

Erasing the Seams: An Integrated, International Strategy to Combat Terrorism

James B. Steinberg

May 3, 2006

Since the attacks of September 11, 2001, the Bush administration and Congress have taken a number of important steps to improve U.S. security against terrorism, not only in the offensive war on terrorism abroad but through protecting the homeland as well. But efforts to date have not adequately redressed one of the most serious flaws of US counter-terrorism strategy: its bifurcation into *domestic* (homeland security) and *foreign* components. This bifurcation pre-dated 9/11, when the threat to the homeland was underestimated by many government agencies, and was carried forward (and the divide in some respects deepened) by the Bush administration's initial response to 9/11. The principal rationale for retaining the domestic/foreign divide was the perceived need to take immediate short-term measures to improve security without risking the time delays and disruption attendant on a more comprehensive rethinking of the pre-9/11 approach, and the preoccupation of the traditional national security community with preparing for military action in Afghanistan.

With the passage of time, there has been ample opportunity to revisit this key question. In some respects there have been major strides in erasing the divide, while other aspects of the counter-terrorism effort have not changed significantly. This report reflects our assessment of the government efforts to date and where we believe further action is necessary.

Our study did not assume that dividing the foreign and domestic dimensions of counter-terrorism is per se undesirable. Rather, in each case it is necessary to weigh the costs and benefits of integration and bifurcation, keeping in mind that while efficacy of the counter-terrorism effort is and ought to be the dominant consideration in assessing desirable structures and organization, other factors legitimately need to be taken into account. These include civil liberties, the need to pursue other policy agendas, which

might be adversely affected by consolidating domestic and foreign counter-terrorism efforts, and bureaucratic and political costs associated with “reform.”

Erasing the Seams: An Integrated, International Strategy to Combat Terrorism

Our study emphasizes five priority areas that we selected on the basis of four criteria: the extent to which there is currently a substantial bifurcation in domestic and international counter-terrorism/intelligence work; the potential impact (either positive or negative) of approaches that would reduce or ameliorate the gap; the plausibility of change (taking into account political, bureaucratic, financial and other constraints); and the “researchability” of the issue (primarily the availability of non-classified information and access to relevant policymakers). The priority issues we identified are the separation of the policy/decision-making machinery into “domestic” and “foreign” processes; the division of intelligence collection and (to a lesser extent) analysis between foreign and domestic collection agencies; the lack of connection between Department of Defense (DoD) planning and operations and the homeland security apparatus; difficulties arising from problems in gaining international cooperation; and the integration of watch lists.

Broadly speaking, it is possible to group current efforts into three categories: areas where the government (Congress and the Executive Branch) has substantially re-engineered processes and substance to integrate foreign and domestic activities; areas where the important institutional and procedural seams remain, but efforts have been made to build better links “across” the seams; and areas where the bifurcation remains dominant.

The most notable efforts falling in the first category include: the creation of the Director of National Intelligence (DNI), with authority over both domestic and foreign intelligence; the creation of the National Counterterrorism Center (NCTC), which, in principle, provides a common home both for analysis and operational planning across the domestic/foreign divide; and the extension abroad of Department of Homeland Security’s (DHS) activities, particularly those related to border protection. In each of these cases the government has at least in principle moved to an integrated model, but it is simply too early to tell whether the will exists to see this implemented in fact. In at least one case –

the linkage between foreign and domestic intelligence collection – early results have been disappointing, as the DNI’s nominal authority has not made much headway in breaking down traditional stovepipes. Therefore, the assessments offered below must rely to a considerable extent on the theoretical costs and benefits of the new approach, rather than an empirical assessment of what gains and losses have accrued.

In the second category (separate structures but improved coordination) fall the relationship between foreign (including the Central Intelligence Agency and National Security Agency) and domestic (including the Federal Bureau of Investigation) in intelligence collection, analysis and dissemination, where there has been little operational “integration” but some nascent efforts to build bridges between the activities of the two agencies; and the relationship between the Homeland Security Council (HSC) and the National Security Council (NSC), where distinct organizational arrangements persist, but dual-hatting arrangements facilitate coordination and deconfliction. In the third category (no significant change) are the relationship between the military and domestic homeland security efforts, where historic and bureaucratic barriers remain substantial; and the continued failure to achieve the goal of consolidated watch lists. The remainder of this final report describes our conclusions in each of the priorities we identified.

