFF database to determine current TIPOFF status. QA queries ACS for all references to the subject. QA coordinates with NCTC's POC for entry, removal or correction of TIPOFF records where needed via telephone and email. ECs are generated where appropriate. Upon final resolution and notification from NCTC, the QA matter is closed and archived.

- TSDB Records: Upon receipt the Call Center sheet is reviewed. A determination is made as to the type of matter needing resolution. The matter is then logged onto a spreadsheet for tracking purposes. QA queries the TSDB database to determine current TSDB status. QA queries ACS for all references to the subject. QA queries TIPOFF to compare all references to the subject. QA coordinates the entry, removal or correction of TSDB records where needed. Upon final resolution the QA matter is closed and archived.

- NICS Records: Upon receipt of Call Center sheet the matter is reviewed to discern matter needing resolution. The QA matter is subsequently logged onto a spreadsheet for tracking purposes. QA's initial responsibility regarding NICS matters is to ensure that NICS related calls are properly logged into the Call Center's database as a "NICS" matter for statistical purposes. If removal from VGTOF is warranted, QA handles same. No further action needed for NICS related matters.

Project initiated to review all records contained in TSDB for accuracy: The TSC is in the process of launching the TSDB QATracker Project. This project will identify inconsistencies within TSDB. Once the inconsistencies are identified, QA will work to resolve same. This project will enable the TSC to work in a pro-active manner versus a reactive manner. (TSCRE #23, #24)

Recommendation #23:

In coordination with the TWWU, streamline operations to ensure nominations are made to the appropriate system in a timely manner and in accordance with HSPD-6 so that domestic terrorist records are not forwarded to the NCTC.

Response:

The TSC agrees with this recommendation and has taken the appropriate steps to resolve this issue.

The VGTOF Nomination Team has addressed this issue with the TWWU on numerous occasions, most recently during a face-to-face meeting held at the TSC on April 5, 2005. While there has been a noticeable difference in the length of time it takes for the TSC to receive DT nomination paperwork from the TWWU, primarily because the TWWU had not worked through their backlog of paperwork, there will always be a gap in the time the Case Agent prepares and submits the nomination paperwork until the time that the TSC receives it. This delay can be days and, as seen in some cases, weeks.

The TSC continues to receive, on a regular basis, IT nominations from the TWWU, as well as receiving DT nomination paperwork and discovering that the same paperwork was forwarded to the NCTC, in error, for entry into TIPOFF.

The TWWU continues to assert that they review and direct IT and DT nominations to the best of their ability, but that the volume of paperwork they receive makes contributes to the lack of 100% accuracy difficult. Other incidences of confusion within the TWWU regarding the handling of DT nominations have also been addressed with them. The TWWU has advised that each nomination packet is reviewed by a supervisor prior to being forwarded to the TSC or the NCTC.

The VGTOF Nomination Team at the TSC has suggested that one of the members of the Team be "detailed" to the TWWU to ensure the proper review and flow of DT nominations; however, the TWWU responded that they did not believe that it was necessary.

The electronic version of the Nomination form will be disseminated throughout the FBI and to the Intelligence Community. With respect to the FBI, all Terrorism cases will be electronically moved from the FBI Field Division to the TWWU for review, with the International Terrorist cases being forwarded to the NCTC for processing and ingesting into the TSDB. The Domestic Terrorist cases will be forwarded to the TSC for direct input into the TSDB. This electronic format will allow for a more thorough electronic examination of each Nomination form to ensure that the 266 FBI classifications for Domestic Terrorist cases are not forwarded to NCTC. Only the 315 FBI classifications for International Terrorist cases will proceed to the NCTC.

It is anticipated that with the implementation of TSDB 1.4, particularly the Nomination form Project, this will relieve 100% of the errors being made through the paper manual process in place now. TSDB 1.4 is scheduled for implementation in May of 2005.

Enclosures/Supporting Documentation:

-E-mails dated 11/17/2004 and 11/18/2004. (TSCRE #29)

-E-mail exchange dated 03/17/2005 and 3/18/2005. (TSCRE #31)

Recommendation #24:

Establish procedures to regularly review the DOS's List of Terrorists under Executive Order 13224 to ensure individuals are accurately included in the TSDB.

Response:

The TSC agrees with this recommendation and has completed this action.

The "DOS's List of Terrorists" referred to in this recommendation is likely the list established by Executive Order 13224 (TSCRE #32) of September 23, 2001 on "Blocking Property and Prohibiting Transaction with Persons Who Commit, Threaten to Commit, or Support Terrorism." This Executive Order authorizes both the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, or the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General, to designate individuals and entities pursuant to specified criteria. Once the Secretary of State or the Secretary of the Treasury designates an individual or entity, the Office of Foreign Assets Control (OFAC) of the Department of the Treasury takes appropriate action to block the assets of the individual or entity in the US or in the possession or control of U.S. persons, including notification of the blocking order to US financial institutions, directing them to block the assets of the designated individual or entity. This list is publicly available online at www.ustreas.gov/offices/enforcement/ofac/sanctions/terrorism.html.

HSPD-6's accompanying MOU, paragraph 10 states, "The TTIC database will include, to the extent permitted by law, all information the U.S. government possesses related to the identities of individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism, with the exception of Purely Domestic Terrorism Information." Paragraph 11 further states, "…Federal departments and agencies will provide to the TTIC on an ongoing basis all relevant Terrorist Information in their possession, custody, or control…" TSC management met with the management team from OFAC in the winter of 2004 and informed them of their responsibility to provide this information to TTIC. As TTIC is now the NCTC, TSC executive management has confirmed that OFAC regularly provides its updated list to NCTC for analysis and possible inclusion of identities contained within it in NCTC's identities database, which is the source of all International Terrorist identities contained in the TSC's TSDB.

Recommendation #25:

Establish supervisory controls to ensure that the work of the Call Center personnel is reviewed on a regular basis for completeness, accuracy, and timeliness.

Response:

The TSC agrees with this recommendation and has implemented procedures to correct this concern.

The DOJ/OIG Draft Audit report indicated that the TSC's response time to terrorist encounters was on the order of 20 minutes. This is no longer the case. The TSC now responds to law enforcement officials who have potentially encountered a known or suspected terrorist in approximately 10 minutes (average). This is due to a number of factors.

In October, 2004, six permanent TSC Call Center employees, all with experience in reviewing the documentation of other screeners for completeness, accuracy and timeliness were designated as team leaders. These team leaders are the supervisors of a particular shift and all documentation regarding a call/encounter is reviewed by them. The team leader also has the responsibility of ensuring all of the documentation is completed prior to disseminating the information to TSOU, the NTC and other law enforcement agencies. To further establish supervisory controls, in November 2004, TSC hired five Watch Commanders, all with experience in various crisis centers, to oversee the operations in the TSC Call Center and a permanent GS-15 FBI Unit Chief arrived in January 2005.

Since December 2003, the TSC Call Center was supervised by TDY FBI agents who possessed various backgrounds, but minimal counterterrorism experience. Upon their arrival, these agents were provided no formal training and were expected to quickly adjust to the informal protocols of the TSC. Often, these agent supervisors never screened a call/encounter, resulting in a lack of knowledge and understanding of what is required to conduct a complete, accurate, and timely call. The lack of experience in working with the various databases also proved to be a problem for the supervisory agents, without the understanding of how to navigate the databases to locate pertinent information needed to make a timely decision and created an extended turnaround times for the caller. The majority of the calls resulted in the TSC forwarding the encounter as inconclusive to TSOU. This resulted in TSOU having to provide redundant checks to make an identity match. As the TSC expanded, it was apparent that the permanent screeners had more knowledge than the TDY agents, who where continually being rotated in and out of the TSC. The agents were relying on the expertise of the veteran screeners, to include their training and reviewing of calls for accuracy. The need for permanent team leaders to review TSC Call Center work product was evident and based upon these facts, TSC executive management approved the designation of team leaders. (TSCRE #33)

Recommendation #26:

Establish protocols for the proper entry and review of data into the Encounter Management database.

Response:

The TSC agrees with this recommendation and has established procedures to address it.

In view of the time constraints experienced by TSC's executive management to ensure the TSC was operational, there was no formal standardization of procedures implemented for EMA. Since its inception, TSC relied upon TDY FBI agents, US Secret Service, US Coast Guard and contract employees in order to identify the proper way of handling incoming calls from the field. Within a short time frame, TSC and the veteran employees began building their own Standard Operating Procedures (SOPs) for handling calls and how the information would be captured. The TSC Call Center management restructured the log sheets to ensure there was gathering of better quality information/data.

