Order Code RL32366

Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6

April 21, 2004

William J. Krouse
Analyst in Social Legislation
Domestic Social Policy Division

Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6

Summary

In Homeland Security Presidential Directive 6 (HSPD-6), the Administration announced plans to establish a Terrorist Screening Center (TSC), as a multi-agency effort to be administered by the Federal Bureau of Investigation (FBI), where several watch lists are being consolidated into a single terrorist screening database (TSDB). The TSC is the latest of three multi-agency efforts undertaken by the Administration to better identify, screen, and track known terrorists, suspected terrorists, and their supporters. The other two are the Foreign Terrorist Tracking Task Force (FTTTF) and the Terrorist Threat Integration Center (TTIC). According to the Administration, the TSC complements the FBI-led FTTTF's efforts to prevent terrorists from entering the United States, and to track and remove them if they manage to enter the country. The TTIC serves as a single locale where terrorism-threat data from all sources are further analyzed to more critically focus on terrorism.

Certain terrorist identification and watch list functions previously performed by the Department of State's Bureau of Intelligence and Research (INR) have been transferred to the TTIC and TSC under HSPD-6. At the TTIC, intelligence analysts are building a Terrorist Identities Database (TID) based on TIPOFF — the U.S. government's principal terrorist watch list database prior to HSPD-6. From TID records, TSC analysts are building a consolidated TSDB. The Administration plans to widen access to, and use of, lookout records by making them available in a "sensitive but unclassified" format to authorized federal, state, local, territorial and tribal authorities; to certain private sector entities; and to certain foreign governments.

Merging watch lists will not likely require integrating entire systems, but there are likely to be technological impediments to merging watch list records. From system to system, and watch list to watch list, there remains no standardization of data elements, such as, name, date of birth, place of birth, nationality, or biometric identifiers. While elevating and expanding the terrorist identification and watch list function is an important step in the wider war on terrorism, additional work will remain to upgrade and integrate other consular and border management systems, criminal history record systems, and biometric systems.

HSPD-6 presents significant opportunities to more effectively share data and increase security, but there are risks as well, not the least of which is the potential loss of privacy and the erosion of civil liberties. In recent hearings, Members of Congress have raised several related issues. For example, is the TSDB fast, accurate, comprehensive, and accessible? Have procedures been established to allow persons, who may be misidentified as terrorists or terrorist supporters, some form of redress and remedy if they are denied civil rights or unduly inconvenienced by a screening agency? Does the establishment of the TSDB require new guidelines and oversight mechanisms to protect privacy and other civil liberties? Or, are existing agency policies under which such data is collected sufficient? Is the FBI the best agency to administer the TSDB? Are the TSC and TSDB, and by extension the TTIC, temporary or permanent solutions? This report will be updated as needed.

Contents

List of Figures

List of Tables

Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6

Introduction

This report analyzes Homeland Security Presidential Directive 6 (HSPD-6) and issues relating to (1) the establishment of a Terrorist Screening Center (TSC), (2) the transfer of certain terrorist identification and lookout record distribution functions from the Department of State to the Terrorist Threat Integration Center (TTIC) and the TSC, and (3) the consolidation of terrorist watch lists into a single, stand-alone, terrorist screening database (TSDB) under the direction of the Federal Bureau of Investigation (FBI) at the TSC. In recent hearings, Members of Congress have raised several issues regarding the establishment of the TSDB. For example,

- Has the Administration committed enough resources to ensure the timely establishment of an integrated terrorism watch list (the TSDB)?
- Is the TSDB fast, accurate, comprehensive, and accessible?
- Have procedures been established to allow persons, who may be misidentified as terrorists or terrorist supporters, some form of redress and remedy if they are denied civil rights or unduly inconvenienced by a screening agency?
- Does the establishment of the TSDB require new guidelines and oversight mechanisms to protect privacy and other civil liberties? Or, are existing agency policies under which such data is collected sufficient?
- Is the FBI the best agency to administer the TSDB?
- Are the TSC and TSDB, and by extension the TTIC, temporary or permanent solutions?

While this report identifies some privacy issues associated with the establishment of a consolidated terrorist screening database, it is not intended to serve as an in-depth legal analysis of the issues related to national security, privacy, and the government's need for information to combat terrorism. Rather, it is a systematic examination of the mission and functions of the TSC in relation to other entities like the TTIC. It also identifies and describes key watch lists, residing in

several computerized systems and databases,[1] that likely will be consolidated at the TSC.

HSPD-6 and Terrorist Watch List Consolidation

In HSPD-6[2] and an accompanying memorandum of understanding (MOU),[3] the Administration announced plans to establish the TSC, as a multi-agency effort to be administered by the FBI, where several watch lists will be consolidated into a single terrorist screening database (TSDB).[4] The *MOU on the Integration and Use of Screening Information to Protect Against Terrorism* was signed by Secretary of State Colin Powell, Attorney General John Ashcroft, Secretary of Homeland Security Thomas Ridge, and Director of Central Intelligence (DCI) George Tenet on September 16, 2003. The measures outlined in HSPD-6 and the MOU can be viewed as an outgrowth of the Administration's *National Strategy for Homeland Security*, which reported in July 2002 that the FBI would be establishing a consolidated terrorism watch list that would be "fully accessible to all law enforcement officers and the intelligence community."[5]

According to the Administration's timetable, the TSC was to be operational on December 1, 2003.[6] According to press accounts, however, the Administration informed Representative Jim Turner, the ranking member of the Select Committee on Homeland Security, that the TSC was not "fully" operational as of the end of

---

[1]A computer system is composed of computer(s), peripheral equipment such as disks, printers and terminals, and the software necessary to make them operate together (according to the American National Standards Institute/Institute of Electrical and Electronic Engineers (ANSI/IEEE) Standard 729-1983). A database is an organized body of machine readable data that can be cross-referenced, updated, retrieved, and searched by computer.

[2]The White House, *Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information* (Washington, Sept. 16, 2003). Available at [http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html].

[3]The *Terrorist Screening Memorandum of Understanding* accompanying HSPD-6 is available at [http://www.fas.org/irp/news/2003/09/tscmou.pdf].

[4]Presidents may exercise executive authority by issuing various kinds of directives. Among the oldest of these are executive orders and proclamations, both of which today are usually published in the *Federal Register*. For example, President George W. Bush established the Office of Homeland Security and the initial Homeland Security Council with E.O. 13228 of Oct. 8, 2001. With the establishment of the National Security Council in 1947, there have emerged a series of variously denominated national security directives, but these are not published. Recently, President Bush inaugurated a similar series of Homeland Security Presidential Directives, the first such being issued on Oct. 29, 2001. While these homeland security directives are not published in the *Federal Register*, they are available from the White House Website and appear in the *Weekly Compilation of Presidential Documents*. For further information see CRS Report 98-61, *Presidential Directives: Background and Overview*, by Harold C. Relyea.

[5]The White House, Office of Homeland Security, *National Strategy for Homeland Security* (July 2002), p. 57.

[6]The White House, Fact Sheet: New Terrorist Screening Center Established (Washington, Sept. 16, 2003), at [http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html].

December 2003 and that the Nation's multiple terrorist watch lists have yet to be consolidated.[7] On March 25, 2004, the TSC Director — Donna Bucella — testified that the TSC had established an unclassified, but law enforcement sensitive TSDB. In addition, the TSC was assisting federal screening agencies in identifying terrorists and their supporters with greater certainty, and TSDB lookout records had been made available to nearly 750,000 state and local law enforcement officers.[8]

The TSC is the latest of three multi-agency efforts undertaken by the Administration to better identify, screen, and track known terrorists, suspected terrorists, and their supporters. The other two are the FTTTF and the TTIC. According to the Administration, the TSC complements the FBI-led FTTTF's efforts to prevent terrorists from entering the United States, and to track and remove them if they manage to enter the country. Under the oversight of the DCI, the TTIC serves as a single locale where terrorism-threat data from all sources, foreign and domestic, are further analyzed to more critically focus on terrorism. As part of that function, under HSPD-6, the TTIC will assume a greater role in identifying individuals who are known, or suspected, to be terrorists, or their supporters.

The Administration has transferred certain *terrorist* identification and watch list functions previously performed by the Department of State's (DOS's) INR to the TTIC and TSC. Through a system known as TIPOFF, the DOS's INR identified known and suspected terrorists, produced lookout records, and distributed those records for inclusion in consular and border inspection systems. Prior to HSPD-6, TIPOFF was the Nation's principal terrorist watch list.[9] Based in part on TIPOFF, the member agencies of TTIC have built a TID into which all *international terrorist*-related data available to the U.S. government will be stored in a single repository.[10] With TID records, the TSC is building a consolidated *international* terrorist watch list, which will be merged with *domestic* terrorist watch list records, in the TSDB.

Under HSPD-6 the Administration plans to widen access to, and use of, watch list records by making them available in a "sensitive but unclassified"[11] format to

---

[7]Chris Strohm, "Congressman Blasts Bush on Terrorist Screening Efforts," *Government Executive Magazine*, Jan. 13, 2004, at [http://www.govexec.com/dailyfed/0104/011304c1.htm].

[8]This testimony was given by TSC Director Donna Bucella on Mar. 25, 2004, before a joint hearing held by the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security and the Select Homeland Security Subcommittee on Intelligence and Counterterrorism.

[9]Watch lists are just that, lists of persons who are of interest to visa issuance and border inspection agencies or law enforcement. Persons may be on watch lists to prevent them from acquiring a visa or to prevent them from entering the country, or both. Persons can be excludable from entry for reasons ranging from public health concerns to tax-motivated citizen renunciates, in addition to being known and suspected terrorists, or their supporters. They may also be wanted by law enforcement agencies for questioning or arrest.

[10]The TID is nearly identical to the system that section 343 of the Intelligence Authorization Act for Fiscal Year 2003 (P.L. 107-306, 116 Stat. 2399) required the DCI to establish.

[11]There is no governmentwide definition of "sensitive but unclassified (SBU)." Within (continued...)

authorized federal, state, local, territorial and tribal authorities; to certain private sector entities; and to certain foreign governments.

Hence, HSPD-6 has elevated and expanded the terrorist identification and watch-list functions, which were previously performed by the DOS's INR for immigration-screening purposes. Moreover, under HSPD-6, the use of watch lists will be expanded to include data taken from on-going criminal and national security investigations that are related to terrorism. The purpose of these measures is to better identify, watch-list, and screen known and suspected terrorists at U.S. consulates abroad and international ports of entry. Such measures could also better enable the U.S. government to track terrorists within the United States if they manage to enter the country. Yet, at the same time, there are significant risks as well, not the least of which is the potential loss of individual privacy and an erosion of civil liberties. In the Intelligence Authorization Act for Fiscal Year 2004,[12] Congress has required the President to report back to Congress on the operations of both the TTIC and TSC.

Terrorist Watch-Listing Prior to HSPD-6

A primary goal of lookout systems and watch lists has been to prevent terrorist attacks, by excluding known or suspected terrorists and their supporters from entry into the United States. Under HSPD-6, the use of watch lists would be expanded to better screen such persons at consular offices and international ports of entry, and to better track them both abroad and, if they manage to enter the United States, at home.

Watch Lists and Lookout Books. The DOS's Bureau of Consular Affairs (CA) and the federal border inspection services, until recently the U.S. Customs Service and the Immigration and Naturalization Service (INS), have long maintained watch lists (or lookout books) for the purpose of excluding "undesirable" persons from the United States. Customs and immigration inspection activities are now carried out by the Bureau of Customs and Border Protection (CBP) at the Department of Homeland Security (DHS).[13] While these watch lists/lookout books were just that

---

[11](...continued)
certain limits set out in statutes and presidential directives, agencies have discretion to define SBU in ways that serve their needs to safeguard information that is unclassified but should be withheld from the public for a variety of reasons. The reasons for safeguarding such information, are likely to include maintaining the privacy rights of individuals and the integrity of ongoing inquiries and investigations. A provision in the Homeland Security Act of 2002 (§892 of P.L. 107-296, 116 Stat. 2253) requires the President to implement procedures to safeguard SBU information that is homeland security-related. For further information, see CRS Report RL31845, *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy*, by Genevieve J. Kneso.