1) Separation of domestic “homeland” security and foreign “counter-terrorism” policymaking processes.

In the immediate aftermath of 9/11, the Bush administration created the Office of Homeland Security (OHS) in the Executive Office of the President (EOP), and an associated HSC. This organizational response was understandable, given the urgent need to give focus to addressing the deficiencies revealed by 9/11, particularly the critical need for coordination and systematic planning to address the threat of terrorism in the United States. Since the initial creation of the OHS, there has been an evolution, spurred on by experience and by the creation of DHS. Today, DHS has superseded most of the operational responsibilities of the OHS, which retains an advisory and coordinating role. By creating the OHS, the Bush Administration had moved away from the Clinton Administration’s approach (embodied in PDD-62, which lodged the primary

responsibility for counter-terrorism coordination in the NSC).¹ In this respect, the Bush Administration also declined to adopt the approach advocated in 2000 by the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (better known as the Gilmore Commission), which called for a new coordinating body in the White House, but one which would have included both domestic and foreign counter-terrorism activities.²

From the beginning, the administration has struggled with how to ensure the linkages between “homeland security,” under the aegis of the OHS/HSC, and the broader counterterrorism effort, which had been the province of the NSC. Shortly after 9/11, in October 2001, the administration created a new position within the NSC, the national director and deputy national security adviser for combating terrorism, who also served as a deputy to the homeland security adviser on “matters relating to global terrorism inside the United States.” The dual-hatted deputy was responsible for the day-to-day coordination of the response to threat information and was intended to be “the President’s principal advisor on matters related to combating global terrorism, including all efforts designed to detect, disrupt, and destroy global terrorist organizations and those who support them.”³ When Frances Townsend was elevated to homeland security adviser in 2004, for a time she kept the deputy national security adviser position at the NSC. In May 2005, with the appointment of Juan Carlos Zarate to the deputy national security adviser position, it reverted to being a dual-hatted one.

While the dual-hatted homeland security adviser /deputy national security adviser has provided an important bridge for tactical counter-terrorism cooperation through daily interagency meetings involving both domestic (e.g. FBI, DHS) and foreign (CIA, DoD)

¹ With the creation of DHS in November 2002, the role of the OHS evolved; today, DHS has assumed most of the operational responsibilities of the OHS, which retains an advisory and coordinating role.

² In its second report “Toward a National Strategy for Combating Terrorism” in 2000 the Commission had called for establishing a senior level coordination entity in the Executive Office of the President with a statutory basis and “responsibility for the full range of deterring, preventing, preparing for, and responding to international as well as domestic terrorism.”

³ See “Fact Sheet: Bush Names Terrorism, Cyberspace Security Advisors,” October 9, 2001 (www.usembassyjakarta.org/Factsheet_bush.html [July 6, 2005]).

agencies, the homeland security adviser and the national security adviser have not participated regularly in the work of the other's policy council.⁴

Predictably, this bifurcated structure has had a direct impact on the policy framework for counter-terrorism. Perhaps most notably, in 2002, the administration developed two separate policy documents and frameworks to govern "national security" and "homeland security," notwithstanding the fact that the "national security strategy" placed considerable emphasis on counter-terrorism, while the homeland security strategy acknowledged the international dimensions of the problem.⁵

Protecting the homeland requires a seamless connection of efforts abroad, across U.S. borders, and in the United States itself. Therefore, we conclude in our study that the HSC should be merged into the NSC to ensure full integration of the domestic and foreign aspects of counter-terrorism, as well as linkage to other related policy problems, most notably weapons of mass destruction. This conclusion was shared by several other studies of this issue including the report of the 9/11 Commission.⁶ It seems increasingly clear that the separation of the HSC is at best artificial, and at worst counter-productive. The activities of domestic agencies not only directly affect the fight against terrorism abroad, but can also have an impact on other important U.S. foreign policy priorities, as the international backlash against domestic detentions and visa policy has shown. While the Gilmore Commission's approach mentioned above solves the domestic/foreign counter-terrorism coordination problem, it fails to build the linkages to other aspects of national security.