In July 2004, the previous Oracle based encounter management system was replaced with EMA to better fit the growing needs of the Call Center. Over the past eight months, TSC has implemented a training program that allows for the EMA training of each Call Center employee. The training module includes a specific section on EMA which details the information a screener needs in order to fill out and complete a call sheet accurately (TSCRE #34). It also encompasses a PowerPoint training guide (TSCRE #35) that walks the employee from opening the database, to finalizing an entry into the application. Upon completion of the training course, the employee is provided a copy of the training received and it is made available on the shared drive for further review. If a deficiency is determined, the employee is provided with additional training that allows the employee the ability to better learn the information, ask additional questions and address the deficiency. There is a proficiency check sheet that allows the team leaders and watch commanders the ability to track the progress of the employees and to identify any further deficiencies.

When a call arrives into the TSC Call Center, the employee takes the information. The employee runs both individuals (traveler and preliminary match) through four systems after the TSDB for derogatory information including Automated Case Support (ACS), NCIC, TIPOFF, and EMA. The employee treats the information as two separate individuals and makes an identity match based upon the information derived from the database checks. Considering most of the information being reviewed is classified, only the information that is deemed unclassified can be placed on the call sheets. To ensure only unclassified information is entered on the call sheets, security policies are addressed during training and all databases are marked with the level of classification it holds. Once the employee has made an identity match, the employee will take the call to the team leader and they will decide whether it is a positive, negative or inconclusive match.

If the match is positive, the call is sent via fax to TSOU and they will act as the liaison between the field offices to assist the case agent in their requests. If the call is a negative match, the caller is advised of the results. If it is inconclusive, the employee and team leader will collectively use the information located in the databases to formulate questions, without revealing classified

information, which will assist in resolving the identity match. Once the identity match is made and notifications are made to the appropriate personnel, the employee will then make the entry into EMA. When the entry is completed, the employee provides the sheet to the team leader to review for accuracy and ensure that no classified information was entered into the system. With the current system of veteran team leaders' review, there is minimal opportunity for classified information to be entered into the system. Once the team leader has reviewed the information in EMA, it is left as pending until there is a final resolution from the agency handling the call. The log is then updated and closed out. In addition, SOPs have been created for the various TSC Call Center special projects to ensure that all employees are familiar with the project and that they understand how to proceed with the project. These SOPs have been provided to the employees and have incorporated into the training process.

Recommendation #27:

Develop an automated method for flagging records in the Encounter Management database that require follow-up actions, and establish procedures to complete the necessary follow-up conducted within a reasonable period of time.

Response:

The TSC agrees with this recommendation and has taken steps to address it.

As discussed in response to recommendation #22, in the portion titled "Computer Modifications requested to manage QA matters," the QA section has requested specific changes to the EMA system to enable automated flagging of encounters for QA follow-up, and electronic tracking of QA matters in EMA or another appropriate application. The TSC has developed a system to prioritize encounters in EMA by assigning Zones to the type and urgency of the possible match. Calls will be ranked by Zone 1 to Zone 5 with Zone 1 being the highest priority. The TSC is in the process of having these zones automatically assigned in EMA as soon as an encounter is entered. As part of this new release, an enhancement to tracking encounters in progress, and encounters needing following up action by units at the TSC, other than the TSC Call Center, is being developed. These are part of the numerous requirements be addressed in EMA, Version 2.0. By using Zones, should there be a specific threat, the system is more flexible and agile to respond to the varied threats.

As also discussed in response to recommendation #22, the QA staff has developed procedures to process QA matters and complete follow-up for all such matters in as timely a fashion as resources currently permit. The QA section intends to establish a formal SOP documenting these procedures this year.

Recommendation #28:

Establish regular training for Call Center screeners to keep them informed of the proper approach to screening subjects in the database and providing information to TSOU, as well as for the entry of appropriate data into the unclassified database.

Response

The TSC agrees with this recommendation and has completed this item.

Prior to December 1, 2004, the position of Training Coordinator for the TSC was vacant and the position was filled by temporary, TDY personnel. Training up to that point was basically conducted "on-the-job" in the TSC Call Center, with no formalized training program in place. On December 1, 2004, a retired FBI Special Agent with extensive teaching experience at the college level, as well as at the FBI Academy, was hired to coordinate the TSC training program. On April 1, 2005, a training assistant was assigned full time to assist the training coordinator. Since December 1, 2004, the following accomplishments have been recorded.

Specific training needs were identified through the use of questionnaires and personnel employee interviews. The results of the questionnaires clearly demonstrated Call Center training, to be a top priority for the TSC.

As a result of this feedback from the questionnaires, a 20 plus hour training syllabus was developed and implemented for TSC Call Center personnel (TSCRE #36). No employee begins work in the TSC until he or she has completed this training. Included in this syllabus is a mandatory Information Security (INFOSEC) briefing; an Overview of the TSC- History and Operations; as well as blocks of instruction on the Nomination process; Intelligence flow process; Outreach/Customer Service responsibilities; NCIC/VGTOF Overview; as well as the EMA, TSDB and TIPOFF data bases. Incorporated in this training is one day of hands on computer work, using specific role playing scenarios that were drafted to mirror live call situations that the trainees will encounter in the Call Center. After the classroom phase of training, the new Call Center employee is assigned to an experienced Call Center operations specialist, for two days of hands on "mentoring."

It should be noted that a dialog with TSOU is on-going. If a specific training need is identified or specific "refresher" training needs to be conducted, it will be addressed on an immediate basis.

After an employee begins work in the Call Center, they are assessed by their team leader as to their skill development. If they have not attained proficiency in the basic skill areas identified for the Call Center, they return to training to address their deficiencies.

Since the inception of this program approximately 60 TDY and new employees have gone through this program. Feedback from these individuals is used to continually assess training and to add or delete modules, when appropriate.

"Refresher" or "advanced" data base training was also provided and scheduled for Call Center employees. Training on NCIC was given by trainers from CJIS and ACS training was provided by representatives from the FBI Academy, Quantico, VA. Additional ACS training is scheduled for April 21, 2005, for Call Center employees, as well as Intelligence Branch employees.

A schedule of "Informational Presentations" that are designed to heighten the awareness of all employees in topical areas related to the war on terrorism was also implemented. To date, the TSC has had approximately twelve presentations. Examples of topics include "How a name gets on the Watch List; "Document Classification Rules and Regulations"; an "Overview of the NTC"; an "Overview of the NCTC"; an "Overview of the FBI Counterterrorism Division"; "Sunni Extremists in the U. S."; "The threat of al – Qa'ida"; and "Arabic Names and How They Relate To The Mission of the TSC", etc. These presentations are provided approximately three times a month by subject mater experts, and are open to all employees of the TSC.

Recommendation #29:

Establish and implement an automated system for tracking the amount of time that elapses between the key events of an encounter, such as when the TSC receives a call, when the call is forwarded to TSOU, the amount of time before instructions are provided to the caller, and the amount of time before a call is resolved.

Response:

The TSC agrees with this recommendation and has taken steps to address it.

The TSC has identified the need to track these timelines in order to provide the best service to TSC customers. The TSC has begun to analyze the scope of work in order to provide these statistics as part of the EMA Case Disposition and Tracking System. Expected implementation date should be within the next six months.

In addition to the above initiative, the TSC is developing an automated system to prioritize encounters within EMA by assigning Zones that reflect the type and urgency of the encounter. Calls received at the TSC will be triaged by these Zones. These changes are part of the numerous requirements being addressed in EMA, Version 2.0.

Recommendation #30:

Establish an automated method for the entry of call data and the sharing of such data with TSOU to eliminate the redundancy of recording call information on the Call Intake Form and in

the Encounter Management database, and to reduce the time it takes for TSOU to receive the data and initiate further actions necessary.

Response:

The TSC agrees with this recommendation and has taken steps to address it.

The TSC has taken steps to address this issue by placing the database the TSC uses to track encounter information, EMA on a local TSC FBI network. The TSC is prepared to place EMA on a global FBI network. This will allow the TSOU to access the same information the TSC has on a real time basis. However, the TSC cannot proceed with the full implementation of this plan until the TSC is migrated to the TRILOGY system designed for universal use within the FBI. Once the TSC has TRILOGY installed (expected timeframe is June 1, 2005), the TSC will be able to effectively have EMA accessed by any computer in the FBI network.

Recommendation #31:

Assign a full-time security officer to handle security requirements and provide the TSC staff guidance and training on the proper handling of national security information.

Response:

The TSC agrees with this recommendation, but has operated to fulfill this recommendation since its inception.