[12]P.L. 108-177, Stat. 2622-2625.

[13]Until the establishment of DHS, federal border inspection services included the Department of the Treasury's Customs Service, the Department of Justice's INS, the Department of Agriculture's Animal and Plant Health Inspection Service (APHIS), and the Department of Health and Human Service's Public Health Service. The Homeland Security (continued...)

— bound paper volumes — the development of computers, computer software, and computer connectivity/networking, allowed these agencies to develop and more efficiently search watch list records during the 1970s and 1980s.

Beginning in 1987, the DOS began keeping watch list (lookout) records on known and suspected terrorists through a system known as TIPOFF. While the DOS had maintained computerized visa records since 1965, including watch lists, the events surrounding the first World Trade Center bombing in 1993 prompted the CA to accelerate the development of the Consular Lookout and Security System (CLASS), so that, among other records, TIPOFF-generated terrorist watch list records could be more easily and efficiently searched by computer at U.S. consular posts and embassies abroad. Consular, intelligence, immigration, and law enforcement officers nominate individuals for inclusion in TIPOFF.

The INS, meanwhile, maintained its own watch list database known as the National Automated Immigration Lookout System II (NAILS II) — a system that is currently maintained by the DHS's Bureau of Immigration and Customs Enforcement (ICE).[14] While the bulk of NAILS II records are related to aliens who have either been removed, failed to depart, or failed to show up for removal hearings, NAILS II includes terrorism-related lookouts as well.

In 1988, Congress mandated the development of the Interagency Border Inspection System (IBIS). This system, previously maintained by the Customs Service, allowed the DOS, INS, and Customs to share watch lists, including terrorist lookout records, at international ports of entry. This system is currently maintained by the DHS's CBP.

Prior to HSPD-6, DOS's INR culled through terrorism-related reports produced by the Intelligence Community[15] to identify individuals as known or suspected terrorists, or their supporters. INR also processed cables — known as Visa Vipers — from consular officers abroad when they learn of individuals associated with

---

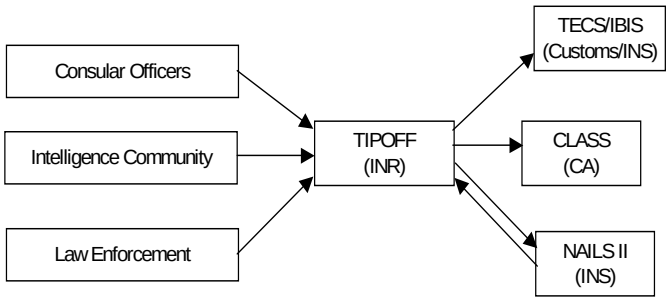
[13](...continued)
Act dismantled INS and transferred its constituent parts, along with Customs and elements of APHIS, to DHS. The border inspection programs of these agencies have been consolidated in DHS's Border and Transportation Security Directorate, as the CBP.

[14]Following the establishment of the DHS, pursuant to P.L. 107-296 (116 Stat. 2135), the Administration merged the investigation branches of the former INS and Customs Service into ICE, along with the immigration detention and removal program, Customs Air and Marine Interdiction program, and the Federal Protective Service. More recently, the Air Marshals program was transferred from the Transportation Security Administration (TSA) to ICE.

[15]The Intelligence Community includes the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); the National Geospatial-Intelligence Agency (GIA); the National Reconnaissance Office (NRO); the other DOD offices that specialize in national intelligence through reconnaissance programs; the intelligence components of the Army, Navy, Air Force, Marine Corps, and Air Force, the FBI, the Department of Energy, and the Coast Guard; the INR at the DOS, the Office of Intelligence and Analysis at Department of the Treasury, and elements of the DHS that are concerned with the analyses of foreign intelligence information (50 U.S.C. §401a(4)).

terrorism. And, INR processed similar data provided by federal law enforcement agencies to produce terrorism-related lookout records. These records were stored in TIPOFF — a classified system. Declassified TIPOFF records were then exported into CLASS, IBIS, and NAILS II. Also, lookout records produced by immigration officers were exported from NAILS II into TIPOFF. See **Figure 1** below.

Figure 1. TIPOFF and Immigration/Border Inspection Systems



Source: Adopted by the Congressional Research Service from a Department of State presentation.

As underscored in recent public testimony, however, watch lists were only as good as the information contained in them, and the agencies responsible for producing these lookout records — principally DOS's INR and DOJ's INS — were dependent upon the information they received from the Intelligence Community and federal law enforcement.[16]

Terrorism-Related Ground for Inadmissability. According to the U.S. government, the term "terrorism" means "the premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience."[17] Prompted by the assassination of President William McKinley in 1901, Congress passed legislation in 1903 to exclude from entry into the United States noncitizens who were anarchists, or who advocated the violent overthrow of the U.S. government.[18] As a security measure during the First World War, the DOS and Department of Labor (DOL)[19]

---

[16]See testimony of Mary Ryan, former Assistant Secretary of State for Consular Affairs, Department of State, and Doris Meissner, former Commissioner, Immigration and Naturalization Service, Department of Justice, before the National Commission on Terrorist Attacks upon the United States, Jan. 26, 2004. At [http://www.9-11commission.gov/hearings/hearing7.htm].

[17]This definition of "terrorism" is taken from 22 U.S.C. §2656f(d). U.S. Department of State, *Patterns of Global Terrorism 2002* (Washington, Apr. 2003), p. xiii.

[18]P.L. 57-162, 32 Stat. 1213.

[19]In 1891, Congress established the office of Superintendent of Immigration in the (continued...)

jointly issued an order in 1917, which required noncitizens to acquire visas from U.S. Consuls abroad and present their visas and passports to U.S. inspectors upon arrival in the United States. This wartime requirement was codified in 1918,[20] and was made a permanent feature of U.S. immigration law in 1924.[21] This requirement was continued by the Immigration and Nationality Act (INA) of 1952.[22]

Visa issuance has long been viewed as a means of preventing undesirable persons, including suspected spies, saboteurs and subversives, from entering the United States. In the Immigration Act of 1990, Congress amended and substantially revised the grounds for exclusion in the INA, including new provisions related to the exclusion of terrorists from the United States.[23] These terrorist exclusion provisions were subsequently amended and widened by the Antiterrorism and Effective Death Penalty Act[24] and the Illegal Immigration and Immigrant Responsibility Act in 1996,[25] and by the USA PATRIOT Act in 2001.[26]

Under the INA, an alien is inadmissible if there is reasonable ground to believe the alien (1) has engaged in terrorist activity; (2) is engaged or is likely to engage in terrorist activity; (3) has, under certain circumstances, indicated an intention to cause death or serious bodily harm, or incited terrorist activity; (4) is a representative of a foreign terrorist organization designated by the Secretary of State, or a political, social, or other similar group whose public endorsement of acts or terrorist activity the Secretary of State has determined undermines U.S. efforts to reduce or eliminate terrorist activities; (5) is a member of a foreign terrorist organization designated by the Secretary of State; or (6) has used his/her position of prominence within any country to endorse or espouse terrorist activity, in a way that the Secretary of State

---

[19](...continued)
Department of the Treasury. The immigration functions remained at Treasury until 1903, when they were transferred by Congress to the Department of Commerce and Labor. In 1906, the immigration and naturalization functions were consolidated in the Bureau of Immigration and Naturalization. In 1913, Congress transferred the Bureau to the newly established DOL, splitting the immigration functions between a Bureau of Immigration and a Bureau of Naturalization. The immigration and naturalization functions were combined again in 1933, as the Immigration and Naturalization Service (INS). In 1940, President Franklin Delano Roosevelt transferred INS to the Department of Justice. The Homeland Security Act of 2002 (P.L. 107-296) abolished INS, transferring its immigration functions to the DHS.

[20]Act of May 22, 1918, 40 Stat. 559.

[21]Act of May 26, 1924, 43 Stat. 153, 156, 161.

[22]INA §§211, 212(a)(7), 221, 8 U.S.C §§1181, 1182(a)(7), 1201.

[23]INA §212(a)(3)(B)(i), 8 U.S.C. §1182(a)(3)(B)(i), as amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 (P.L. 107-56).

[24]P.L. 104-132, 110 Stat. 1214.

[25]P.L. 104-208, 110 Stat. 3009-546.

[26]P.L. 107-56, 115 Stat. 272.

has determined undermines United States activity to reduce or eliminate terrorism activities.[27]

Diplomatic Considerations. More than 2½ years following the September 11, 2001 attacks, there is considerable momentum to watch-list additional persons as known or suspected terrorists, or their supporters. Nevertheless, the exclusion or watch-listing of persons for ideological or political beliefs has long been a source of controversy. While it is clearly within the U.S. government's mandate to screen and track persons who are intent on inciting or engaging in terrorist activities, the determination of who may be a member or supporter of a foreign terrorist organization and, therefore, be prevented from entering the United States or be subject to police surveillance is ultimately a subjective consideration made by intelligence analysts and special agents based on the best information available.[28]

Failures to Identify, Watch-List, and Screen 9/11 Hijackers

Despite measures following the first World Trade Center bombing to more effectively identify and screen known and suspected terrorists, all 19 hijackers who participated in the September 11, 2001 attacks had been issued visas by the DOS in accordance with statutorily required watch-list name checks and other visa issuance requirements, and had entered the country legally. While watch lists will never contain the names of all terrorists, it is generally agreed that members of the Intelligence Community possessed sufficient information to watch-list at least two, possibly three, of the al Qaeda hijackers. Better use of watch lists may have at least disrupted the activities of the September 11, 2001 hijackers.

According to the congressional 9/11 Joint Inquiry, the Intelligence Community missed repeated opportunities to watch-list two of the hijackers, Khalid al-Mihdhar and Nawaf al-Hazmi.[29] By January 2001, the CIA had identified al-Mihdhar and al-Hazmi from surveillance photos of a major meeting of known al Qaeda operatives in Kuala Lumpur, Malaysia on January 5 and 8, 2000. In the same month, the CIA obtained a copy of al-Mihdhar's Saudi passport. It was also known that al-Mihdhar

---

[27]P.L. 101-649, 104 Stat. 4978. For more information on the process of designation of foreign terrorist organizations and other related foreign terrorist lists, see CRS Report RL32120, *The "FTO List" and Congress: Sanctioning Designated Foreign Terrorist Organizations*; and CRS Report RL32223, *Foreign Terrorist Organizations*, both by Audrey Cronin.

[28]Section 212(d) of the INA provides the Secretary of Homeland Security with authority to waive the inadmissibility of members and supporters of foreign terrorist organizations, if it is in the national interest to do so. Under current law, such visa denial waivers would be granted at the request of the Secretary of State.

[29]U.S. Congress, U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After The Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd sess., S.Rept. 107-351, H.Rept. 107-792 (Washington: GPO, 2002), p. 12.

had been issued a U.S. visa in Jeddah, Saudi Arabia, in April 1999, which was valid through April 2000. Nevertheless, the CIA did not watch-list him.[30]

On January 15, 2000, al-Mihdhar and al-Hazmi entered the United States at Los Angeles International Airport (LAX). By March 2000, the CIA had learned that al-Hazmi — an experienced Mujahadeen[31] — had entered the United States through LAX. For about five months, al-Mihdhar and al-Hazmi stayed in San Diego, taking flight lessons. In addition to being in contact with an FBI confidential informant in San Diego, they were also in contact with another September 11, 2001 co-conspirator — Hani Hanjour, who subsequently piloted American Airlines Flight 77 into the Pentagon. On June 10, 2000, al-Mihdhar departed the United States; on July 12, al-Hazmi applied to the INS for a visa extension. Al-Hazmi moved to Phoenix, AZ, linked up with Hanjour, and subsequently overstayed his visa.[32]

By late May 2001, the CIA transferred to the FBI the surveillance photos of the January 2000 Kuala Lumpur meeting. While al-Mihdhar and al-Hazmi were identified, along with Khallad bin-Atash, a leading al Qaeda operative and planner of the USS Cole bombing, neither the CIA nor the FBI watch-listed them. On June 13, 2001, with a new passport, al-Mihdhar obtained another U.S. visa in Jeddah. He falsely stated on the visa application that he had never been to the United States. He reentered the United States at John F. Kennedy (JFK) airport in New York City on July 4, 2001.