The principal objections to merging the two coordinating bodies and their associated staffs have been the risk of overload on the national security adviser and the need to include agencies in NSC deliberations that have not traditionally participated. The first concern should not be treated lightly. But even today, the national security

⁴ There is considerable overlap between the compositions of the HSC and NSC and the HSA and NSA are invited to each other's Council and principals committee meetings, but both policy councils operate independently.

⁵ *National Strategy for Homeland Security* (Washington, DC: Office of Homeland Security, 2002); *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2002).

⁶ "To improve coordination at the White House, we believe the existing Homeland Security Council should soon be merged into a single National Security Council." National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York, NY: W.W. Norton & Co, 2004) 406.

adviser is often involved in issues concerning the HSC, and given the priority on counterterrorism, it stands to reason that that should be an important focus of the adviser. The creation of the NCTC, which has responsibility for intelligence and operational planning across all agencies, foreign and domestic, is a further impetus, since according to the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act) the NCTC reports to the NSC. Some of the staffing burden can be moved to DHS, which should have a more prominent role in leading the interagency process on many operational aspects of homeland security and response.⁷

Problems associated with including agencies unfamiliar with NSC seem overstated. In recent years many agencies, primarily thought of as domestic, have joined NSC deliberations on appropriate issues—the inclusion of the Department of Health and Human Services and the Centers for Disease Control and Prevention on AIDS and bioterrorism before 9/11 are examples. So the idea of flexibility for NSC processes is nothing new.

Integrating the two councils will not only provide a better opportunity for coordinating strategy, but will also allow “homeland” security efforts to benefit from the more well-established NSC processes, which through long experience and the stature of the national security adviser have proved perhaps the most effective mechanism for inter-agency coordination.

2) Division of intelligence collection and analysis between foreign and domestic collection agencies

The problem of disconnect between foreign and domestic intelligence collection and analysis has been at the heart of post-9/11 analysis of “what went wrong.” There is probably no more glaring example of the problem than the failure of the CIA to alert the FBI and border agencies to the identity of the “Malaysia” conspirators, which might have prevented their entry into the U.S. or at a minimum triggered a more effective post-entry

⁷ The CSIS–Heritage Foundation report *DHS 2.0: Rethinking the Department of Homeland Security* (December 2004) suggested “strengthening the Secretary of Homeland Security’s policymaking function by creating an Undersecretary for Policy” (p. 5).

investigation.⁸ It is very plausible that such an effort might well have thwarted the 9/11 plot, at least in the form that it actually took. Similar disconnects contributed to the failure to identify Zacarias Moussaoui as a “foreign” terrorist, a problem which contributed to the FBI’s failure to seek and obtain a Foreign Intelligence Surveillance Act (FISA) court order prior to 9/11.

The divide between domestic and foreign intelligence has its roots in the 1947 National Security Act, which circumscribed the activities of the CIA in the United States, and was reinforced by the Nixon-era intelligence abuses that led to the Church/Pike Committee hearings, the Levi Guidelines, and the United States Signals Intelligence Directive of the 1970s. These contributed to an atrophy of the “domestic” intelligence functions post mid-1970s, which were almost exclusively focused on counter-intelligence and counter-espionage operations against foreign governments operating in the United States (and to a limited degree against “domestic” extremist groups). In addition to virtually non-existent domestic security capabilities, a high barrier arose between foreign and domestic intelligence activities, a barrier that had its roots in law, the culture of the relevant agencies, and the incompatibility of information storage and retrieval systems that made sharing difficult even when the will existed. To be fair, even among agencies with responsibility for foreign intelligence, sharing was grudging, as each sought to protect its most valuable assets – sources (both human and technical) and the intelligence they produced – from the risk of compromise or inadvertent disclosure.

These tensions between the agencies responsible for domestic and foreign intelligence began to surface in the mid-1990s as terrorist attacks against U.S. personnel and interests abroad began to proliferate. They took many forms, including the failure of the FBI and Justice Department to share information with national security agencies with respect to terrorists and terrorist organizations developed in criminal investigations and grand jury proceedings on the grounds that such sharing would violate Rule 6(e) of the Federal Rules of Criminal Procedure, jeopardize successful prosecutions, and politicize law enforcement decisions. Tensions also arose through competition between the FBI and national security agencies over handling investigations of terrorist activities abroad (such

⁸ Khalid Almihdhar and Nawaf Alhazmi – two of the September 11 hijackers on American Airlines Flight 77 – were known to have been at a meeting in Malaysia of terrorist suspects.

as in the case of the attacks on the Khobar Towers and the American embassies in Africa) and how to prioritize the need for information to allow for successful prosecutions with the need to maintain good liaison relationships with foreign intelligence services. The problems were epitomized by the failure of the NSC and FBI to agree on a Memorandum of Understanding (MoU) governing the sharing of domestically-derived intelligence information with national security agencies. These turf problems were temporarily put aside in connection with the investigation of the Millennium plots in late 1999, but the structural issues remained unresolved up to 9/11.