As the TSC was brought to initial operating capability, the Counterterrorism Division (CTD) assigned a Security Specialist (SS) to the TSC as the Security Officer (SO). The TSC was assigned a long-term TDY employee to address personnel security matters in January of 2004, Personnel Security Specialist (PSS). In March of 2004, the TSC SO was replaced by an FBI Supervisory Special Agent (SSA). Also in March of 2004, the TSC hired an FBI Information Systems Security Manager (ISSM), and a TSC Information Systems Security Officer (ISSO). In April of 2004, the FBI SSA was transferred to another FBI Field Office and the PSS was assigned primary responsibilities for the Security Officer of the TSC.

Due to the transfer of the FBI SSA, and the lack of ability for the CTD to assign an onsite SO, the CTD authorized the posting of a Security Specialist for the TSC, which was accounted for in the initial staffing authorization in January of 2004. As a result, on June 3, 2004, a vacancy was posted for a full time SS to act as the SO for the TSC. This position was career boarded on July 16, 2004, and interviews were conducted in July, with primary and alternate selections made on July 28, 2004. Candidates were placed into background after receipt of their FD-140 applications.

In October of 2004, the TSC hired a Management Assistant (MA), who was immediately cross trained in all PSS responsibilities. As of November 5, 2005, the PSS was reassigned to FBIHQ, and the MA assumed all the PSS personnel security responsibilities. At the same time, the SS was reassigned to the TSC to act as the CTD TSC SO in the absence of the PSS, and later in November, another SS replaced the original SS as the CTD TSC SO.

In December of 2004, the TSC posted for a permanent PSS. After career boarding this position, the TSC interviewed viable candidates in January of 2005 and selected a primary candidate for background. Also in January of 2005, the ISSO was replaced by a Management Assistant and a Senior Chief of the US Coast Guard was appointed to the onsite SO for the TSC to work with the SS (CTD SO for the TSC), ISSM, MA (acting as PSS) and MA (acting as ISSO).

On April 18, 2005, the FBI hired a full time onsite FBI SO for the TSC. The SO will work with the ISSM, MA (acting as PSS), MA (acting as ISSO), and Senior Chief (Deputy Security Officer). On April 21, 2005, the primary candidate for PSS was removed from the background process. On April 22, a new request to post the PSS was made.

Per the above sequence of events, the TSC has had all security functions addressed since early March of 2004 with a combination of personnel. As of January of 2005, the TSC has had a permanent interim onsite SO with a full complement of personnel to address all necessary facets of the security process. As of April 18, the TSC has a permanent SO with a full complement of personnel (four) to address all aspects of the security for the TSC.

Recommendation #32:

Review all records in the Encounter Management database for classified data within the unclassified system and develop a process for regularly checking the work of the call screeners to ensure that classified information is not entered into the unclassified system.

Response:

The TSC disagrees with this recommendation and the explanation follows below.

On February 2, 2005, the Encounter Management Application (EMA) was moved to a classified network. As such, a comprehensive review of all records in EMA for classified data, and the development of a process to ensure classified information is not entered into the unclassified system, is no longer necessary.

On February 4, 2005, the Information System Security Officer (ISSO) organized and facilitated cleanup procedures for EMA. Two TSC Contractors wrote a local script in Sequel 7 code, following guidance by the ISSO. The newly appointed Project Manager (PM) for EMA, was informed of all updates. (TSCRE #37)

For cleanup, the script first accessed the schemas and disabled all of the triggers, or snags, in the database. This was to ensure that the data would not stay on as residual data or be restored in the future. The code found each of the comment fields and began an overwrite process, matching the value of characters in the field. This method ensured that the data would be overwritten, instead of creating new sectors. This method of data allocation is unique to Oracle clients.

The script made 3 passes of the comments: The first pass had overwritten with a 1, the second pass had overwritten with a 0, and the last pass had overwritten the data using the hexadecimal character 1A. This surgical method was necessary so EMA could continue on the unclassified network until the FBI approved EMA to be relocated.

In February, 2005, after the surgical cleanup was complete, a Change Control Board request was made to move EMA to the SECRET enclave. Attached is a hard copy of the Change Request (TSCRE #38) and announcement of the move (TSCRE #39). The Call Center analyst can now process and store higher level data.

Regarding backups, the ISSO has marked any backups of TESTNET, DEVNET, and TSBD as SECRET. The backups have not been used and are destroyed after their cycle is over. If a backup containing data is necessary for mission requirements, the ISSO will run the sequel script on the new instance, and verify that the hardware is sterile before use.

Recommendation #33:

Develop a method for recording and reporting security breaches.

Response:

The TSC agrees with this recommendation and has taken steps to address it.

The ISSO handles all security incidents within the TSC (TSCRE #40). A breach, violation, or other system anomaly may be discovered and reported to the ISSO by a number of means. The most common reporting methods are by user-driven events, system administrative notification of anomalies, and ISSO auditing.

Upon notification of an incident, the ISSO determines the category, threat, and potential impact of the incident. For normal issues, the ISSO follows a template and procedural guideline for crisis handling. This documentation can be found in Attachment G of every System Security Plan (SSP) for our network (TSCRE #41).

All actions will be handled after the incident has been contained. The ISSO will notify the system owner immediately and attempt to contact the ISSM. If the ISSM cannot be reached, the ISSO will contact the ESOC.

The ESOC will determine what actions need to be taken either in conjunction with or in lieu of previous actions taken by the ISSO. After the situation is contained, the ISSO will fill out the ESOC Incident Response Form (TSCRE #42) and create memorandum of record. The memorandum will have a file descriptor of TSC-IR-2005-xxx, where xxx is denoted by the number of the incident. TSC-IR-2005-003 is attached as an example (TSCRE #43). The ISSO then coordinates with the TSC Security Officer to draft an Electronic Communication (EC) referencing TSC-IR-2005-xxx. Once approved, the ISSO maintains a hard and soft copy at all times.

The TSC Information Assurance Office is committed to compliance with FBI and DOJ/OIG requirements concerning the tenets of information security.

Recommendation #34:

Work with partner agencies such as TSOU and DHS's NTC to reduce possible redundancies and duplication of effort.

Response:

The TSC agrees with this recommendation and has taken steps to address it.

In November and December 2004, the TSC hired five Watch Commanders to oversee operations in the TSC Call Center. In order to better coordinate TSC operations with its partner agencies, the TSC Watch Commanders took the initiative to arrange monthly meetings with the NTC and TSOU. The first Watch Commanders meeting was held on February 2, 2005, at the TSC with Watch Commanders representing the FBI TSOU, the NTC, and a representative from the TSA's Transportation Security Intelligence Section (TSIS). Subsequent to the first meeting, TSIS Watch Commanders were invited to attend the meetings and participate in the discussion of issues. Watch Commander's meetings are held on the first Wednesday of each month at the TSC, NTC, TSIS, and TSOU on a rotating basis. The agenda for the meetings includes discussions regarding the integrity of the information contained in the TSDB, Secure Flight, and downgrading NOFLY/Selectees, and policy and protocols to enhance the effectiveness and efficiency of the screening process.

The TSC, through the FAMs liaison to the TSC, visited the TSA Headquarters (TSAHQ) Mission Operations Center (MOC) and met with FAMs executive management. The result of these liaison efforts was a new screening process with the FAMs, and TSC Watch Commanders being provided access to the FAMs Tactical Information Sharing System (TISS). The new screening process notifies FAMs when Selectees board airplanes (Selectee flights), information that was not previously shared with the FAMs. The TSA notifies the TSC about a traveling Selectee, and the TSC notifies the FAM MOC. The MOC notifies the FAMs of these Selectee flights, who monitor the Selectee's activities and provide a report. The Watch Commanders have

access to FAMs reports through the TISS. The FAMs attend weekly meetings at the TSC, and the monthly Watch Commanders meetings. (TSCRE #'s 44, 45, & 46)

The TSC also initiated liaison with the Office of Transportation Vetting and Credentialing (OTVC) – formerly the Office of National Risk Assessment (ONRA) in the DHS. These efforts resulted in an MOU being signed that initiated testing of domestic airline Passenger Name Records (PNR) against the consolidated terrorist watchlist provided by TSC. All issues relating to the security posture of OTVC, non-disclosure agreements, computer hardware and software, audit trails, and post-test cleanups of data have been resolved. The TSC provided input regarding an additional MOU that is being drafted to address policies and protocols relative to the Secure Flight Program.

Recommendation #35

Strengthen procedures for handling misidentifications and articulate in a formal written document the protocol supporting such procedures, as well as provide training to staff on the proper way to manage misidentifications.

Response:

The TSC agrees with this recommendation, and has taken steps to produce a formal written document setting forth protocols for handling misidentifications.