On the request of the CIA, al-Mihdhar and al-Hazmi were watch-listed on August 23, 2001 — less than three weeks before the September 11, 2001 terrorist attacks.[33] While FBI agents in Phoenix and Minneapolis were following up other leads that may have led them to the September 11, 2001 conspirators, the repeated failures by the Intelligence Community — principally the CIA and FBI — to watch-list al-Mihdhar and al-Hazmi were crucial lost opportunities associated with the September 11, 2001 attacks, according to the 9/11 Joint Inquiry.[34]

More recently, the National Commission on the Terrorist Attacks Upon the United States, known as the Kean Commission for its Chair — Thomas H. Kean, characterized these lost opportunities to watch-list al-Mihdhar and al-Hazmi as "failures." The Commission purports that there was evidence to watch-list Salem al-Hazmi — Nawaf al-Hazmi's brother as well. Despite the efforts of key INR officials who developed TIPOFF, the Kean Commission found that within the Intelligence

---

[30]Ibid., p. 145.

[31] Mujahadeen, in the sense used here, are fighters trained in insurgent and terrorist techniques, often in training camps sponsored by or associated with al Qaeda. In the context of the 1979-1989 war in Afghanistan, the Mujahadeen were often Muslim men from other countries who fought with the indigenous Afghan guerillas against the Soviets. Some of these Mujahadeen later formed the core of the al Qaeda movement.

[32]U.S. Congress, *Joint Inquiry Into Intelligence Community Activities Before and After The Terrorist Attacks of September 11, 2001*, p. 148.

[33]Ibid., p. 152.

[34]Ibid., p. 81.

Community "watchlisting" was not viewed as integral to intelligence work; rather it was viewed as "a chore off to the side...."[35]

Elevating and Expanding Terrorist Identification, Screening, and Tracking under HSPD-6

On September 16, 2003, the White House issued HSPD-6, which set in motion several measures to improve intelligence gathering and analysis on terrorists and their activities by establishing additional mechanisms to ensure secure, effective, and timely interagency information sharing. In other words, getting the right information to the right people, securely and at the right time. The centerpiece of HSPD-6 is the establishment of the TSC — the latest of three multi-agency efforts undertaken by the Administration to better identify, screen, and track known terrorists, suspected terrorists, and their supporters. The other two are the FTTTF and the TTIC, both of which are described in greater detail below.[36]

Besides establishing the TSC, HSPD-6 transferred the terrorist identification and watch list functions previously performed by the DOS's INR to the TTIC and TSC. The TIPOFF system was developed by the DOS's INR to identify, watch-list, and screen terrorists and their supporters. Consular, immigration, and customs officers used TIPOFF-generated lookout records to exclude terrorists from entry into the United States and, if they managed to enter, to remove them from the United States. As part of its larger mission to assess terrorist threats, under HSPD-6, TTIC's member elements are now charged with identifying foreign terrorists as well. The TSC is charged with consolidating terrorist watch lists and making that data available in a useful format to screening agencies, and the FTTTF, with assisting federal law enforcement agencies with tracking foreign terrorists at home and abroad.

Foreign Terrorist Tracking Task Force (FTTTF). On October 30, 2001, President George W. Bush directed that the FTTTF be established as part of Homeland Security Presidential Directive 2 (HSPD-2).[37] On August 6, 2002, the Attorney General placed the FTTTF administratively within the FBI. As a multi-agency effort, the mission of the FTTTF is to provide federal law enforcement agencies with the best possible information to: (1) prevent foreign terrorists and their supporters from entering the United States; and (2) locate, detain, prosecute, or remove them if they manage to enter the United States. Since the issuance of HSPD-2, the mission of the FTTTF has evolved. While the FTTTF continues to assist

---

[35]National Commission on Terrorist Attacks upon the United States, "Three 9/11 Hijackers: Identification, Watchlisting, and Tracking," Staff Statement no. 2, (Washington, 2004), p. 1.

[36]Other examples of interagency groups include the Secret Service's Document Security Alliance Groups, the Migrant Smuggling and Trafficking in Persons Coordination Center, and the Data Management Improvement Act Task Force. For further information on interagency efforts, see CRS Report RL31357, *Federal Interagency Coordinative Mechanisms: Varied Types and Numerous Devices*, by Frederick M. Kaiser.

[37]The White House, *Homeland Security Presidential Directive-2, Subject: Combatting Terrorism Through Immigration Policies*, Oct. 29, 2001. Click on [http://www.whitehouse.gov/news/releases/2001/10/20011030-2.html].

federal investigators in locating terrorism-related suspects, much of its original mission to screen terrorists at ports of entry has been passed on to the TSC, as is more fully described below.

In many areas, the FTTTF has facilitated and coordinated information sharing agreements among participating agencies and commercial data providers. By accessing and analyzing this data, the FTTTF assists counterterrorism investigations being conducted by the FBI's National Joint Terrorism Task Force (National JTTF)[38] and 84 regional Joint Terrorism Task Forces (JTTFs).[39] By data-mining public and proprietary data systems, the FTTTF can track the "electronic footprints" of known and suspected terrorists.[40] In so doing, the FTTTF assists the 85 JTTFs nationwide, the 56 FBI field offices, the 46 FBI legal attaches[41] abroad, and the DHS in locating suspected terrorists and their supporters.

Besides the FBI, key FTTTF players include the DOD, the DHS CBP and ICE, the DOS, the Social Security Administration, the Office of Personnel Management, the Department of Energy, and the CIA. The FTTTF has also established liaisons with Canada, Australia, and the United Kingdom. The FTTTF was funded for FY2004 as a stand alone line item in the FY2004 Consolidated Appropriations Act in the amount of nearly $62 million.[42] Congress provided the same amount in FY2003 as well.[43]

Terrorist Threat Integration Center (TTIC). In the State of the Union Address, on January 28, 2003, President George W. Bush announced the establishment of the TTIC. On the same date, the While House issued a *Fact Sheet: Strengthening Intelligence to Better Protect America*, which outlined the Center's mission and functions.[44] They include

---

[38]The FBI established the National JTTF in 2002 at the Bureau's Washington command center. The mission of the National JTTF is to collect terrorism-related intelligence and funnel it to the JTTFs, other FBI terrorism units, and partner agencies. Representatives from nearly 30 different agencies are detailed to the National JTTF, bringing outside expertise that includes intelligence, public safety, and state and local law enforcement.

[39]Several JTTFs were first formed in the early 1980s as teams of state and local law enforcement officers, FBI Special Agents, and other federal law enforcement officers. According to the FBI, by combining the assets of different agencies, the JTTFs act as "force multipliers" that allow for greater coverage in the war on terror. There are currently 84 JTTFs.

[40]For further information on issues related to data mining, see CRS Report RL31798, *Data Mining: An Overview*, by Jeffrey W. Seifert.

[41]As part of the Foreign Attache Program, the FBI has established 46 foreign legation offices overseas to establish cooperative efforts with foreign police partners as part of the FBI's domestic law enforcement mission.

[42]P.L. 108-199, 118 Stat. 3.

[43]P.L. 108-7, 117 Stat. 56.

[44]This fact sheet is available on the White House website, at [http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html].

- to optimize the use of terrorist threat-related information, expertise, and capabilities to conduct threat analysis and inform collection strategies;
- to create a structure that ensures information sharing across agency lines;
- to integrate domestic and foreign terrorist-related information and form the most comprehensive possible threat picture; and
- be responsible and accountable for providing terrorist threat assessments for our national leadership.

TTIC became operational on May 1, 2003. John Brennan, a career CIA official, was appointed by the Administration to be the Director of TTIC. An FBI special agent serves as the Center's Deputy Director. Funding for TTIC is provided by participating agencies, including the DHS, DOS, DOJ, DOD, and the Intelligence Community. While TTIC is under the DCI, the Administration emphasizes that it is a "multi-agency joint venture," and is not part of the CIA. TTIC's mission is to form the most comprehensive threat picture possible by serving as a central hub for the fusion and analysis of all-source information collected from foreign and domestic sources on international terrorist threats.

TTIC's operations will encompass elements of both the FBI's Counterterrorism Division (CTD)[45] and the DCI's Counterterrorism Center (CTC).[46] In September 2003, there were about 100 analysts on board at TTIC, and the Administration plans to have about 300 analysts total on board in May 2004, when the Center is scheduled to be moved to a location outside of the CIA.[47] Collocating the DCI's CTC and the FBI's CTD at TTIC is designed to encourage greater cooperation and information sharing between the wider Intelligence Community and the FBI.[48]

In the past, information sharing between the CIA and FBI has been hampered by differing priorities and methods. The CIA is banned from having any role in domestic law enforcement or internal security functions by the National Security Act of 1947,[49] and the DCI is mandated to protect "sources and methods from unauthorized disclosure."[50] Like the CIA, the FBI also protects its sources and methods — particularly the identities of confidential informants, so as not to jeopardize on-going investigations.

---

[45]The mission of the FBI's CTD is to detect and deter terrorist acts within the United States, and to investigate terrorist attacks against U.S. interests and the American people at home and abroad.

[46]The mission of the DCI's CTC is to exploit all-source intelligence to produce in-depth strategic and tactical analyses of terrorist groups. The CTC also coordinates the Intelligence Community's counterterrorism activities and operations.

[47]Kevin Whitelaw, "Inside the Government's New Terrorism Threat Integration Center," *U.S. News & World Report*, Sept. 15, 2003, p. 31.

[48]See also, CRS Report RL32336, *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress*, by Alfred Cumming and Todd Masse.

[49]50 U.S.C. §403-3(d)(1).

[50]50 U.S.C. §403-3(c)(7).

The FBI, however, is also bound by other criminal laws and guidelines related to protecting grand jury information and limiting criminal investigations, undercover operations, and covert surveillance that are, in large part, designed to protect privacy and civil liberties. Consequently, the CIA takes a long-term strategic view of intelligence gathering and analysis, while the FBI takes a short-term tactical view that is geared towards resolving investigations.[51]

Nevertheless, according to the Administration, TTIC will not collect intelligence; instead, as the primary consumer of terrorism-related intelligence, one of the Center's core functions is to ensure information-sharing across agency lines. TTIC is also responsible for setting requirements and tasking other federal agencies in the area of shared databases. The Attorney General is responsible for ensuring that the FBI's information technology modernization programs are configured to share information easily with TTIC.

In terms of more broadly disseminating intelligence reports, an administration official has recently testified that TTIC's Information Sharing Program Office has worked to reduce the number of terrorism-related documents and records that are not under "originator control," meaning the information contained in those records could compromise sources and methods. Consequently, before another agency uses that document or record, it must gain the permission of the originating agency.

Other methods being employed more frequently at TTIC are "writing for release" and "tear lines."[52] Writing for release means producing useful, but less sensitive intelligence reports. Tear lines are employed to divide reports. The substance of the information appears above the tear line, and the sources and methods by which the information was acquired appears below the tear line.

To effect rapid interagency information-sharing, TTIC has established a classified web-accessible service — TTIC Online. TTIC is developing less sensitive mirror images of TTIC Online to more broadly disseminate information and analysis to appropriate entities.[53] See **Figure 2** below.