In 2002, the Congressional Joint Inquiry into intelligence community activities detailed in a report the problems of the “wall” between various agencies, stating that it was “not a single barrier, but a series of restrictions between and within agencies constructed over sixty years as a result of legal, policy, institutional, and personal factors. These walls separate foreign from domestic activities, foreign intelligence from law-enforcement operations, the FBI from the CIA, communications intelligence from other types of intelligence, the intelligence community from other federal agencies, and national-security information from other forms of evidence.” This wall in January 2000 led the CIA to inform the FBI of the activities of one of the future hijackers but not that he had an American visa; in August 2001 it led to FBI headquarters refusing to open a criminal investigation against two “bin-Laden related individuals” on whom it had received information from the CIA since it was “intelligence information.”⁹ This wall was both real and perceived; the 9/11 Commission stated that “agents in the field began to believe – incorrectly – that no FISA information could be shared with agents working on criminal investigations. This perception evolved into the still more exaggerated belief that the FBI could not share *any* intelligence information with criminal investigators, even if no FISA procedures had been used. Thus, relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators.”¹⁰

⁹ Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and US House Permanent Select Committee on Intelligence*, Dec. 2002: 363-368.

¹⁰ National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York, NY: W.W. Norton & Co, 2004) 79.

In the immediate aftermath of the 9/11 attacks some of these problems received immediate attention. The Rule 6(e) and associated barriers were erased by the USA PATRIOT Act of 2001. Congress sought to increase the integration of intelligence sharing through the Homeland Security Act by creating a new intelligence component in DHS and mandating its access (with important limitations) to raw intelligence from both domestic and foreign sources. The administration took a different tack toward addressing this problem through the creation of the Terrorist Threat Information Center (TTIC), which was supposed to broker the sharing of information between both domestic and foreign intelligence agencies, under the joint direction of the FBI and CIA.

But each of these “solutions” failed because they relied on the goodwill of the participating agencies to cooperate, rather than empowering anyone to ensure integration. The embodiment of the limitations of this approach was the TTIC itself, where analysts from various agencies sat in a common room, with access to their “home” agencies’ intelligence, which could be shared manually between analysts at the TTIC but not beyond without permission from the home agencies, and which in any event was separated by physical barriers from access by other agencies.

More generally, the decision to retain the FBI as the principal agency responsible for intelligence collection and counter-terrorism in the United States, rather than create a new agency has had the effect of perpetuating the lack of coordination between foreign and domestic intelligence operations. Conflicts which had already begun to develop pre-9/11 between the CIA and the FBI over the CIA’s activities in the US and the FBI’s activities abroad expanded post-9/11. In particular, the FBI has stepped up recruitment of foreigners in the United States and sought to maintain control over those sources after they return overseas (even while fighting hard to maintain its role as the lead agency for intelligence activities in the United States, in the face of calls for a greater role for DHS/CIA or the creation of a new domestic intelligence agency along the lines of the United Kingdom’s MI5). There have also been recent cases in which FBI agents operating abroad have failed to inform the CIA of their operations. Similarly, the CIA had also begun a limited expansion of its own activities within the territorial United States, based on its authority to take actions (including the recruitment of sources) with

respect to non-US residents and to debrief returning U.S. citizens.¹¹ These efforts risk uncoordinated and potentially conflicting operations. The dangers range from the risk of false corroboration (both agencies receiving reports from a single source but believing that the reports come from two different agents) to compromising sensitive operations. The FBI and CIA had been in negotiations to resolve these conflicts and establish rules governing their respective roles.¹² They have jointly developed a classified MoU to address this problem, which the DNI has approved.¹³