From the earliest days of TSC's operation, TSC Call Center screeners have been using data about known misidentified persons from the TSC encounter database to quickly identify and clear those individuals during the screening process. In January 2005, the TSC developed a high-level concept for a redress process, a very important component of which was a more sophisticated and efficient procedure to help misidentified persons. Since the beginning of 2005, TSC has worked with screening agencies to develop program-specific solutions to the misidentified persons problem. Ultimately, however, TSC envisions a comprehensive, government-wide solution that would use information technology to develop a consolidated "misidentified persons list" that would be used both by TSC and the screening agencies to prevent repeated misidentifications in the terrorist screening processes.

TSC has recently established a formal internal process for receipt and processing of redress inquiries it receives from screening agencies and is currently working to finalize an SOP to document that process, which will include procedures for handling known misidentified persons (TSCRE #47). Once the SOP is finalized, TSC will provide internal training on how to manage misidentified persons.

Recommendation #36:

Develop a formal process for evaluating the effectiveness of the TSC.

Response:

The TSC agrees with this recommendation, but has operated according to this recommendation since its inception.

The TSC has used formalized performance metrics as part of its process for evaluating effectiveness since its inception. As early as January of 2004, the TSC was producing weekly reports to capture statistical accomplishments associated with the TSC Call Center, however statistical tracking which allows the TSC to evaluate its effectiveness dates back to December 1, 2003, the first day of TSC operation.

The most current report for the week ending April 21, 2005 captures statistics and has been provided as an attachment. These performance metrics assist the TSC in judging the effectiveness of its operation as trends and patterns are developed and analyzed.

Furthermore, the TSC will be developing a much more structured performance metric process in association with its strategic plan.

Recommendation #37:

Develop a formal, comprehensive strategic plan to establish the framework necessary for accomplishing the mission, goals and objectives of the organization.

Response:

The TSC agrees with this recommendation, but notes that it has had a formal Strategic Plan since its inception.

Under the supervision of TSC Director Donna A. Bucella, the TSC began the process of preparing for the establishment of the TSC's IOC in late October of 2003. During the course of that preparation, an initial planning document and a manual of Process Flows was developed. Simultaneously, work was initiated on the TSC Strategic Plan. By December of 2003, a graphical representation of the TSC Strategic Plan was produced, and has been updated periodically in accordance with the mission, goals and objectives of the organization (TSCRE #48). In January of 2005, a secondary effort was initiated to translate the graphical Strategic Plan into a formal narrative document. That effort was spearheaded by a Federal Funded Research and Development Center contract company under TSC direction. Those efforts have been completed and passed to the TSC staff for review and revision. It is estimated that the TSC will have a formal narrative version of its longstanding Strategic Plan by May 2005.

Recommendation #38:

Enhance the COOP and EAP to: a) include preparations for access to the consolidated terrorist information database at the established back-up site, b) identify a location for the storage of database backup disks in preparation for the loss of database information should a power surge or disaster occur, c) establish an off-site system that is equipped to run the TSDB software as well as connect to the end-user databases for data export, and d) ensure that proper safeguards are in place for the security and temperature control of the TSC.

Response:

The TSC agrees with this recommendation and has taken steps to address it.

a) The TSC, as of April 16, 2005, has established a disaster recovery site at the [SENSITIVE INFORMATION REDACTED], and exercised the capability to respond to a disaster requiring the movement of personnel and resources to an alternate site for continuous operations of the TSC. This was a successful operation (TSCRE #49). The TSC now has the ability to respond to the disaster recovery location with full access to data, networks and systems necessary to keep continuous operation of the TSC during a disaster. In addition, a second disaster recovery site is being implemented at the [SENSITIVE INFORMATION REDACTED], and should be operational by the end of May, 2005. This will give the TSC two alternatives in the event of any type of disaster. The TSC Emergency Action Plan (EAP) is in the process of being updated to reflect these new protocols.

b) The TSC is now storing back-up data disks at [SENSITIVE INFORMATION REDACTED] as its primary disaster recovery site. A redundancy of this capability is being implemented at the [SENSITIVE INFORMATION REDACTED] as its secondary disaster recovery site. This action should be completed by the end of May, 2005.

c) As of April 16, 2005, the TSC now has the capability at [SENSITIVE INFORMATION REDACTED] to run all TSDB software as well as connect to end-user databases for data export. Redundancy of this capability will be implemented at [SENSITIVE INFORMATION REDACTED] by the end of May, 2005.

d) The TSC was previously co-located with the Foreign Terrorist Tracking Task Force (FTTTF). The FTTTF has established the security controls and heating, ventilation and air conditioning (HVAC) protocols that affected the TSC. The FTTTF began the process of relocating from September of 2004 through March 15, 2005. Through this transition, as the TSC began to assume responsibility for the security and HVAC, several longstanding issues with the facility were identified and corrected where possible.

[SENSITIVE INFORMATION REDACTED]

Recommendation #39:

Ensure that the COOP and EAP are fully implemented including employee training, equipment testing, and plan exercising.

Response:

The TSC agrees with this recommendation and has taken steps to address it.

Per the responses to recommendation #38, the TSC has a primary back-up location for disaster recovery at the [SENSITIVE INFORMATION REDACTED]. Furthermore, the TSC will have a secondary location established for disaster recovery at TSOU by the end of May, 2005. The first operational test of this capability with full system use was on April 16, 2005, which was successful. The April 16, 2005 test was the first of quarterly training that will be the normal course of business for the TSC.

With regard to Continuity of Operations (COOP), the TSC is cooperating fully with the FBI, and the FBI Office of the Chief Information Officer (OCIO). The FBI OCIO is charged with the responsibility of coordinating the entire COOP programs under the administrative purview of the FBI for the purpose of effectiveness, efficiency and cost saving to the US Government and the American people. The TSC has developed a COOP plan under the FBI guidelines and tendered it to the OCIO for evaluation and integration with the FBI COOP program. The TSC has also been conducting exploratory missions with the [SENSITIVE INFORMATION REDACTED] to determine the viability of utilizing one of these sites or a similar one as the TSC COOP location. The TSC will continue to coordinate the execution of a COOP site and the budget implications from such an operation with the FBI, the DOJ and the Office of Management and Budget.

Recommendation #40:

Consider the transfer of the Encounter Management database to a classified network capable of maintaining the database at the various classification levels.

Response:

The TSC agrees with this recommendation and has completed it.

The TSC transferred the Encounter Management Application to classified network on February 2, 2005 (TSCRE# 39).

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

The TSC provided comments on our draft audit report, which can be found in Appendix IV. In addition to its response in excess of 40 pages, the TSC provided numerous attachments, which are referenced throughout its response. Due to their volume, these attachments were not included in our final report. Our analysis of the TSC's comments on each recommendation is found below.

Recommendation Number:

1. Resolved. In response to this recommendation to create a plan for the maturation of its information technology efforts, the TSC stated that it agreed with the OIG, but that it has operated in accordance with this recommendation since its inception. In its support for this statement, the TSC referred to the creation of an initial formal staffing plan in January 2004, supported by an Electronic Communication to the FBI Counterterrorism Division entitled "Request to Establish Funded Staffing Level for the Terrorist Screening Center," as well as to a draft TSC organizational chart dated November 18, 2003. Additionally, the TSC stated that it had become apparent that the TSC's requirements would exceed its proposed staff, and as a result in August 2004 the TSC created a Master Staffing Plan. The TSC also supported its response by describing future enhancements to the TSDB, including three separate software products that it expects will have a significant impact on its ability to add audit trails within the database. Further, the TSC stated that "[i]n its Strategic Plan, the TSC has, from its inception, planned to increase connectivity, search capabilities, and development of new capability derived from constant review of the TSC mission, function, and requirements."

While we acknowledge that some of the essential components of an IT strategic plan exist in some form, as of May 2005 no formal, integrated, and comprehensive strategic plan existed for the TSC's IT environment. Throughout our audit work, the TSC verbally communicated its vision for the current consolidated watch list database and for future databases. However, until the assignment of a Chief Information Officer (CIO) in August 2004, the vision for specific aspects of the database and the TSC's IT environment was in a constant state of flux, with many of the critical decisions made on an ad hoc basis and without strong IT oversight. Since the CIO came on board, the TSC's plans for its IT environment have begun to solidify and become clearer. However, we believe that the TSC would benefit from establishing a formal, written

document that addresses systematically IT organizational and resource planning, management, and performance measurement.