TTIC will also establish and maintain the TID, which will be a repository for all-source information on known and suspected terrorists.[54] The TID is envisioned

---

[51]Frederick P. Hitz and Brian J. Weiss, "Helping the CIA and FBI Connect the Dots in the War on Terror," *International Journal of Intelligence and Counterintelligence*, spring 2004, vol. 17, no. 1, p. 13.

[52]Russell E. Travers, TTIC Associate Director for Defense Issues, Statement Before the National Commission on Terrorist Attacks Upon the United States, Jan. 26, 2004, p. 7.

[53]Testimony of John Brennan, Terrorist Threat Integration Center Director, in U.S. Congress, Senate Judiciary Subcommittee on Immigration and Border Security (Washington, Sept. 23, 2003), p. 2.

[54]The TID is nearly identical to a system required under section 343 of the Intelligence Authorization Act for Fiscal Year 2003 (P.L. 107-306, 116 Stat. 2399), which requires the DCI to establish a "terrorist identification classification system" that would be a list of individuals who are known or suspected terrorists, and organizations that are known or

(continued...)

as becoming the primary source for international terrorist data provided by TTIC to the TSC. Such information will include names, aliases, dates and places of birth, identification and travel documents, unique and distinguishing physical features, biometric data, and individuals' past affiliation with terrorist acts or groups. In the past, much of this information was stored in disparate databases maintained by several agencies. Consolidating and expanding this data could remedy systemic weaknesses that in the past prevented intelligence analysts and investigators from positively identifying known and suspected terrorists.

To build the TID and prevent duplication of effort, functions of the DOS Bureau of Intelligence and Research's TIPOFF system — particularly those aspects related to the identification of foreign terrorists — have been transferred to TTIC. The entire TIPOFF database of about 120,000 names is now the core of the TID. TIPOFF staff have been split, with part going to the TTIC and part going to the TSC. Under HSPD-6, the President directed all heads of executive departments and agencies to provide to TTIC on a continual basis all appropriate data regarding terrorists and related activities to the extent that the law allows. In turn, TTIC is to provide the TSC with all appropriate information. See **Figure 2** below.

TTIC and IAIP Reporting Requirements. Unlike the FTTTF, the establishment of TTIC has generated some controversy.[55] Some Members of Congress have questioned whether the functions currently assigned to TTIC, like intelligence fusion and threat assessment, would not be better housed in DHS's Directorate for Information Analysis and Infrastructure Protection (IAIP), as the Homeland Security Act gave responsibility for all-source terrorist threat analysis to the new department.[56] In September 2003, William Parrish — the former DHS Acting Assistant Secretary for Information Analysis — testified that DHS will overlay TTIC-generated threat assessments on IAIP-identified vulnerabilities, so that protective measures can be developed and implemented.[57] In other words, with TTIC-generated threat information, IAIP could be better equipped to identify and prioritize the nation's critical infrastructure that needs to be more closely guarded so that security resources can be more efficiently deployed.

---

[54](...continued)
suspected terrorist organizations.

[55]For further information, see CRS Report RS21283, *Homeland Security: Intelligence Support*, by Richard A. Best, Jr.

[56]The House Select Committee on Homeland Security and the Committee on the Judiciary held a hearing on TTIC on July 22, 2003. The Senate Judiciary Subcommittee on Immigration and Border Security held a hearing on HSPD-6, in which the role of TTIC was questioned, on Sept. 23, 2003.

[57]Testimony of William Parrish, Acting Assistant Secretary for Information Analysis, in U.S. Congress, Senate Judiciary Subcommittee on Immigration and Border Security (Washington, Sept. 23, 2003), p. 2.

Regarding the respective roles of the DHS's IAIP and the DCI's TTIC, Section 359 in Intelligence Authorization Act for Fiscal Year 2004[58] requires the President to submit a report to the appropriate committees of Congress[59] by May 1, 2004, on the operations on both the IAIP Directorate and TTIC. This provision sets out that this report should include the following elements:

- an assessment of the operations of the IAIP and TTIC;
- an assessment of the ability of TTIC to carry out the responsibilities assigned to it by the President;
- an assessment of the ability of IAIP to carry out the responsibilities assigned to it under section 201 of the Homeland Security Act;[60]
- an action plan to bring TTIC to full operational capacity as outlined in the President's State of the Union address, including milestones, funding, and sources of funding;
- a delineation of responsibilities and duties for the IAIP and TTIC;
- a delineation and summary of overlapping areas of responsibilities and duties carried out by IAIP, TTIC, and any other element of the federal government;
- an assessment of where these areas of overlap, if any, represent an inefficient use of resources;
- a description of the policies and procedures adopted by IAIP and TTIC to ensure compliance with the Constitution, any applicable statues, executive orders, and regulations of the United States;
- an assessment of the practical impact that TTIC operations, if any, may have on individual liberties and privacy; and
- any other information the President deems appropriate that provides a fuller explanation as to why TTIC should be established as a "joint venture" of participating agencies rather than as an element of IAIP.

This provision sets out further that the report be presented in an unclassified format, which may include a classified annex if necessary.

Terrorist Screening Center (TSC). According to the Administration, the primary mission of the TSC is to consolidate all federal terrorist watch lists into a consolidated terrorist screening database, so that all federal agencies would have access to the best and most complete information. A TSA official, Donna Bucella, has been detailed to the FBI and appointed head of the TSC. A DHS official, Richard Kopel, has been appointed second-in-command at the TSC. As a multi-agency effort, the Center's staff will include designees from the DOS, DOJ, and DHS, as well as other intelligence community entities. TSC personnel are to be given access to TTIC databases, including the TID, as well as any relevant intelligence that advances terrorist screening.

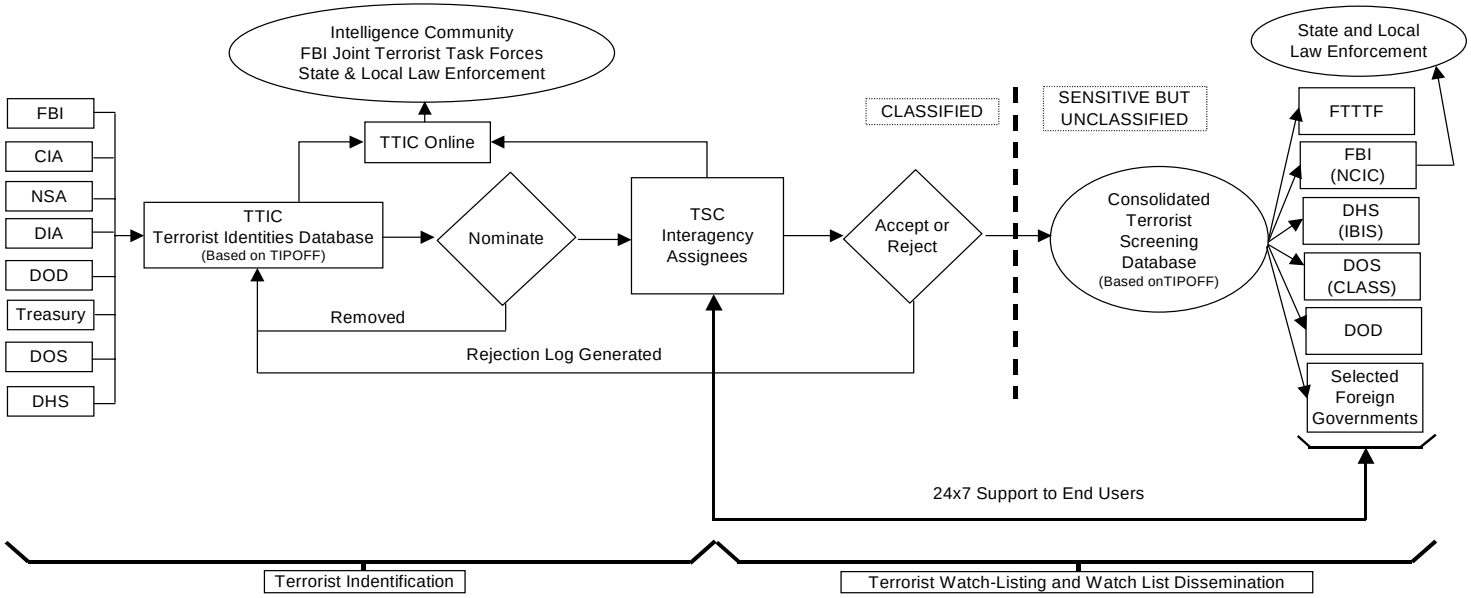
---

[58]P.L. 108-177, 117 Stat. 2622.

[59]For purposes of this provision the appropriate committees of Congress include the Senate committees on Intelligence, Governmental Affairs, the Judiciary, and Appropriations; and in the House, the committees on Intelligence, Homeland Security, the Judiciary, and Appropriations.

[60]P.L. 107-296, 116 Stat. 2145.

Figure 2. Terrorist Identification, Watch-listing, and Watch List Dissemination under HSPD-6



Source: Adopted by the Congressional Research Service from a Department of State presentation.

Under HSPD-6, the Administration envisions that terrorist watch lists will be used much more frequently in the future. In the past, terrorism-related watch lists were used principally for purposes of screening noncitizens applying for visas abroad at consular offices and at the border when applying for admission at international ports of entry. Today, as described more fully below, state and local law enforcement officers are able to screen persons stopped for routine traffic violations against terrorist TSDB lookout records. See **Figure 2** above.

The TTIC Director, the TSC Director, the heads of federal departments or agencies, or their designees "nominate" persons for inclusion in the TSDB by notifying either the TTIC or the FBI. The TSC Director is responsible for establishing procedures to review these records when new information is developed concerning the persons about whom the records are maintained. According to the Administration, TTIC is providing international terrorism data, and the FBI is providing domestic terrorism data for inclusion in the TSDB. Both sets of data are merged in the TSC-maintained TSDB.

According to the FBI, international terrorists include those persons who carry out terrorist activities *under foreign direction*. For this purpose, they may include citizens or noncitizens, under the rationale that citizens could be recruited by foreign terrorist groups. Or, noncitizens (aliens) could immigrate to the United States and naturalize (become citizens), having been unidentified terrorists before entry, or having been recruited as terrorists sometime after their entry into the United States. By comparison, domestic terrorists *are not under foreign direction*, and operate entirely within the United States. According to the Administration, when appropriate, both sets of data will include information on "United States persons."[61] Criteria for the inclusion of U.S. persons in the database will be developed by an interagency working group. The term "United States persons" includes U.S. citizens and legal permanent residents (immigrants).

For agencies responsible for screening terrorists, the TSC Director and agency designees will determine the "screening processes" that will be supported and the amount and type of data that will be provided, depending on an agency's mission. Based on recent congressional testimony, it is clear that the TSC is supporting the screening missions of the DOS's CA and DHS's CBP. It is less clear how much support the TSC is providing the DHS's TSA and ICE. To determine whether to allow screening agencies access to certain records, the TSC is to consider, but not be limited to, the following elements:

- the nature of the person's association with terrorism;
- the quality of data, including credibility, reliability, and extent of corroboration;

---

[61]The definition of "United States person" is found at 50 U.S.C. §1801(i): a citizen of the United States, an alien lawfully admitted for permanent residence (as defined §1101(a)(2) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

- the extent of uniquely identifying personal data;
- the authority or authorities under which the data were obtained, and any restrictions on how these data may be shared or used;
- the authority or authorities of the screening entity;
- the circumstances, including changes in the Homeland Security Alert Level, under which screening will occur; and
- the action the screening agency will take if a person is identified as a person in the TSC's terrorist screening database.

These elements serve as a rough guide to what should be included in lookout records. Nevertheless, HSPD-6 does not speak to the issue that the FBI-administered TSC will need to fully assess the missions of many different agencies in order to provide the appropriate amount of information and handling codes in the lookout records, which will then be disseminated from the consolidated TSDB. While departmental and agency designees will have a voice at the table, and each agency will determine which known or suspected terrorists are placed in the respective lookout systems under HSPD-6, the FBI will be the lead agency and likely play an important role in the final decision.