There is another dimension to the problem as well – a state and local one – with actions such as those taken by the New York City Police Department (NYPD), which has placed officers in seven different cities around the world through its overseas liaison program to collect information, among other activities. NYPD officials stated that one reason for this action was that they were being kept out of the loop by the federal agencies and that if they had not taken such a step, they would not have had access to information from those sites; even if they did receive information, they said, it would take months to get it. While their role is limited and does not include participating in enforcement activities or investigations, their efforts are deeply resented by the FBI where, in a complaint that ironically mirrors that of the CIA about the FBI's activities abroad, the feeling is that they add to the confusion about who officially represents the U.S. government. To add to the problem, there is little coordination: for example, a NYPD officer stationed in Israel had little, if any, contact with the FBI agent working out of the embassy in Tel Aviv.¹⁴

To some extent, the failure to find effective ways to erase the seams is a function of the FBI's incomplete efforts to transform itself into an effective counter-terrorism/intelligence agency. It is difficult for the FBI to cooperate with agencies focused on foreign intelligence when the bureau lacks well-trained agents of its own,

¹¹ Dana Priest, "CIA Is Expanding Domestic Operations; More Offices, More Agents with FBI," *Washington Post*, October 23, 2002, p. A02.

¹² Mark Sherman, "FBI, CIA Seek Ground Rules on Intelligence," *Associated Press*, January 28, 2005; Robb-Silberman Commission, *Report to the President of the United States*, pp. 468–71.

¹³ "CIA, FBI Agree Intelligence Roles, Officials Say," Reuters, June 12, 2005; See "Bush Administration Actions to Implement WMD Commission Recommendations," June 29, 2005 (www.whitehouse.gov/news/releases/2005/06/20050629-5.html [July 6, 2005]).

¹⁴ Judith Miller, "A New York Cop in Israel, Stepping a Bit on the FBI's Toes," *New York Times*, May 15, 2005, p. 37.

when its information technology does not allow effective information sharing within the FBI, much less with others, and the stature of the intelligence dimension of the bureau's work remains in the shadow of more traditional law enforcement activities. Even on counter-terrorism, the culture of the bureau tends to reward successful prosecutions rather than intelligence operations per se. While Director Robert Mueller is aware of these problems, and there has been a dramatic increase in resources for intelligence and counter-terrorism, there is still much more "talking the talk" than "walking the walk."

There has been an effort to adapt both technology and training to the new counterterrorism mission in addition to organizational changes like the creation of a Directorate of Intelligence and National Security Branch (NSB), but serious problems remain; some are inherent in the role and culture of the FBI, and changing mindsets is far more difficult than changing organization charts. But many of the problems stem simply from failure to implement a well-considered vision, which would go much farther than adaptation at the margin.

Despite the creation of new roles and reporting relationships as well as new training and career tracks, the FBI still has limited intelligence capability in the field and limited analytical capabilities. Its field intelligence groups (FIGs) have run into both cultural and budgetary obstacles. Analysts at the FIGs lack the standing to task special agents to collect needed intelligence (or hold them accountable) as well as resources such as desktop Internet access.¹⁵ While the number of intelligence reports emanating from the bureau has increased, the quality of intelligence still arouses skepticism, especially in the rest of the intelligence community. The reports emerging from analysts in the field still seemed to be focused on tactical rather than strategic analysis. The overall functioning of the FBI is still highly decentralized, with special agents in charge (SACs) still in control. The focus still tends to be on building cases rather than identifying and assessing potential threats, and there is still a reluctance to work with other agencies, with only marginal linkages in practice. The attempt at upgrading the computer systems proved a

¹⁵ See Alfred Cumming and Todd Masse, "Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress" (Washington: Congressional Research Service, August 16, 2005) (www.fas.org/sgp/crs/intel/RL33033.pdf [September 16, 2005]). See also Siobhan Gorman, "FBI Might Lack Tools to Analyze Terrorism; New Field Units Short of Equipment, Authority, Government Study Says," *Baltimore Sun*, September 14, 2005, 1A.

disastrous failure, with the result that technology is still a major barrier to sharing. The bureau has hired new personnel and retrained old personnel, but retention has proved a problem both at the lower and higher levels (there were five chief intelligence officers over the period 2002–03, and the FBI’s last head of the counterterrorism division was its sixth since 9/11).