In conjunction with the TSC's strategic plan, the IT strategic plan should provide for the evolution of the IT environment and combine in one document the TSC's plans regarding its current and future IT environment. It should account for factors such as changing regulations, evolving technology, and emerging customers and uses. This plan should include an evaluation of the impact of each factor, TSC's specific IT strategies and timelines for adapting and accomplishing its overall mission, and specific methods for measuring achievement and performance. Included in these considerations are systems engineering and architecture planning, application development, project management, and resource planning (such as budget, staffing, and facilities).

This recommendation can be closed when the TSC provides a written, comprehensive plan for its IT environment that addresses: a) IT staffing needs on a project-by-project basis; b) controls to ensure data integrity; c) adequate oversight of IT contracts and contractors; and d) future improvements in the areas of TSDB connectivity, name search capabilities, acceptance of biometric data, and other IT planning issues.

2. **Resolved.** This recommendation is resolved based on the TSC's agreement and resulting efforts to develop requirements and software for the application of audit trails to track activity within the TSDB. According to the information provided by the TSC, these enhancements will be implemented beginning in May 2005. This recommendation can be closed when the TSC provides evidence that it has fully implemented audit trails in the TSDB.

3. **Resolved.** In response to this recommendation to develop staffing protocols, the TSC stated that it agreed with the OIG, but that it has operated according to the recommendation since its inception. To support this statement, similar to its response to recommendation 1, the TSC referred to the creation of an initial staffing plan in January 2004, supported by an electronic communication to the FBI Counterterrorism Division. Additionally, the TSC stated that in August 2004 the TSC began to work on a Master Staffing Plan to reflect the current and anticipated needs of the TSC. According to the TSC, this Master Staffing Plan was published via electronic communication to the Director of the FBI and other entities as of October 29, 2004. The TSC further stated that this Master Staffing

Plan is "the staffing protocol that governs the staffing of the TSC to include the levels of participation from other agencies."

While we are aware of the TSC's efforts to maintain this Master Staffing Plan and ensure that vacant positions are filled with individuals from all participating agencies, we do not believe that this plan suffices as protocol to mandate that the TSC be staffed with personnel from all participating agencies. The plan reveals the TSC's calculated total number of personnel necessary from each participating agency and the resulting branch and work area at the TSC to which each position is currently assigned. However, the plan does not direct the TSC to fill future vacant positions with individuals from the participating agencies. In addition, the plan is strictly an internal document and does not reflect agreement from the leadership of the participating agencies. As a result, the TSC is vulnerable to future staffing plan modifications that may not reflect an adequate representation of each participating agency.

Additionally, the TSC provided correspondence from the Department of Homeland Security (DHS) dated April 22, 2005, which stated that the DHS has only fulfilled half of its staffing obligation to the TSC, or 21 detailees. This correspondence further stated that to fill the necessary 21 additional DHS positions at the TSC, the DHS would assign detailees to the TSC no later than May 9, 2005, and would do so for a period of 1 year, when possible.

As a result, this recommendation can be closed when the TSC provides evidence that the DHS has filled the 21 positions identified as vacant. In addition, the TSC should formalize its staffing agreements with all participating agencies.

4. **Resolved.** The TSC agreed with this recommendation, stating that it had taken steps to increase the number of permanent and long-term loaned personnel and reduce the need for orientation and training of new staff. Upon our review of the supporting documentation provided by the TSC, it appears that the TSC is making important efforts to hire qualified, permanent staff to fill vacancies at the TSC.

For example, the TSC reported that since November 2004 it has increased its permanent FBI staff by five, with an additional four individuals awaiting completion of their background investigations to complete the hiring process. Further, as noted in Recommendation 3, 21 additional DHS detailees were to be assigned to the TSC by May 9, 2005, for details of 1 year (when possible). Also, the Marine Forces North was requested to send an individual to the TSC for a 1-year tour

of duty. According to the TSC, it has recently mandated that all temporary duty (TDY) employees serve for a minimum of 90 days to minimize the need for constant orientation and training.

This recommendation can be closed when we receive a copy of the new policy that all TDY employees be assigned to the TSC for at least 90 days.

5. **Resolved.** The TSC agreed with this recommendation, stating that it had begun to take appropriate corrective action. The TSC provided documentation that addresses the need for ensuring that the TSDB accurately represents the data that was submitted by the nominating agency and that the TSC can trace the origin of a record back to the nominating agency. This recommendation can be closed when we receive evidence that the project for automating the FBI nomination process and the TSDB 1.4 as a whole have been implemented, enabling an automated nomination process with a built-in audit capability that can track system transactions between the TSC and the FBI's National Crime Information Center (NCIC). Additionally, for this recommendation to be closed the TSC must provide evidence that the TSDB 1.5 has been implemented. According to the TSC, this will provide a transactional audit history of the information flow from the National Counterterrorism Center (NCTC) to the TSDB, and will enforce over 35 business rules in the receipt of data between NCTC and the TSDB.

6. **Resolved.** The TSC agreed with this recommendation and stated that it has begun taking corrective action. The TSC stated that the TSDB 1.5 (scheduled to be implemented as part of the TIDE project) will facilitate the reduction of human review and intervention because the software will enforce enhanced automated controls. Currently, a TSC employee must physically review, for accuracy and consistency, each record nominated for inclusion in the TSDB. The TSC's new business rules, contained in the "TSDB 1.5 Business Rule and Cartesian Product Formatting" document, are designed to validate that the data received from NCTC complies with legal and negotiated restrictions on data relationships.

Further, the TSC asserted that a significant obstacle to fully automating the information-sharing process resulted from the technological and organizational impediments experienced by the Intelligence Community in establishing "trusted network connections" capable of moving data from Top Secret to the Sensitive But Unclassified level.

Based on our review of the TSDB 1.5 support provided by the TSC, this recommendation can be closed when we receive evidence to support that the TSDB 1.5 has been implemented and has automated the daily upload of records nominated for inclusion in the TSDB.

7. **Resolved.** The TSC agreed with this recommendation and provided a summary of its outreach efforts. We recognize that the TSC has conducted outreach since its inception and has enhanced its outreach efforts in the last year, including the creation of a TSC video and brochure. However, the TSC has not developed a formal, vigorous outreach plan that defines the target organizations, timelines for the completion of outreach goals, staffing levels needed to conduct outreach, and funding needed to perform outreach activities now and in the future. For example, in its response the TSC stated that it has a plan for ensuring that TSC presentations are made in all 50 states, that it will be training all FBI Legal Attaches, and that a website will be created. However, no documentation of these plans was referenced or provided to us. This recommendation can be closed when the TSC provides documentation to support that a formal outreach plan has been developed.

8. **Resolved.** The TSC agreed with this recommendation and noted that it had initiated meetings related to the DHS's responsibility for establishing guidelines for private sector screening. While we recognize the TSC's complementary role to the DHS in this effort, we noted that the TSC stated it had taken action in this area in the last 6 months, but the documentation provided to us with the response was dated in August 2004. Therefore, to close the recommendation, please provide an up-to-date account of the TSC's efforts to encourage the DHS to finalize private sector screening guidelines.

9. **Closed.** The TSC agreed with this recommendation and stated that, on March 16, 2005, the TSC sent 1,183 TSDB 1A records to NCTC for analysis and, if appropriate, nomination into the TSDB. The TSC reported that 1,131 of these records were transferred back to the TSDB, while 52 duplicate records were identified and therefore not transferred. In addition, the TSC provided support that 1,131 records were received into the TSDB on the April 18, 2005. Therefore, this recommendation is closed.

10. **Resolved.** The TSC agreed with this recommendation and stated that it is taking steps to review every record within the TSDB to identify and correct the duplicate record issue. This recommendation can be closed when we receive evidence from the TSC that this records review

has been completed and all 31 duplicate records identified during our audit have been removed from the TSDB.

11. Resolved. The TSC agreed with this recommendation and stated that it is taking steps to review every record within the TSDB to identify and correct the duplicate record issue, including records with duplicate TIPOFF identification numbers. This recommendation can be closed when we receive evidence from the TSC that this records review has been completed and all four records identified to have duplicate TIPOFF identification numbers have been corrected in the TSDB.

12. Resolved. The TSC agreed with this recommendation and noted that it has taken steps to complete it, including the creation of a new Data Management Office that will develop tools to help increase the quality of TSC data. According to the TSC's response, the Data Management Office is currently creating structured query language (SQL) and small-scale database tools to improve data quality.

The TSC stated that it is also modifying the TSDB 1.5 software to accept the entire TSDB as a batch file, so that all of the TSC business rules envisioned for the future receipt of data files from the TIDE system will be applied to the existing TIPOFF records within the TSDB. This recommendation can be closed when we receive documentation showing that these tools have been implemented and SQLs have been run to ensure that the TSDB data is complete, accurate, and non-duplicative.