Expanding Use of Terrorist Watch Lists. Prior to September 11, 2001, watch lists were used principally for federal border and transportation security, and law enforcement. In HSPD-6, the Administration has clearly signaled that the use of watch lists will be expanded beyond those purposes traditionally associated with border and transportation security, and federal law enforcement. Under HSPD-6, to the extent permitted by law, the consolidated TSDB will be made available to:

- state, local, territorial, and tribal law enforcement agencies;
- other appropriate state, local, territorial, and tribal authorities;
- private sector entities charged with managing critical infrastructure or organizers of large events (e.g., the Salt Lake City Winter Olympics); and
- foreign governments that have entered into immigration agreements with the United States or that are engaged in the global war on terrorism as partners with the United States.

As described below, the Administration has made such records available to state and local law enforcement, and plans to make such records available in limited cases with foreign governments through the FBI's National Crime Information Center (NCIC) in a sensitive but unclassified format. NCIC is an FBI-administered telecommunications system that allows authorized law enforcement officers, including state and local officers, to access and search several automated databases pertaining to fugitives, missing persons, stolen property, and criminal histories.

In regard to noncitizens, the Attorney General, in consultation with the Secretary of Homeland Security, or their designees at the TSC, is to determine which records are entered into NCIC. For all other persons, the Attorney General is to determine which records relating to alleged terrorists are entered into NCIC. The Secretary of Homeland Security, or his TSC designee, is to determine whether such records should be available to other non-law enforcement authorities at the state, local, territorial, and tribal levels for other purposes. Such purposes may include screening persons when they apply for driver's licenses or licenses to transfer hazardous

material. The Secretary of State, in consultation with the Attorney General, Secretary of DHS, and the DCI, will determine which records will be made available to foreign governments.

TSC Level of Operations. According to the Administration's timetable, TSC operations were to be phased in rapidly, and the center was to be operational by December 1, 2003.[62] According to press accounts, however, the Administration informed Representative Jim Turner, the ranking Member of the Select Committee on Homeland Security, that the TSC was not "fully" operational as of the end of December and that the Nation's multiple terrorist watch lists had yet to be consolidated.[63] Director Bucella publically testified that the TSC was operational on December 1, 2003.[64] According to that testimony, as part of phase one, the TSC has had the ability to

- provide the names and identifying information of known or suspected terrorists to federal, state, and local law enforcement;
- review whether a known or suspected terrorist should be included in the agency watch lists or should be deleted from such lists;
- ensure that persons, who may share a name with a known or suspected terrorist, are not unduly inconvenienced by screening processes conducted by the U.S. government; and
- adjust or delete outdated or incorrect information to prevent problems arising from misidentifications.[65]

On March 25, 2004, Director Bucella testified before a joint hearing of the House Judiciary Committee's Crime, Terrorism and Homeland Security Subcommittee and the Select Homeland Security Committee's Intelligence and Counterterrorism Subcommittee.[66] In that testimony, Director Bucella reported that phase two of the TSC's implementation had been completed and an unclassified but law enforcement sensitive TSDB had been established. As of April 1, 2004, the TSDB contained about 79,289 lookout records.

Through March, the TSC had provided DOS's CA with 54,000 security advisory opinions, of which 90 were related to terrorism, and 56 resulted in visa revocations. In addition, the CBP's National Targeting Center Director, Charles Bartoldus, testified that CBP officers were routinely working with the TSC to evaluate and assess potential matches between terrorist lookout records and individuals applying for admission into the United States. With TSC's assistance, CBP inspectors are

---

[62]U.S. Department of Justice, *Fact Sheet: Terrorist Screening Center*, Sept. 16, 2003, at [http://www.fbi.gov/pressrel/pressrel03/tscfactsheet091603.htm].

[63]Chris Strohm, "Congressman Blasts Bush on Terrorist Screening Efforts," *Government Executive Magazine*, Jan. 13, 2004, at [http://www.govexec.com/dailyfed/0104/011304c1.htm].

[64]Donna Bucella, Terrorist Screening Center Director, Testimony Before the National Commission on Terrorist Attacks Upon the United States, Jan. 26, 2004, p. 1.

[65]Ibid., p. 2.

[66]This hearing can be viewed by webcast at [http://www.house.gov/judiciary/crime.htm].

currently able to resolve potential matches more expeditiously, resulting in the more timely release of individuals who have been misidentified. Members also asked Director Bucella about the TSC's interactions with the DHS's TSA, but it was less clear from her responses whether TSA was consulting with the TSC about terrorism-related hits in the Computer Assisted Passenger Profiling System.

Furthermore, TSDB-generated lookout records are currently being disseminated to state and local law enforcement officers through the NCIC. The unclassified portion of TSDB-generated lookout records (name, date of birth, passport number, and country of origin) have been loaded into the NCIC's Violent Gang and Terrorist Organizations File (VGTOF). According to Director Bucella, the TSC has set up a protocol for when NCIC queries by state or local law enforcement officers result in a terrorism-related hit.

When NCIC terrorism-related hits occur, the state and local officers stand by, while their dispatchers contact the TSC. Through the dispatchers, the TSC operators will elicit certain information from the state or local officers to determine whether there is a match. Such information could include identifiers, like height, weight, eye color, hair color, tattoos, or scars, which may be classified. If the TSC deems that a match has been made, the TSC will contact the FBI Counterterrorism Watch unit (CT Watch unit) at FBI headquarters.

If needed, the CT Watch unit will contact and consult the appropriate JTTF and designated case officer. Following such consultations, the TSC operators will provide the state and local officers with the most appropriate course of action. Such actions include four possible scenarios: arrest, detain and question, question and release, or proceed with normal police procedure. According to Director Bucella, the TSC is able to process most state and local NCIC terrorism-related hits within 20 to 30 minutes.

The TSC is presently engaged in a large-scale outreach program to inform state and local law enforcement agencies about the TSC. Some Members at the hearing, however, questioned whether most state and local agencies were aware of the TSC or the changes to NCIC's VGTOF. They also questioned whether some federal law enforcement units, like the Border Patrol, had access to NCIC, and whether such queries were routinely made on aliens attempting to enter the country between ports of entry.

As part of this outreach process, the TSC is also working with those agencies to determine if the TSDB could be incorporated into screening processes conducted by those agencies. In addition, the TSC is contacting other federal agencies to determine whether they have terrorism-related records that would be of use to the TSC. In this regard, several members raised concerns that the Department of Defense had not done enough to transfer terrorism-related data to the TSC, and possibly the TTIC, concerning al Qaeda and Taliban combatants who had been previously detained at Guantanamo, but who had subsequently been released. Director Bucella indicated that some data regarding these persons had been transferred to the TSC.

Director Bucella outlined phase three of the TSC implementation. By December 2004, the TSC is scheduled to use the TSDB as a single, integrated system for entering known and suspected terrorist identities. At that point, the TSDB will be integrated ("dynamically linked") into all appropriate screening processes. In addition, selected private sector entities, such as operators of critical infrastructure facilities or organizers of large events, will be allowed to submit lists of persons associated with those events to the U.S. government to be screened for any connection with terrorism. Meanwhile, the DOS is working to establish mechanisms by which terrorist screening information can be shared with foreign countries cooperating with the United States in global efforts to counter terrorism.

Legal Safeguards. The TSC Director is responsible for developing policies and procedures related to criteria for inclusion into the database; and measures to be taken in regard to misidentifications, erroneous entries, outdated data, and privacy concerns. As described above, according to TSC Director Bucella, procedures have been developed regarding the inclusion of persons in the TSDB, the correction of erroneous data, the purging of outdated data, and the incorporation of new data to prevent further misidentifications of persons who share the same or similar names as persons for whom terrorism-related lookout records exist.

The Administration maintains that since the TSC does not collect intelligence, and has no authority to do so, that all intelligence or data entered into the TSDB has been collected in accordance with the preexisting authorities of the collecting agencies. Nonetheless, these existing agency policy and procedures probably do not address information sharing with private entities for security purposes. Members of Congress and other outside observers have questioned whether there should be new policy and procedures at different levels (such as, visa issuance, border inspections, commercial aviation security, domestic law enforcement, and security of public events) for the inclusion of persons in the TSDB.[67]

Also, Members have asked how a person would find out if they were in the TSDB, and if so, how did they get there? In congressional testimony, Director Bucella surmised that a person would learn of being in the TSDB when a screening agency encountered them and, perhaps, denied them a visa or entry into the United States, or arrested them. Director Bucella also suggested that the TSC would probably be unable to confirm or deny whether the person was in the TSDB under current law.

Consequently, persons who have been identified or misidentified as terrorists or their supporters by the TSC would have to pursue such matters through the screening agency. However, the screening agency might not have been the source of the record in which case, a lengthy process of referrals may have to be initiated. Under such conditions, persons identified as terrorists or their supporters may turn to the Freedom of Information Act (FOIA) or the Privacy Act as a last alternative.

---

[67]For further information, see CRS Report RL31730, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, by Gina Marie Stevens.

Under FOIA,[68] any person, including a noncitizen or nonpermanent resident, may file a request with any executive branch agency or department, such as the DOS or DHS, for records indicating they are on a watch list. Under national security and law enforcement FOIA exemptions, the Departments may withhold records on whether an individual is on a watch list.[69]

In addition to a FOIA request, a citizen or legal permanent resident may file a Privacy Act[70] request with DHS and/or Justice to discern whether the TSA or the FBI has records on them. However, the law enforcement exemption under the Privacy Act may permit the Departments to withhold such records. Under the Privacy Act, a citizen or legal permanent resident may request an amendment of their record if information in the record is inaccurate, untimely, irrelevant, or incomplete. Under both FOIA and the Privacy Act, there are provisions for administrative and judicial appeal. If a request is denied, the citizen or legal permanent resident is required to exhaust their administrative remedies prior to bringing an action in U.S. District Court to challenge the agency's action.

The Administration has pledged that terrorist screening information will be gathered and employed within constitutional and other legal parameters. While the Privacy Act generally does not restrict information-sharing related to known and suspected terrorists who are not U.S. persons for the purposes of visa issuance and border inspections, it does restrict the sharing of information on U.S. persons (citizens and legal permanent residents) for purely intelligence purposes, who *are not* the subject of on-going foreign intelligence or criminal investigations.[71]

Consequently, legal questions concerning the inclusion of U.S. persons in these systems under criminal or national security predicates may arise. Protocols have been established for state and local law enforcement to cover the eventuality that a positive NCIC VGTOF hit indicates that they have encountered a known or suspected terrorist. However, it is unclear whether protocols have been established for false positives if a person is misidentified. In addition, questions of compensation for persons mistakenly damaged by inclusion in these databases will likely be an issue.

TSC Reporting Requirements. Section 360 of the Intelligence Authorization Act for Fiscal Year 2004[72] requires the President to submit a report to Congress by September 16, 2004 on the operations of the TSC, as established under HSPD-6. This provision sets out that this report should include the following elements:

---

[68]5 U.S.C. §522.

[69]5 U.S.C. §§522(b), (c), 522a(j).

[70]5 U.S.C. § 522a.

[71]Department of State, *Testimony to the Joint Congressional Intelligence Committee,* p. 5.

[72]P.L. 108-177, 117 Stat. 2623.