To resolve these problems, both the joint inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, and the 9/11 Commission recommended a powerful DNI whose responsibilities would bridge the foreign/domestic divide, to include the military as well as civilian components on the foreign side. After much political tussle, Congress finally enacted the Intelligence Reform Act, which gives the DNI authority over both foreign and domestic intelligence, including military intelligence other than tactical military intelligence. This broad authority to integrate is further strengthened by the creation of the NCTC, which supersedes the TTIC and provides more centralized authority over both analysis and operational planning, although not over counter-terrorism operations themselves.

Our study suggests that the creation of the DNI offers an opportunity to clarify the roles and missions of all the agencies with a potential role in foreign intelligence collection. Whenever possible, the rules should be designed to foster specialization and avoid the hazards of unnecessary duplication and conflict. The FBI should be responsible primarily for handling foreign intelligence collection in the United States as well as collection on civilians in support of protecting military facilities in the United States. (The FBI already collaborates with the Pentagon’s Counterintelligence Field Activity Group, which is responsible for protecting military infrastructure from terrorist and foreign intelligence agencies’ espionage activities). Sources developed by the FBI in the United States who move abroad should be transferred to CIA handlers. The Robb-Silberman Commission called for formation within the CIA of the Human Intelligence Directorate, which would be responsible for coordinating the work of “all U.S. agencies conducting human intelligence operations overseas” (including the CIA’s own Directorate of Operations).¹⁶ They wanted this directorate to also develop a national

¹⁶ Robb-Silberman Commission, *Report to the President of the United States*, p. 22.

HUMINT strategy, and, as appropriate, integrate collection and reporting systems. As part of its response to these recommendations, the Bush administration emphasized that the CIA's authority over overseas human intelligence operations would be strengthened. A national HUMINT (human intelligence) manager—a senior CIA official—would coordinate human intelligence activities conducted by all agencies abroad.¹⁷ More recently, the DNI and the Director of the CIA announced the creation of a National Clandestine Service (NCS) within the CIA. The senior CIA official who would head the service would also coordinate, but not supervise or direct, the human intelligence operations of all the agencies collecting intelligence overseas.¹⁸ While the office of the DNI “will establish policy related to clandestine HUMINT, the NCS will execute and implement that policy across the IC.”¹⁹ Implementing this initiative correctly is going to be important. The Director of the NCS will have to ensure that all of the agencies, not just a few, consistently coordinate their operations. In the case of state and local agencies with foreign liaisons, the solution is to get the FBI and CIA to cooperate more and be more responsive to the needs of state and local authorities.

For intelligence collection in the United States, we conclude that a separate domestic intelligence agency is still the best option; in lieu of such an agency, the FBI needs to strengthen the sense of a separate intelligence service within the bureau. In implementing the recommendations of the Robb-Silverman Commission, the SACs could be like ambassadors with chief-of-mission responsibilities, but the intelligence side of the bureau should have clear and separate links and the authority to supervise its own agents and analysts. The new security branch will have to work hard to establish itself as an effective player in the intelligence community. In addition, the bureau should work harder to integrate its intelligence function with that of the rest of the intelligence community. A step in the right direction has been the administration's delegation to the DNI of coordination and budgetary authority over the FBI's new NSB.²⁰

¹⁷ Walter Pincus, “CIA, Pentagon Seek to Avoid Overlap,” *Washington Post*, July 4, 2005, p. A02.

¹⁸ See “DNI and D/CIA Announce Establishment of the National Clandestine Service,” October 13, 2005 (www.cia.gov/cia/public_affairs/press_release/2005/pr10132005.html [October 27, 2005]).

¹⁹ See “Fact Sheet: Creation of the National Humint Manager,” October 13, 2005 (www.cia.gov/cia/public_affairs/press_release/2005/fs10132005.html [October 27, 2005]).