13. Resolved. The TSC agreed with this recommendation and stated that it has taken appropriate steps to implement it. Specifically, the TSC's response stated that NCTC will provide to the TSC the source of each international terrorist record within the TSDB and that this information will be captured in the upcoming TSDB 1.5. The TSC stated that because it is responsible for inputting all domestic terrorism records into the TSDB, the TSC Nominations Unit will track the source of the domestic terrorist information. This recommendation can be closed when we receive evidence from the TSC that all records within the TSDB can be traced to either the FBI or the NCTC database.

14. Resolved. The TSC agreed with this recommendation and stated in its response that it has taken steps to implement it. Specifically, the TSC stated that in October 2004 it requested that three new Immigration and Nationality Act (INA) codes be established for the sole purpose of describing domestic terrorist activity. However, the TSC's response did not provide the INA code numbers that will be used for the three new codes. Also, the TSC did not provide a description of

the distinctions between the new domestic terrorist codes or how the new INA codes will describe the domestic terrorist activity associated with the watch-listed individual.

This recommendation can be closed when we receive evidence from the TSC that: 1) the INA codes have been established, 2) specific INA code numbers have been assigned, 3) the new codes describe the domestic terrorist activities of the watch listed individuals, and 4) the new codes support the distinctions between the new domestic terrorist INA codes.

15. **Resolved.** The TSC agreed with this recommendation and stated that it has taken steps to implement it. Specifically, TSC stated that three new INA codes were requested in October 2004 to be established for the sole purpose of describing domestic terrorist activity. Additionally, the TSC stated that a review of the INA code applied to each domestic terrorist record will also be conducted during the previously mentioned record-by-record review of the TSDB. This recommendation can be closed when we receive evidence from the TSC that the three new domestic terrorist INA codes have been appropriately applied to all domestic terrorist records within the TSDB.

16. **Resolved.** The TSC agreed with this recommendation and stated that it has taken steps to complete it. Specifically, the TSC stated that it addressed the 336 records without handling codes during the previously mentioned record-by-record review of the TSDB. However, it did not provide evidence to support that action has been taken on the 336 records noted in our report. This recommendation can be closed when we receive evidence from the TSC that the 336 records have each been assigned the proper handling code.

17. **Unresolved.** The TSC stated that it did not agree with this recommendation. The TSC's response stated that none of the four existing handling codes are considered "low-threat." [SENSITIVE INFORMATION REDACTED]

Therefore, while handling codes may not specifically equate to the level of threat posed by watch listed persons, we believe that the correlating instructions to responding law enforcement officials provide insight into the level of threat posed by the individuals.

The TSC's response further stated that "there is no link with VGTOF handling codes used to inform state and local law enforcement officers

with the TIPOFF INA Codes used to classify the type of known or suspected terrorists." During our audit, we obtained the TSC's Nomination/Handling Code Criteria and Nomination Review Process in which eight INA codes were marked as "armed and dangerous." We were informed by the TSC Nominations Unit and FBI personnel that [SENSITIVE INFORMATION REDACTED]. Further, as discussed on page 55 of our report, we determined that the TSC had requested that the FBI's programming language for preparing records for transfer from VGTOF to the TSDB electronically apply an INA code to each domestic record based on the handling code assigned. Specifically, the program applied an "armed and dangerous" INA code to a handling code 4 and a non-armed and dangerous INA code to handling codes 1, 2, and 3.[67] Therefore, although there may not be a direct and absolute link between the INA and handling codes, there has been a relationship in the application of the codes and it is reasonable to conclude that in most instances the information in the two fields should not be inconsistent.

We agree that the TSC should use all legacy information available in order to compile the most effective and comprehensive consolidated database, including the INA code with armed and dangerous designations. However, it seems inconceivable to us that 22,809 records of individuals with INA codes that identify the person as [SENSITIVE INFORMATION REDACTED] or describe the subject as likely to engage in terrorism if in the United States (INA code 7) would be assigned a handling code 4, which requires the lowest level of law enforcement response. [SENSITIVE INFORMATION REDACTED]

Further, at our exit conference in April 2005, TSC officials reported that changes had been made to records within the TSDB and that handling code 3 now represented the largest portion of the database.[68] The information provided at the exit conference suggested to us that the TSC recognized that too many individuals' records were applied a handling code 4. As a result, this recommendation can be resolved and closed when we receive data from the TSC that shows it has determined that the appropriate handling code has been assigned to all records in the database, especially those with "armed and dangerous" INA codes.

---

[67] According to a TSC official, the opposite instruction was intended. That is, the TSC wanted non-armed and dangerous codes to be applied to handling code 4 records.

[68] At the time of our audit, handling code 4 represented the largest portion of the database.

18. Resolved. The TSC agreed with this recommendation and stated that in October 2004 the "Wedge Project," which was designed to address the fields in TIPOFF that could be exported from NCTC but were not displayed in the TSDB, was placed into production.

The TSC further stated in its response that [SENSITIVE INFORMATION REDACTED] and [SENSITIVE INFORMATION REDACTED] were included in these fields. We reviewed the TSDB Wedge Release 1.1 System Requirements Specification provided as support for this statement and identified several software modifications. However, because we were not provided with field descriptions, we were unable to confirm that separate fields for [SENSITIVE INFORMATION REDACTED] and [SENSITIVE INFORMATION REDACTED] were included in this project. Upon receipt of evidence confirming that the [SENSITIVE INFORMATION REDACTED] and [SENSITIVE INFORMATION REDACTED] are separate fields as a result of the Wedge Project, this recommendation can be closed.

19. Resolved. The TSC agreed with this recommendation and stated that the Wedge Project, placed into production in October 2004 (as noted in the preceding recommendation), activated and populated all fields of information, with the exception of those associated with the TIDE implementation which will be activated later in 2005. Because the referenced attachment to the TSC response (TSCRE #27B) did not exist, the supporting documentation provided for the Wedge Project in TSCRE #27 was used as evidence for this statement.

We recognize that the TSC has taken measures through the completion of its Wedge Project to ensure that the additional record information can be received into the TSDB. However, the TSC's response did not address whether all information has been received or whether the information is displayed on the TSDB screen. This recommendation can be closed when the TSC provides us with evidence documenting that this additional information is available in the TSDB and is currently displayed on the TSDB screen.

20. Resolved. The TSC agreed with this recommendation and stated in its response that it has taken steps to complete this action. Specifically, the TSC stated that the previously discussed record-by-record review being performed by the Quality Assurance staff will address the eight VGTOF records and the three TIPOFF records that were not in the TSDB at the time of our testing. The TSC further stated in its response that agencies nominating records for inclusion in the TSDB are responsible for sending accurate, consistent, and

complete information to the TSC for receive into the consolidated database. Further, as part of the TSDB 1.5 project, TSC officials stated that built-in protections and buffers will serve as automated procedures to help ensure data integrity.

As a result, this recommendation can be closed when the TSC provides us with evidence that the TSDB 1.5 project has been successfully implemented. However, because the record-by-record review is being performed on records that are in the TSDB database, this effort will not assist in ensuring that the omitted records are added to the database. Therefore, the TSC should also provide evidence that the eight VGTOF records and the three TIPOFF records that were omitted from the TSDB are now included in the database, if appropriate.[69]

21. Resolved. The TSC agreed with this recommendation and stated that it has taken steps to implement standardization of the data field definitions. According to the TSC, the Intelligence Community Metadata Working Group adopted the Terrorist Watch Person Data Exchange Standard (TWPDES) and the TSC will be the only entity interacting with the Interface Control to use the new standard. Further, accounting for its two primary data sources, the TSC stated that it has integrated the TWPDES into its data flow from NCTC to the TSC, and the TWPDES is being integrated with the Justice Global Information Sharing XML 3.0 standard.

TSC provided an unsigned copy of its agreement with NCTC entitled "Nominations Interface Control Document (ICD)." Our review of the Nominations ICD indicates that, once signed and implemented, the two organizations will have reached a comprehensive agreement regarding the definition and incorporation of a standardized protocol for terrorist watch list information and transmission. However, we have not received adequate documentation related to the incorporation of the TWPDES and the Justice Global Information Sharing XML 3.0 standard to determine the extent to which the TSC has standardized its protocol for terrorist watch list information and transmission with the FBI VGTOF database. Further, it remains unclear what relationship the incorporation of the standardized protocol with NCTC and FBI will have on databases such as CLASS and the TSA No-Fly list that receive information from the TSDB.