- an analysis of TSC operations to ensure that the TSC does not violate the Constitution, or any statute, executive order, or regulation of the United States;
- a description of the TSC database architecture, including the number of databases operated or maintained by the TSC, and an assessment of the extent to which these databases have been integrated;
- a determination of whether the data from all the watch lists, enumerated in the GAO report entitled *Information Technology: Terrorist Watch Lists Should be Consolidated to Promote Better Integration and Sharing* (described below), have been incorporated into the consolidated terrorist screening database system;
- a determination of whether any other databases ought to be integrated into the consolidated terrorist screening database;
- a schedule setting out the dates by which identified databases, which are not yet integrated into the consolidated terrorist screening database system, would be integrated into that system;
- a description of the protocols that have been established to ensure the protection of classified and sensitive information that is contained within the consolidated terrorist screening database;
- a description of processes that have been established to ensure that the information in the consolidated terrorist screening database is systematically and frequently reviewed for timeliness and accuracy;
- a description of the mechanism that has been established to ensure that the information in the consolidated terrorist screening database is synchronized and replicated throughout that database;
- a description of the extent to which, and the criteria under which, the TSC makes the information in the consolidated terrorist screening database available to the private sector and critical infrastructure components;
- the number of individuals listed in the consolidated terrorist screening database;
- the estimated budget of, and sources of funding for, the TSC for each of the fiscal years 2004, 2005, and 2006;
- an assessment of the impact of the TSC and the consolidated terrorist screening database on current law enforcement systems;
- the practical impact, if any, of TSC operations on individual liberties and privacy; and
- such recommendations as the President deems appropriate for modifications to law or policy to ensure the continued operations of the TSC.

This provision requires further that the report be presented in an unclassified format, which may include a classified annex if necessary.

Selected Watch List, Criminal, and Biometric Systems

To provide border and transportation security, a number of federal agencies have long maintained watch lists, or lookout books, for the purposes of excluding certain "undesirable" aliens, including known and suspected terrorists, from travel to, and entry into, the United States. These watch lists reside on consular and border management computer systems, as well as on criminal history record computer systems. In addition, to identify individuals with greater certainty, several biometric

systems have been developed in parallel with these systems. It is notable that most of these systems were developed separately and for different purposes that reflect agency-specific missions and legal authorities.

The U.S. government's principal terrorist watch list system has been the DOS's TIPOFF system, which is classified. While the other members of the Intelligence Community have begun culling through their intelligence reports and producing additional lookout records, prior to September 11, 2001, the staff of INR's TIPOFF produced by far the lion's share of terrorist lookout records. For the purposes of visa issuance and border inspections, TIPOFF lookout records are loaded into two unclassified systems: CA's CLASS and DHS's IBIS.

CLASS is a computerized system used to manage visa applications, among other consular-related activities. Border inspectors use the IBIS system to process travelers entering the United States at international ports of entry.[73] Many agencies compile watch lists for law enforcement and other purposes, which are also loaded into IBIS. Hence, inspectors act as agents of these agencies when processing travelers. As an integrated system, IBIS allows inspectors to seamlessly and simultaneously search several law enforcement and border management databases.

While data sharing between some of these systems is routine, with others it is not. For example, declassified lookout records are downloaded from TIPOFF and uploaded into the DOS CLASS system and the NAILS II, a legacy INS system that is currently maintained by DHS's ICE. Prior to TIPOFF's transfer, this was done weekly, but priority cases could be uploaded into IBIS within minutes if needed. At the TSC, it will be done daily, if not more often. In turn, NAILS II records are uploaded into TIPOFF, since immigration officers produce terrorist-related lookout records as well. It is likely that these practices will be continued at the TSC, but it is unknown how frequently or in what manner they will be accomplished. Until required to by the USA PATRIOT Act, the DOJ was unwilling to share criminal history records with the DOS, including terrorist lookout records contained in NCIC.

Merging watch lists will not likely require integrating entire systems. Nonetheless, there are likely to be other technological impediments. For example, from system to system, and watch list to watch list, there remains no standardization of data elements, such as, name, date of birth, place of birth, or nationality. In the past decade, digitized biometrics (principally fingerprints) have been used increasingly to identify individuals with greater certainty, but most biometric systems have been developed separately from other systems. Integrating data from biometric systems, such as IAFIS and IDENT, into either the TID or the TSDB could be

---

[73]In most cases, the U.S. Border Patrol — formerly part of the INS — does *not* have access to IBIS, since Border Patrol agents were and are responsible principally for monitoring territory between land border ports of entry, rather than screening travelers at ports of entry, as customs and immigration inspectors do. As a consequence, some apprehended aliens who are paroled, or released on their own recognizance, into the United States, are not checked against watch lists or criminal history record systems. Initiatives are underway to provide agents with lap top computers, which include access watch lists and other data in a SBU format, but most Border Patrol stations do not have access to IBIS for reasons of cost and logistics.

technologically difficult and costly. Under HSPD-6, the TTIC director has been charged with the responsibility for setting uniform system standards for watch list records.

At the same time, while elevating and expanding the terrorist watch list function under HSPD-6 is an important step in the wider war on terrorism, specialists in the area of national security have observed that homeland (border) security could be improved by upgrading and integrating existing consular/immigration and border management systems, criminal record history systems, and biometric systems.[74]

GAO Watch List Recommendations. In April 2003, the General Accounting Office (GAO) issued a report that included findings and several recommendations regarding terrorist watch lists. GAO found that at least nine agencies maintained 12 terrorist and criminal watch lists that were used principally for border security or law enforcement purposes. GAO reported that data sharing was hampered by incompatible system architectures — computer hardware, software, and networking. Therefore, GAO recommended that a central authority (leadership), spanning several departments and agencies, be made responsible for standardizing and consolidating watch lists. According to GAO, the new system should be developed to allow agencies to effectively carry out their missions by enforcing all relevant laws in their unique operational environments.[75] At a minimum, lookout records from at least some of these systems (described below) would likely be incorporated into the TSDB.

Of the 12 systems listed by GAO that include watch lists, nine are described below. **Table 1** below lists these nine systems and the departments and agencies responsible for maintaining them. The systems that GAO listed, which are not described below, include the U.S. Marshals' "wants and warrants" file, the U.S. Air Force Office of Special Investigations' Top 10 Fugitive List, and U.S. Central Bureau for Interpol's terrorism watch list. These lists were not included in the treatment below because: the Marshals' wants and warrants file is incorporated into NCIC; the Air Force list is small by comparison to the rest; and Interpol records were reviewed by the FBI and INR for inclusion in NCIC and TIPOFF. At the TTIC, it is likely that Interpol records will continue to be reviewed for inclusion in the TID and, by extension, in the TSDB.

While not included in the GAO study, the Regional Information Sharing System/Law Enforcement Online (RISS/LEO) is described below, because state and local investigators support this system. Not only could RISS/LEO be used to share lookout records with state and local law enforcement, but investigative files could also be shared in some cases. In terms of biometric technology, two systems figure prominently, IAFIS and IDENT. Furthermore, Justice has recently built a biometric

---

[74]Lee S. Strickland, J.D., and Jennifer Willard, M.L.S., "Reengineering the Immigration System: As Case for Data Mining and Information Assurance to Enhance Homeland Security," *Homeland Security Journal*, Oct. 2002, p. 9.

[75]For further information, see GAO Report GAO-03-322, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing* (Washington, Apr. 2003), p. 28.

capability into NCIC. Brief mention is also given to State's Consolidated Consular Database, which serves as a central repository for all visa applications, including digitized visa photos and, in some cases, fingerprints.

Table 1. Selected Lookout, Border Security, Criminal History, and Biometric Computer Systems

Department	Agency	System
State	Bureau of Intelligence and Research	TIPOFF
State	Bureau of Consular Affairs	Consular Lookout and Support System (CLASS)
DHS	Bureau of Immigration and Customs Enforcement	National Automated Immigration Lookout System II (NAILS II)
DHS	Bureau of Customs and Border Protection	Interagency Border Inspection System (IBIS)
DHS	Transportation Security Administration	Selectee Process (CAPPS)
DHS	Transportation Security Administration	No Fly List (CAPPS)
Justice	Federal Bureau of Investigation	National Crime Information Center (NCIC)
Justice	Federal Bureau of Investigation	Integrated Automated Fingerprint Identification System (IAFIS)
DHS	Bureau of Customs and Border Protection and Bureau of Immigration and Customs Enforcement	IDENT

Source: Table prepared by the Congressional Research Service.

TIPOFF.[76] TIPOFF is a *classified* computer lookout system, which was maintained by the DOS's INR to identify and watch-list known and suspected terrorists.[77] Created in 1987, it originally consisted of 3x5 index cards in a shoe box. TIPOFF staff used specialized computer search engines to systematically cull through all-source data, from highly classified central intelligence reports to intelligence products based on open sources, to identify known and suspected terrorists. These classified records are scrubbed to protect intelligence sources and methods, and biographic identifiers are declassified, and exported into lookout systems (CLASS and IBIS). Consular officers can query these records electronically in CLASS to deny visas to terrorists and their supporters. Immigration and customs inspectors query these records in IBIS to deny terrorists entry into the United States at international ports of entry.

---

[76]Briefing with DOS's Bureau of Intelligence and Research, Oct. 23, 2003.

[77]For several years past, the INR was expanding TIPOFF to include records on known and suspected international criminals and drug traffickers as well. Under HSPD-6, this function will remain at INR.

Following the 1993 World Trade Center bombing, the Visa Viper process was established, as a dedicated/secure telegraphic channel that allows consular and intelligence officers to report known and suspected terrorists to INR for inclusion in TIPOFF. There are more than 120,000 records of terrorists and other criminals in TIPOFF, nearly double the number on September 11, 2001. Due to the use of aliases among terrorists, some of these records involve the same individuals. There are nearly 81,000 distinct individual terrorist names in TIPOFF.

Until recently, all subjects of TIPOFF records were non-U.S. persons — roughly speaking those persons who are not legal permanent residents (immigrants) or citizens of the United States. Under HSPD-6, the terrorist identification process currently performed by INR will be expanded and transferred to TTIC. A mirror image of INR's TIPOFF system has been built at TTIC to feed terrorist lookout records into a terrorist identities database (TID). Since September 11, 2001, other members of the Intelligence Community have combed through their products and case files to identify additional terrorists who should be excluded from entering the United States. As part of these efforts, records on U.S. persons (citizens and legal permanent residents) who are the subject of ongoing criminal or national security investigations will be entered into the TID as well. The process performed by INR of declassifying lookout records and exporting them to the appropriate consular, border security, and law enforcement agencies has been transferred to TSC.

Consular Lookout and Support System (CLASS).[78] The CLASS system is the DOS's principal unclassified lookout database that is used by consular officers abroad to check the names of visa and passport applicants against several watch lists that are maintained for various purposes, including screening known and suspected terrorists. While the DOS has maintained an automated visa lookout system since 1970, the development of CLASS was accelerated after the first World Trade Center bombing and the conspiracy to blow up the Holland and Lincoln Tunnels, and the United Nations Headquarters, in New York City.[79]

In terms of name recognition, the CLASS system is the most advanced lookout system currently maintained by the federal government. It includes a compressed name search capability, as well as sophisticated Arabic, Russian/Slavic, East Asian, Hispanic, date of birth, and country of birth algorithms. The language algorithms, for example, search for variations in name spelling based on the phonetic transliteration of names from other languages into the Roman alphabet. The algorithm scores the searches to arrange them in order of likelihood of a match. All consular posts can directly access CLASS online. There are about 15.4 million

---

[78]Briefing with DOS's Bureau of Consular Affairs, Oct. 23, 2003.

[79]The case of Sheikh Omar Abdel Rahman is illustrative. He had been implicated in the assassination of Egyptian President Anwar Sadat in 1981 and watch-listed, yet he was issued a visa in Khartoum, Sudan. At the time, the Khartoum consulate lookout records were on microfiche and there were several variations of Rahman's name. He was convicted for his part in the conspiracy to blow up the Holland and Lincoln Tunnels, and the United Nations Headquarters, in New York City.

records in CLASS, including 90,000 records on suspected or known terrorists and their supporters.[80]

National Automated Immigration Lookout System II (NAILS II).[81] The NAILS II system is the lookout system formerly maintained by INS, until that agency was dismantled and its constituent parts were transferred to DHS. Today, NAILS II is maintained by the DHS's ICE. NAILS II contains about 3.8 million files, including biographical and case data on persons who may be inadmissible or are being sought by immigration officers for other reasons related to immigration enforcement. Of these files, 58,000 files concern suspected or known terrorists and their supporters. The NAILS II system can be searched by name, variations on the name, alien registration number, and date of birth. The name recognition technology in NAILS II is Soundex, a technology that was patented some 100 years ago.[82] Lookout records are downloaded from TIPOFF and uploaded into NAILS II on an hourly basis, and from NAILS II into CLASS on a weekly basis, or as needed. At the TSC, this process will be performed daily.

Interagency Border Inspection System (IBIS).[83] The IBIS system, an unclassified system, was maintained by the Department of the Treasury's U.S. Customs Service, until Customs was transferred to DHS. INS was also a major stakeholder in this system, since both Customs and Immigration inspectors screen aliens for admission into the United States at ports of entry.

The IBIS system was congressionally mandated by the Omnibus Drug Initiative Act of 1988[84] in order to share lookout records maintained separately by INS, State, and Customs. The Customs Service supported about 17 different watch lists by downloading lookout records from other agencies into the IBIS. IBIS provides inspectors with the ability to perform a single, all purpose query in the primary inspection lanes.[85] If the system generates a hit, the inspector diverts the traveler to secondary inspection for additional clearance procedures. Developed by the Customs

---

[80]CLASS data on immigrant and nonimmigrant visa holders are downloaded several times daily into IBIS through NAILS II and the Treasury Enforcement Communications System II (TECS II), which are both maintained currently by DHS.

[81]Mark T. Kenmore, "Update on U.S. Ports of Entry," *Immigration & Nationality Law Handbook, 2002-2003 Edition*, vol. 1 (Washington, 2002), p. 257.

[82]Dr. John C. Hermansen, Name-Recognition Technology Aids the Fight Against Terrorism, *Journal of Counterterrorism & Homeland Security International* (winter 2003), p. 2.

[83]Briefing with the U.S. Customs Service, Nov. 16, 2001.

[84]§4604 of P.L. 100-690, 102 Stat. 4289.

[85]In is notable that at land border ports of entry during primary inspections, the border inspectors do not enter the names and other pertinent biographic identifiers of border crossers who arrive in private conveyance into IBIS. Instead, the inspectors enter vehicle license plate numbers into IBIS and visually scan the border crossers' travel documents.

Service, IBIS utilizes the pre-existing TECS II. Today, TECS II and IBIS are maintained by the CBP at DHS.[86]

IBIS exchanges data with CLASS and several immigration systems, including the NAILS II (described above) and the Deportable Alien Control System (DACS), among others. It also allows inspectors to access the FBI's NCIC and National Law Enforcement Telecommunications System (NLETS), as well as the Drug Enforcement Administration's Narcotics and Dangerous Drugs Identification System (NADDIS). The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Secret Service, Internal Revenue Service, and the Royal Canadian Mounted Police (RCMP) also provide lookout records for inclusion in IBIS. Law enforcement and regulatory personnel from 20 other federal agencies use IBIS.

In addition, the Advanced Passenger Inspection System (APIS) was grafted onto IBIS to establish alien entry/exit control in the airport environment (as opposed to land border and sea ports). As required by the Border Security Act (P.L. 107-173), the DHS has rolled out the U.S. VISIT program, a newly developed automated entry/exit control system that includes scanners and readers to verify and collect biometric information on foreign travelers.[87] Under the U.S. VISIT program, IBIS and the APIS interface with two systems with biometric capabilities, IDENT and the Consular Consolidated Database.

As in NAILS II, the name search capability in IBIS is Soundex. While IBIS is considered superior to NAILS II in terms of systems performance and name recognition, it is not considered as robust as the CLASS system in terms of certain search functions. There are about 16 million records in IBIS, including nearly 80,000 records on known and suspected terrorists. In regard to IBIS another key issue for Congress is systems availability. There have been press accounts that IBIS has been inaccessible at certain ports of entry for extended periods of time, during which allegedly foreign travelers were not screened against watch lists.[88]

Computer Assisted Passenger Profiling System (CAPPS).[89] TSA administers the CAPPS system, a classified system, which includes a "selectee" process and a "no fly" list. The operational concept underlying CAPPS is to select "high-risk" travelers based on ticket purchasing patterns, among other things, for greater scrutiny in terms of body and baggage searches, while expediting processing for "low-risk" travelers. The "selectee" process is the core of CAPPS. It was

---

[86]Under an administrative reorganization within the DHS, INS enforcement programs were merged with Customs, and reconstituted as the CBP and the ICE. Both Customs and Immigration Inspectors are now part of CBP.

[87]For further information, see CRS Report RL32234, *U.S. Visitor and Immigrant Status Indicator Technology Program (U.S.-VISIT)*, by Lisa Seghetti and Stephen Vina.

[88]Alfonso Chardy, "Airport Terrorist Database Often Offline; Official Says Backups Are In Place to Prevent Disaster," *Miami Herald*, Mar. 8, 2002, p. B1.

[89]*Federal Register*, Aug. 1, 2003, p. 45265.

authorized in the 1996 Federal Aviation Administration Act.[90] The system was mandated in 1999 by the Federal Aviation Administration, prior to the establishment of TSA, to promote aviation security following several aircraft bombings. In addition, the Aviation and Transportation Security Act[91] authorized the development of a "no fly" list, which is essentially a list of persons who are prohibited from boarding a commercial aircraft for a host of reasons. The actual system, however, was developed and is managed by the airline industry.

More recently, TSA has been testing a second generation system, CAPPS-II, that, among other things, uses sophisticated algorithms to data mine (search) government and proprietary (commercial) databases to acquire limited background information on air travelers to authenticate their identity. Critics point out that terrorists could "beat" the system by adopting another person's identity. They point to the increasing frequency and ease with which criminals engage in identity fraud. In addition, the system will assign travelers a color coded categorical risk assessment.[92]

- Green-coded passengers would not be considered a risk and would only be subject to basic screening procedures — metal detectors and baggage x-rays.
- Yellow-coded passengers would be deemed either unknown or possible risk, and would be subject to extra screening procedures — bag and body searches.
- Red-coded passengers would be considered high risk and would not be allowed to travel, and law enforcement officials would be notified of their attempts to board commercial aircraft.

Critics, however, decry the cloak of secrecy under which TSA is developing CAPPS II. They assert that identity-based profiling under CAPPS II would result in a loss of privacy that would not be counterbalanced by a corresponding increase in security. Because of these fears, others maintain that transparency is vital to the system's further development and success.[93] Some legal scholars also question whether it would be permissible to prevent a person from boarding an aircraft on a mere suspicion of organizational affiliation.[94]

Congress, meanwhile, included Section 519 in the FY2004 Homeland Security Appropriations Act,[95] which prohibits the expenditure of any funding provided under that act to deploy or implement this new system until it has been evaluated by GAO. Since then, GAO has reported that the development of this system is behind schedule, and TSA has encountered major impediments in testing CAPPS II. In particular, the European Union and commercial airlines have been reluctant to hand

---

[90]P.L. 104-848.

[91]See 49 U.S.C. §114(h)(3), or §101 of P.L. 107-71, 115 Stat. 597.

[92]*Federal Register*, Aug. 1, 2003, p. 45266.

[93]Jill D. Rhodes, "CAPPS II: Red Light, Green Light, or 'Mother, May I?,'" *The Homeland Security Journal*, Mar. 2004, p. 1.

[94]Ibid., p. 7.

[95]P.L. 108-90, 117 Stat. 1137.

over crucial data because of privacy concerns. Moreover, GAO underscored that the CAPPS II, as designed, would be vulnerable to terrorists who adopted (stole) another person's identity.[96] TSA anticipates that CAPPS-II will be integrated with US-VISIT, DHS's newly developed automated entry/exit control program.[97] Such a measure would introduce a biometric component into the CAPPS-II process for non-citizens, so that their identities could be confirmed with greater certainty.

National Crime Information Center (NCIC).[98] The FBI maintains the NCIC, a national computer database for criminal justice records. NCIC is linked to an index system — the Interstate Identification Index (III), which points authorized law enforcement authorities to federal, state, and local criminal records. In 1999, NCIC 2000 was brought online by the FBI. Major improvements built into NCIC 2000 include an improved name search capability, digitized right index finger prints and mug shots, other digitized images (tatoos, scars, or stolen vehicles), a sexual offenders file, an incarcerated persons file, a convicted person on supervised release (probation or parole) file, user manuals on line, information linking capabilities, online system support, and other improvements.

Another major enhancement associated with NCIC 2000 is the ability for patrol officers to receive and send data to the system from their patrol cars or other temporary locations with laptop computers, hand-held fingerprint scanners, or digital cameras. The total budget to develop NCIC 2000 was about $183 million.[99] For FY2003, about $36 million was allocated by the FBI to administer and maintain NCIC 2000.

NCIC 2000 gives law enforcement officers access to over 43 million records: 41 million criminal history records and 2.5 million hot files. Hot files would include lookouts on suspected and known terrorists, which are included in the Violent Gang and Terrorist Organization File (VGTOF). As in IBIS and NAILS II, however, the name recognition technology in NCIC 2000 is Soundex, which is not nearly as robust as the name recognition technologies built into CLASS. For example, the length of the name field in NCIC is only 28 characters, while it is over 80 in CLASS.[100]

For years, Justice denied the DOS access to NCIC on the grounds that CA was not a law enforcement agency, but State was given authority to access NCIC in the

---

[96]U.S. General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385, Feb. 2004, p. 4.

[97]*Federal Register*, Aug. 1, 2003, p. 45266.

[98]For further information, click on [http://www.fbi.gov/hq/cjisd/ncic.htm].

[99]U.S. Department of Justice, Federal Bureau of Investigation, National Crime Information Center 2000 (Washington, July 15, 1999), p. 3 at [http://www.fbi.gov/pressrel/pressre199/ncic2000.htm]

[100]Briefing with DOS's Bureau of Intelligence and Research, Oct. 23, 2003.

USA PATRIOT Act.[101] As of August 2002, between 7 to 8 million files on non-U.S. persons with FBI criminal records were added to CLASS from NCIC.[102] When Customs and Immigration inspectors query IBIS in the primary inspection lanes, the system queries NCIC's hot files like the U.S. Marshal Service's want and warrants file and the VGTOF, but full criminal background history checks are only performed when travelers are diverted into secondary inspections for certain irregularities or suspicious behavior. Under HSPD-6, NCIC is the platform on which additional terrorist screening records from the TSC's TSDB have been disseminated to duly authorized state, local, territorial, and tribal law enforcement agencies.[103]

Regional Information Sharing System/Law Enforcement Online.[104] The Regional Information Sharing System (RISS) is an unclassified, but secured web-accessible system of six regional computer networks that were established to share state and local investigative data involving criminal gangs and drug trafficking.[105] RISS is funded through the DOJ Office of Justice Programs, but is administered and operated jointly by several state agencies.

Section 701 of the USA PATRIOT Act[106] amends the Omnibus Crime Control and Safe Streets Act of 1968 to authorize the use of RISS to share investigative data that might involve potential terrorist conspiracies and activities. As required by law, criminal files included in RISS must be based on "probable cause" that the subjects of the file have committed, or are about to commit, a crime.[107] While a cigarette bootlegging conspiracy, for example, may appear to have no terrorism nexus, by analyzing investigative data in RISS, other patterns of criminal or terrorist activity may emerge.

Law Enforcement Online (LEO) is a secured web-accessible portfolio of applications and information sources made available by the FBI to state and local law enforcement agencies. More recently, RISS has been merged with the FBI's LEO system. The RISS/LEO merger will facilitate federal/state communications on a secured/web accessible system, as opposed to older teletype systems like the

---

[101]See §403(a) of P.L. 107-56, 115 Stat. 343.

[102]U.S. Department of State, Testimony to the Joint Congressional Intelligence Committee Inquiry by Ambassador Francis X. Taylor, Coordinator for Counterterrorism (Washington, Oct. 1, 2002), p. 2.