This recommendation can be closed when we receive a version of the TWPDES signed by representatives of the TSC and NCTC, as well as

[69] As previously discussed, the TSDB 1A database is no longer in existence, and, as a result, the TIPOFF records missing solely from 1A are no longer of concern.

evidence that the protocol has been fully implemented. In addition, please provide further evidence and clarification regarding the extent to which the TSC is standardizing its protocol for information and transmission with the FBI's VGTOF database, as well as recipient systems.

22. **Resolved.** The TSC agreed with this recommendation and stated in its response that it has had procedures to identify and resolve missing and conflicting record information since its inception. While we recognize that the TSC has made efforts to resolve missing or conflicting record information on a reactive basis, during our audit we were not provided with evidence of regular, proactive procedures to identify missing or conflicting information. The TSC stated in its response that the previously mentioned record-by-record review that is being conducted by the TSC will identify and correct any missing or conflicting records. The TSC also stated that efforts are underway to modify the TSC's existing Encounter Management database, which will allow data quality issues that surface during actual encounters to be submitted electronically to Quality Assurance personnel.

    We have been provided evidence that this record-by-record review of the TSDB has been initiated. However, we are unclear as to whether the TSC will perform regular testing of TSDB records to identify and resolve missing and conflicting record information after the initial record-by-record review has been completed. As a result, this recommendation can be closed when we receive documentation supporting the TSC's plans to continue to perform regular testing of records within the TSDB after the initial review of all records has been completed.

23. **Resolved.** The TSC agreed with this recommendation and stated that it has taken steps within its power to improve operations for proper data receipt from the TWWU. It also provided supporting documents, such as e-mail correspondence between the TWWU and the TSC, to document the TSC's efforts to address the matter. The TSC stated that it continues to receive international terrorism nominations that were incorrectly forwarded from the TWWU and continues to discover domestic terrorism nominations that were incorrectly forwarded to NCTC. However, the TSC stated that it believes the electronic nomination process, which was to be implemented as part of the TSDB 1.4 in May 2005, will correct/address the errors being made through the current process. This recommendation can be closed when we receive evidence that the TSDB 1.4 has been fully

implemented, thereby launching the electronic nomination process and reducing the instances of improperly transferred information.

24. Closed. The TSC agreed with this recommendation and reported that officials met with individuals in the Department of the Treasury regarding the Current List of Terrorists and Groups Under Executive Order 13224. The TSC stated that its executive management has confirmed that an updated version of this list of names is regularly provided to NCTC for analysis and possible inclusion of the identities into the NCTC database, the source of international terrorist information for the TSDB. As a result, this recommendation is closed.

25. Resolved. The TSC agreed with this recommendation. In its response, the TSC acknowledged that since December 2003 and prior to the arrival of these newly hired, permanent supervisors, the Call Center had been supervised by FBI agents on loan who possessed a variety of backgrounds but minimal counterterrorism experience. The TSC stated that no formal training was provided to these agents upon their arrival at the TSC. Further, in many cases these agents had never screened a call/encounter before and had no experience in working with the various databases.

According to the TSC, it has implemented procedures to correct this concern about call center supervision. Specifically, the TSC stated that it now responds to law enforcement encounters in an average of approximately 10 minutes. This is a reduction of 10 minutes from the previous average of 20 minutes per encounter the OIG was informed during our field work.[70] The TSC stated that in October 2004, six permanent Call Center employees were brought on board as team leaders. They are responsible for ensuring that all of the documentation from a call is reviewed and is complete prior to disseminating the information to the CT Watch (now the Terrorist Screening Operations Unit, or TSOU), the DHS National Targeting Center, and other law enforcement agencies. In addition, the TSC stated that it brought on board five Watch Commanders in November 2004 and one permanent GS-15 FBI Unit Chief in January 2005.

[70] While on site at the TSC, we became aware that neither the TSC nor CT Watch had established a formal method for tracking, recording, and analyzing the time it takes to respond to law enforcement regarding an encounter. An official at CT Watch had provided us with what the individual believed was the average time it took to respond to law enforcement inquiries, or 20 minutes. However, the individual stated that no method of tracking the exact times existed. As a result, we need to know the method the TSC used to calculate the approximate 10 minutes that it stated it takes for the TSC to respond to law enforcement officials who have potentially encountered an individual. This matter is further addressed in Recommendation 29.

Based on the information provided, this recommendation can be closed when we receive evidence of the TSC's official protocol that requires the regular, supervisory review of the work of Call Center personnel for completeness, accuracy, and timeliness. Sufficient evidence may include formally established procedures for Call Center supervisory review, as well as correspondence between supervisors and Call Center staff as to what requirements exist for an encounter to be considered as having received supervisory review.

26. Resolved. The TSC agreed with this recommendation and stated that it has established procedures to address it. Specifically, the TSC stated that over the past 8 months it has implemented a training program in which each Call Center employee will participate. From the documentation provided, we believe that the TSC is attempting to train employees on the proper procedures for obtaining and recording call information on the Call Intake Form. The TSC's training guide on the Encounter Management database appears to be thorough and shows that the Encounter Management database now has stronger controls for data field entry with establishment of drop down boxes to minimize the number of errors that can occur from standard data entry. Additionally, our review of the training guide identified that the disposition and the final resolution fields are reserved for Team Leader input only, potentially reducing the risk that information would be incorrectly entered by Call Center personnel into the Encounter Management database. However, it does not appear that there are any controls to identify instances in which personnel aside from Team Leaders enter information into these fields. Additionally, while there is a check box for Call Center personnel to mark when a record is ready for supervisory review, we are not aware of any controls in place to ensure that this box is checked, and we were provided no indication while on site as to whether records not checked for supervisory review would be found in the system and timely reviewed prior to the record being closed.

This recommendation can be closed when we receive evidence that sufficient controls have been implemented to ensure that each record is reviewed by the appropriate personnel before it is closed.

27. Resolved. The TSC agreed with this recommendation and stated that it has taken steps to address it. Specifically, the TSC stated that it has planned enhancements, discussed in Recommendation 22, to Version 2.0 of the Encounter Management database. This recommendation can be closed when we receive evidence that the Encounter Management database Version 2.0 has been fully

implemented and has enhanced the tracking capability and timely follow-up measures for encounters.

28. Resolved. The TSC agreed with this recommendation and stated that it has completed this item. Specifically, the TSC stated that on December 1, 2004, a retired FBI Special Agent with extensive teaching experience was hired to coordinate the TSC training program.

Our review of the training materials provided to us during a recent visit to the TSC showed that the TSC is expending significantly more effort to ensure that personnel are trained in Call Center operations. In addition, we witnessed one of the informational presentations that are held approximately three times per month by subject matter experts designed to heighten the awareness of all employees in the topical areas related to the war on terrorism.

This recommendation can be closed when we receive evidence that these new training practices have been formalized in official TSC protocol documentation.

29. Resolved. The TSC agreed with this recommendation and stated that it recognizes the importance of tracking the timeliness of the encounter process in order to provide the best service to its customers. The TSC reported that it has begun to analyze the scope of work in order to provide these statistics as part of the Case Disposition and Tracking System, which is expected to be implemented within the next 6 months.

As a result, this recommendation can be closed when we receive evidence that the TSC has fully implemented a system for tracking the amount of time that elapses between the key events of an encounter.

30. Resolved. The TSC agreed with this recommendation and stated that it has taken steps to address it. Specifically, the TSC has placed its Encounter Management database on a local classified network, and has stated that it is prepared to place this database on the global FBI classified network. However, the TSC stated that it must wait to be migrated to the FBI's new computer network designed for universal use within the FBI. The TSC expects to be migrated in June 2005.

This recommendation can be closed when we receive evidence that the TSC has placed the Encounter Management database on the global FBI network, enabling the electronic sharing of encounter information with CT Watch (now TSOU).

31. Resolved. The TSC agreed with this recommendation for the assignment of a security officer and stated that it has operated to fulfill this recommendation since its inception. However, as indicated by its response, the TSC has not had stability or permanence in the Security Officer position since its inception. While the TSC has ensured that a complement of loaned, on-site, and other personnel have been assigned the tasks of Security Officer, no less than nine individuals have performed the functions in the 17-month period from December 2003 through April 2005. As noted in our report, we identified significant security concerns that could be mitigated through the assignment of staff to this function. Therefore, to close this recommendation, please provide evidence that, as of April 18, 2005, the TSC has a permanent Security Officer with a full compliment of staff to address all aspects of security for the TSC. This should include position descriptions and approved Notice of Personnel Action forms (SF-50) for each related individual/position.

32. Resolved. The TSC disagreed with this recommendation, stating that the Encounter Management database was moved to a classified network on February 2, 2005. As a result, the TSC stated that a comprehensive review of all records in the Encounter Management database for classified data, as well as the development of a process to ensure that classified information is not entered into the unclassified database, is no longer necessary.