[103]Memorandum of Understanding accompanying HSPD-6, item 18, p. 5.

[104]For further information, click on [http://www.iir.com/RISS/].

[105]Wilson P. Dizard III, "All Points Bulletin: FBI and Justice Link, Get the Word Out," *Post-Newsweek Business Information, Inc.* (Lexus/Nexus: Oct. 7, 2003), p. 1. (Hereafter cited as Dizzard, "All Points Bulletin: FBI and Justice Link.")

[106]P.L. 107-56, 115 Stat. 374.

[107]28 *Code of Federal Regulations*, § 23.3(b)(3). "Criminal intelligence information means data which has been evaluated to determine that it is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity."

NLETS.[108] Through RISS/LEO, the FBI will distribute to state and local law enforcement agencies selected open source (unclassified) reports, as well as sensitive but unclassified law enforcement reports. RISS/LEO enjoys considerable support among state and local law enforcement agencies as a user-friendly and web-accessible system.

Biometric Systems for Identity Verification. "Biometrics" are physical characteristics or personal traits of an individual used to identify him, or verify his claim to a certain identity. Examples of biometrics include fingerprints, facial and hand geometry, iris and retina scans, voice recognition, and handwritten signatures. While most biometric technologies have only been developed in the past 10 to 15 years, fingerprints have been used by law enforcement to verify identity for the past century. For these purposes, the FBI maintains the Integrated Automated Fingerprint Identification System (IAFIS), an automated 10-fingerprint matching system that captures rolled prints. All 50 states are connected to IAFIS. With over 47 million sets of fingerprints, it is the largest biometric database in the world.[109]

In 1995, the INS piloted the Automated Biometric Fingerprint Identification System (IDENT) in California. In the following year, IDENT was deployed to over 34 sites on the Southwest border, and over 3,000 criminal aliens were identified attempting to enter the United States. IDENT is a two flat fingerprint system that includes prints of 4.5 million aliens who have been (1) apprehended while attempting to enter the United States illegally between ports of entry or allowed to withdraw their application for admission at a port of entry (4 million records), (2) previously apprehended (300,000 records), or (3) convicted of aggravated felonies (240,000).

Some Members of Congress, particularly those serving on the Appropriations Committees, were concerned that two incompatible fingerprint identification systems were being developed within the DOJ. This issue became heated following revelations that the INS had apprehended a suspected murderer, Rafael Resendez-Ramirez, but allowed him to voluntarily return to Mexico. Resendez-Ramirez subsequently reentered the United States and committed four additional murders. Language in the FY2000 Commerce-Justice-State appropriations act expressed dismay that other federal, state and local law enforcement officers did not have access to IDENT data. In response, the Attorney General put the IDENT/IAFIS migration project under the supervision of Justice Management Division (JMD).

JMD conducted several pilot programs, which examined the feasibility of interchanging data between the two systems.[110] For example, IAFIS data for

---

[108]Dizard, "All-Points Bulletin: FBI and Justice Link," p. 1.

[109]U.S. General Accounting Office, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174, Nov. 2002, p. 149.

[110]IDENT is instrumental in identifying how many times an alien has been apprehended. According to the DOJ, however, there are legal concerns, about entering such data into criminal databases like IAFIS for aliens who may have attempted to enter the United States illegally, but were not convicted of a criminal violation. Indeed, most aliens attempting to enter the United States illegally between ports of entry are apprehended up to five to seven

(continued...)

individuals in the "wants and warrants" file was downloaded into IDENT. JMD also developed an IDENT/IAFIS workstation that allowed Border Patrol agents and immigration inspectors to run IDENT prints against IAFIS. This system had a 10 minute response time and required agents to process each apprehended person twice, once under IDENT and again through the IDENT/IAFIS work station.

In addition, JMD conducted a criminality study, which examined IDENT records from the 1998 through mid-2000 time frame and found that about 8.5 % of those individuals had some notable charge placed against them.[111] The transfer of the components of the former INS to the DHS, however, has hampered this project. According to the DOJ Office of the Inspector General, despite a delay of two years, a partially integrated version of the IDENT/IAFIS system was available for deployment in December 2003. Full integration and deployment of the system, however, may extend past FY2008.[112] Meanwhile, about 4,500 FBI fingerprint files of known or suspected terrorists have been entered into IDENT.[113]

The DOS, meanwhile, has established the capacity at consular posts abroad to capture electronic records of nonimmigrant visas, including digitized visa photos, which are transmitted and replicated in State's Consolidated Consular Database. In FY2001, DOS and INS conducted a pilot nonimmigrant visa data-sharing program at the Newark International Airport. As part of this program, nonimmigrant visa records were transmitted to IBIS, including digitized photos. These visa photos are useful for identity verification, and reportedly this capability has been deployed at all air ports of entry.

In addition, the DOS has begun testing facial recognition (biometric) technologies with nonimmigrant visa photos as a means to verify identity as well, but these technologies are less mature than those using fingerprint. As a biometric measurement for nonimmigrant visa applicants, however, the DOS strongly favors facial recognition to fingerprints, because it does not require the applicant to submit to an active measurement procedure. In addition, facial recognition biometric measurements can be derived from photos and videotape gathered by the intelligence community in order to identify known terrorists and other persons who may be excludable from the United States for national security reasons.

HSPD-6 directs that the TTIC's TID and the FBI domestic terrorist database incorporate all available biometric data, to the extent permitted by law, including data on persons yet to be identified (e.g., latent prints gathered at a crime scene or the

---

[110](...continued)
times before they are charged with misdemeanor illegal entry. If they are subsequently apprehended, they are charged with felony reentry.

[111]U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, "DOJ Agencies Team Up To Improve The Security At U.S. Borders," *The CJIS Link* (Clarksburg, WV, spring 2002), p. 2.

[112]U.S. Department of Justice, Office of the Inspector General, Report No. 1-2003-005, *Status of IDENT/IAFIS Integration*, (Washington, Feb. 2004), p. 11.

[113]Ibid., 18.

caves of Afghanistan). In addition, these systems are to be designed so that new advancements in biometrics technology can be incorporated into them.

Possible Issues for Congress

While watch lists have long been maintained by law enforcement and border security agencies, the Administration's plans to expand these lists and widen their dissemination raises issues related to individual privacy and the security of the nation. For Congress, several immediate issues have emerged or may emerge, including the following:

- Has the transfer of the TIPOFF terrorist identification function to TTIC and TIPOFF terrorist watch list function to the TSC been accomplished without degrading the capabilities of other governmental entities charged with identifying, screening, and tracking known and suspected terrorists? If not, how and in what way has the system been improved?
- How operational is the TSC at this time? Will the TSDB be fully integrated ("dynamically linked") with the visa issuance, border inspection, commercial aviation security systems by the end of CY2004? Has the Administration committed enough resources to create a single, fully integrated TSDB?
- With the bulk of the Nation's terrorism-related lookout records in a single, integrated TSDB, what measures have and will be taken to insure the security of the TSDB?
- Will the TSC Director have a role in evaluating the security and adequacy of the systems used by screening agencies?
- What measures have been or will be taken to improve the name search capabilities of NCIC and IBIS?
- How expeditiously will the TSC be able to respond to terrorist-related NCIC hits made by state and local law enforcement officers? Is there a bench mark for how long such persons can be stopped for questioning?
- If persons identified as known or suspected terrorists, or their supporters, are not arrested or detained, what governmental entities will be notified of their presence in the United States? What measures will be taken to monitor their whereabouts and activities while in the United States? What other actions might be taken by those to whom the information is disseminated?
- What is the criteria for including persons in the TSDB as suspected or known terrorists, or their supporters? Will sufficient safeguards be put in place to protect constitutional rights? Should policies and guidelines regarding the inclusion of such persons in the TSDB be made public?
- What redress is or will be available to an individual wrongly placed on a watch list? Will there be a formal appeals process? If so, what agency will handle this process?
- What mechanisms will be put in place to audit system users to determine whether they are abusing the system? Should there be associated civil or criminal penalties for such abuse?
- Should Congress consider requiring a statutory authorization for the TSC, the consolidated TSDB, and related activities as a means of assuring greater accountability?

- Are there cultural or tradecraft issues related to information sharing that the FBI and other agencies will need to overcome in order to more effectively share information and properly manage lookout records for other agencies?
- Would the database and watch list functions be better located and consolidated in a single Executive Branch agency with clearer lines of authority and responsibility?
- Finally, are the TSC and TSDB, and by extension the TTIC, temporary or permanent solutions?

Conclusion

There is an emerging consensus that the U.S. intelligence and law enforcement community missed several vital opportunities to watch-list and screen several conspirators involved in the September 11, 2001 terrorist attacks. Under HSPD-6, the Bush Administration has taken steps to elevate and expand terrorist identification and watch-list functions. These measures, if effectively implemented, will better equip the U.S. government to screen and monitor the whereabouts of known and suspected terrorists, and their supporters. Furthermore, working from common terrorist identities and watch list databases could be an effective mechanism to break down institutional and cultural firewalls and promote greater interagency cooperation and data sharing.

Conversely, as the U.S. government pursues a more aggressive policy in identifying and watch-listing known and suspected terrorists, and their supporters, there is significant potential for a corresponding loss of privacy and an erosion of civil liberties. While the Administration asserts that such information will be collected according to preexisting authorities and individual agency policies and procedures, it is inevitable that individuals will be misidentified. In such cases, most would agree that it will be incumbent upon the U.S. government to act swiftly to correct such mistakes, and perhaps compensate those individuals for their inconveniences or possible damages.

Establishing a TSDB by merging watch lists will not likely require integrating entire systems. Nonetheless, there are likely to be technological impediments to merging watch list records. From system to system, and watch list to watch list, there remains no standardization of data elements, such as, name, date of birth, place of birth, or nationality. In the past decade, moreover, digitized biometrics (principally fingerprints) have been developed to identify individuals with greater certainty, but most biometric systems have been developed separately from other systems. Integrating data from biometric systems into either the TID or the TSDB could be technologically difficult and costly.

Under HSPD-6, the Administration has established the TSC as a "multi-agency effort." At the same time, establishing a consolidated TSDB and effectively disseminating lookout records to screening agencies, including state and local law enforcement, is not likely to be a small or short-term endeavor. At this time, congressional input into this process is confined to oversight by several congressional committees and appropriating funding to several participating agencies.

Appendix A. Frequently Used Abbreviations

To aid the reader, the following list of abbreviations is provided.

APIS	Advanced Passenger Information System
CA	Bureau of Consular Affairs
CAPPS	Computer Assisted Passenger Profiling System
CIA	Central Intelligence Agency
CBP	Bureau of Customs and Border Protection
CLASS	Consular Lookout and Support System
CT Watch	Counterterrorism Watch
CTC	CIA's Counterterrorism Center
CTD	FBI's Counterterrorism Division
DCI	Director of Central Intelligence
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOD	Department of Defense
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
FTTTF	Foreign Terrorist Tracking Task Force
HSPD-6	Homeland Security Presidential Directive 6
IAFIS	Integrated Automated Fingerprint Inspection System
IAIP	Information Analysis and Infrastructure Protection Directorate
IBIS	Interagency Border Inspection System
ICE	Bureau of Immigration and Customs Enforcement
IDENT	Automated Biometric Fingerprint Identification System
INA	Immigration and Nationality Act
INR	Bureau of Intelligence and Research
INS	Immigration and Naturalization Service
JMD	Justice Management Division
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Online
MOU	Memorandum of Understanding
NAILS II	National Automated Border Inspection System II
NSA	National Security Agency
NCIC	National Crime Information Center
NJTTF	National Joint Terrorist Task Force
NTC	National Targeting Center
RISS	Regional Information Sharing System
TID	Terrorist Identities Database
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TTIC	Terrorism Threat Integration Center
U.S.-VISIT	U.S. Visitor and Immigrant Status Indicator Technology Program
VGTOF	Violent Crime and Terrorist Organization Fil