We agree with TSC's argument regarding the movement and classification of the Encounter Management database and have resolved the recommendation as a result of this and the resulting protection of data in the database.[71] However, during our review we identified significant weaknesses related to the TSC's handling of classified information. Given the unique mission of the TSC, the amount of information that is shared by other agencies, and the variety of media used to record information, we believe that TSC employees need to be more aware of the classification level of the information they are handling.

Further, we noted that the CT Watch (now TSOU) identifies the classification level of each paragraph of information within its electronic log, which is similar in function to the Encounter Management database. Based on our observations, we consider the CT Watch procedure of marking the classification level of each paragraph within its electronic log to represent a best practice, and we

[71] In Recommendation 40, we suggest that the TSC consider moving the database to a classified environment.

strongly recommend that the TSC adopt this procedure for marking the classification level of each paragraph within its Encounter Management database.

Additionally, the TSC included in its response language stating that the backups of various files, including the TSDB, have been marked Secret. While the backup of files was not included in our recommendation to the TSC, we request clarification from the TSC as to why backups for the TSDB, a database mandated by HPSD-6 to be unclassified, has been marked Secret.

This recommendation can be closed when we receive clarification from the TSC regarding the classification level of the TSDB backup and a response to our suggestion regarding adopting paragraph markings in its database.

33. Closed. The TSC agreed with this recommendation. The TSC has established a Standard Operating Procedure to provide operational guidance and limitations to all users at the TSC regarding the proper method for reporting and handling security incidents. The TSC has also developed procedures for recording the parties involved, events, and corrective actions regarding each incident that occurs. As a result, this recommendation is closed.

34. Closed. The TSC agreed with this recommendation and stated that the TSC Watch Commanders arranged for monthly meetings with NTC and the CT Watch (now TSOU), the first of which was held on February 2, 2005, and included a representative from the TSA's Transportation Security Intelligence Section (TSIS). The TSC stated that these meetings include discussions regarding the integrity of the information contained within the TSDB and policies and protocols to enhance the effectiveness and efficiency of the screening process. Additionally, the TSC stated that it has increased coordination with the Federal Air Marshals and the Office of Transportation Vetting and Credentialing (OTVC) within the Department of Homeland Security. The TSC's response and the supporting documentation provided indicate that the TSC has implemented an ongoing effort to improve the efficiency of the screening process. Therefore, this recommendation is closed.

35. Resolved. The TSC agreed with this recommendation, stating that it has taken steps to produce a formal, written document setting forth protocols for handling misidentifications. The TSC stated that in January 2005 it developed a high-level concept document for a redress

process, an important component of which was a more sophisticated and efficient procedure to help misidentified persons. The TSC further stated that it has worked with screening agencies to develop program-specific solutions to the matter of misidentified persons. The TSC stated that it has recently established a formal, internal process for receipt and processing of redress inquiries it receives from screening agencies, and that it is currently working to finalize a Standard Operating Procedure to document such a process, which will include procedures for handling known misidentified persons. The TSC stated that once the Standard Operating Procedure is finalized, the TSC will provide internal training on how to manage misidentified persons.

This recommendation can be closed when we receive evidence that the TSC has finalized its Standard Operating Procedure for the appropriate handling of known misidentifications and has provided training to staff on the proper way to manage misidentifications.

36. Resolved. The TSC agreed with this recommendation, but stated that it has operated according to this recommendation since its inception. Specifically, the TSC stated that as early as January 2004, the organization was producing weekly reports to capture statistical accomplishments associated with the TSC Call Center, and further stated that statistical tracking dates back to December 1, 2003.

However, the Director of the TSC told us during our audit that no process was in place to evaluate the effectiveness of having one consolidated database to track terrorism suspects. The weekly reports mentioned by the TSC capture summary statistics on calls received by the Call Center, but they are only one tool in a comprehensive analysis of performance measurement. Alone they do not measure the achievement of specific performance goals and the added value to having one consolidated terrorist watch list. As a result, this recommendation can be closed when we receive evidence that the TSC has established a formal plan for evaluating the effectiveness of the TSC.

37. Resolved. The TSC agreed with this recommendation, but stated that it has had a formal strategic plan since its inception. In its response, the TSC stated that it initiated the development of a strategic plan concurrent to the development of its initial planning document and a manual of process flows. Further, the TSC provided a graphical representation of its in-process strategic plan. The TSC also stated that it anticipated a formal narrative strategic plan would be completed by May 2005. During the course of our audit, we obtained draft copies

of the initial planning document and the manual of process flows, as well as the graphical representation of the strategic plan mentioned by the TSC.

We acknowledge that these documents represent some of the essential components of a strategic plan and exist in varying degrees of finality and permanence, but as of May 2005 no formal, integrated, and comprehensive narrative strategic plan for the TSC had been provided to the OIG. In addition, while the TSC provided a graphical representation of the in-process strategic plan, we believe that the document, in its current state, is virtually unusable. In order to graphically depict many of the elements of a strategic plan, the document is either inordinately large so as to be unwieldy or the text reduced so as to be unreadable. Further, many essential components to an effective strategic plan such as timelines, strategies, and performance measures are omitted.

We concluded that the TSC would benefit from establishing a formal, written document that addresses all aspects of organizational and resource planning, management, and performance measurement. The TSC's strategic plan should provide for the continued development of the TSC organization, and it should combine, in one location, TSC's vision regarding the current and future environment and account for factors such as changing regulations, evolving technology, and emerging customers and uses. This plan should also provide a broad framework for the organization and include a comprehensive evaluation of the impact of each factor, the TSC's specific strategies and timelines for adapting and accomplishing its overall mission, and specific methods for measuring achievement and performance. Included in these considerations are goals for each major operational unit within the TSC and strategies for administrative areas, such as resource planning, continuity of operations planning, and information security.

This recommendation can be closed when the TSC demonstrates that it has developed a formal, comprehensive, narrative strategic plan that provides a framework for the accomplishment of the organizational mission, goals, and objectives, as well as specific timelines and performance measurements.

38. Resolved. The TSC agreed with this recommendation and stated that it has taken steps to address it. Specifically, documentation that the TSC provided stated that the [SENSITIVE INFORMATION REDACTED] serves as the primary disaster recovery site for the TSC and now has a

copy of the TSDB and the Encounter Management database for call screening purposes. The TSC stated that by May 2005 a second disaster recovery site should be operational at the [SENSITIVE INFORMATION REDACTED]. The TSC stated that it is updating its Emergency Action Plan to reflect the new protocol.

Additionally, the TSC stated in its response that it is now storing back-up data disks at [SENSITIVE INFORMATION REDACTED] as its primary disaster recovery site. The TSC stated that once the secondary site is established at [SENSITIVE INFORMATION REDACTED], back-up disks will be stored there as well. Also, the TSC stated that as of April 16, 2005, the TSC has had the capability at [SENSITIVE INFORMATION REDACTED] to run all TSDB software as well as connect to end-user databases for data export. However, we were not provided any documentation to support the formalization of the protocol related to the back-up disk locations or to support the export capability at [SENSITIVE INFORMATION REDACTED].

With respect to the basic security safeguards of the TSC's main facility, the TSC stated that it has recently made modifications to its facility in an effort to improve security. Further, the TSC stated that it [SENSITIVE INFORMATION REDACTED] has submitted requests to the Office of Management and Budget to move its personnel to a stand-alone secure facility. The TSC said it anticipates authorization for this move later in FY 2005, but must wait for additional funding.

As a result, this recommendation can be closed when we receive evidence from the TSC to support: 1) the back-up data disk storage locations, 2) the data export capability at [SENSITIVE INFORMATION REDACTED], and 3) all facility modifications discussed in the TSC's response.

39. Resolved. The TSC agreed with this recommendation and stated that it has taken steps to address it. Specifically, the TSC provided evidence that it performed a disaster recovery COOP exercise on April 16, 2005. According to the TSC, this test was the first instance of quarterly training that will be the normal course of business for the organization. The TSC further stated that it has been exploring the option of using one of two sites as a remote TSC COOP location, and will continue to coordinate the execution of a COOP site.[72]

[72] The results of the COOP exercise indicated that the TSC should pursue a disaster recovery site [SENSITIVE INFORMATION REDACTED].

This recommendation can be closed when we receive evidence from the TSC that quarterly training will be its normal course of business. We also request that the TSC inform us of its progress in establishing a remote COOP location.

40. Closed. The TSC agreed with this recommendation and reported that it transferred the Encounter Management database to a classified network on February 2, 2005. As a result, this recommendation is closed.