²⁰ See “Bush Administration Actions to Implement WMD Commission Recommendations,” June 29, 2005 (www.whitehouse.gov/news/releases/2005/06/20050629-5.html [July 6, 2005]). The administration has

Institutional and organizational changes are necessary but not sufficient to acquire the synergies and benefits achieved by a deeper integration of foreign and domestic intelligence collection and analysis. To a considerable degree, “cultural” barriers inhibit cooperation and will persist even if the wiring diagrams are changed. Even strong centralized authority in the DNI is unlikely to achieve the kind of cooperation necessary if individuals see their mission in terms of their individual agency’s responsibilities rather than the collective good. At the same time, diversity in the intelligence community also has value in that it can broaden the range of expertise available and help avoid group think. For this reason, to combat the “cultural” barriers to collaboration and sharing in the intelligence and counter-terrorism communities, we conclude that there is an urgent need to develop a sense of “jointness” in the intelligence community, drawing on the experience of the military under the Goldwater Nichols Act of 1986, which sought to reduce the traditional tension between the military services that impeded effective warfighting. Every major post-9/11 review has suggested a strategy for this.

Elements of the strategy include career incentives to participate in joint assignments, training, and education and to accept assignment to billets in other services. The Intelligence Reform Act specifically mandated steps along these lines by requiring incentives for service in joint positions such as on the staff of the DNI and the NCTC and for mechanisms for rotating personnel among intelligence agencies and establishing training and education requirements across the community. However, the statute largely exempts military personnel from these provisions.

Following up on the Robb-Silberman Commission’s recommendations, the administration directed the DNI (to be assisted by a chief human capital officer) to develop “creative performance incentives and a ‘joint’ personnel rotation system” and stated that a National Intelligence University system would be established, which could facilitate joint training. A senior training and education officer in the office of the DNI would oversee its establishment and management.²¹ To overcome cultural differences that inhibit joint efforts and to foster a collaborative work ethic and common practices,

also directed a reorganization of the Justice Department so that its intelligence and counterterrorism assets would be brought together under a new assistant attorney general for national security.

²¹ See “Bush Administration Actions to Implement WMD Commission Recommendations,” June 29, 2005 (www.whitehouse.gov/news/releases/2005/06/20050629-5.html [July 6, 2005]).

the Markle Task Force has recommended that the DNI should also develop a common federal government curriculum for intelligence analysts across at least all the agencies involved in counterterrorism; an entry-level core curriculum that would establish a basic standard of training for the intelligence community; and a system of details and exchange assignments that would be required for promotion.²²

The experience under the Goldwater-Nichols Act suggests that effective implementation of these provisions could play a crucial role in changing cultures and breaking down stovepipes, but the barriers to doing so are daunting. Unlike in the military, the concept of rotation is not ingrained in most civilian agencies, which have highly vertical structures, and the ability of the DNI to oversee the personnel policies of highly diverse agencies will prove challenging at a time when other more time-sensitive concerns associated with establishing the new position compete for attention. To date the penalties for inappropriate disclosure of sensitive information are clear and substantial, the rewards for sharing minimal at best. It is vital that the DNI move quickly to adopt procedures to implement these aspects of the Intelligence Reform Act and the recommendations mentioned above to give a strong signal, even to those not serving in a cross-agency appointment, that collaboration and cooperation are the norm for career advancement.²³

Finally, there is a critical need to implement the Information Sharing Environment (ISE) mandated by Congress in the Intelligence Reform Act. The constant turmoil over

²² See Markle Task Force, *Networked Analytic Methods and Tools*.

²³ The Intelligence Reform Act states that the DNI should “provide incentives for personnel of elements of the intelligence community” to serve on his or her own staff, the national intelligence centers, the National Counterterrorism Center, and “in other positions in support of the intelligence community management functions of the Director.” Incentives could be financial or whatever the DNI considered appropriate; promotions would be dependent on what had been assigned or detailed; and the DNI would have to “prescribe mechanisms to facilitate the rotation of personnel of the intelligence community through various elements of the intelligence community in the course of their careers.” It furthermore states, “It is the sense of Congress that the mechanisms prescribed under this subsection should, to the extent practical, seek to duplicate for civilian personnel within the intelligence community the joint officer management policies established by chapter 38 of title 10, United States Code, and the other amendments made by title IV of the Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99-433).” See Intelligence Reform and Terrorism Prevention Act of December 17, 2004 (Public Law 108-458).

the role of the Program Manager and frequent turnover in the position has led to serious challenges in implementing an effective cross-agency information sharing system .²⁴

3) Lack of connection between DoD planning and operations and the homeland security apparatus

For much of American history, there has been a deep reluctance to involve the U.S. military in activities in the United States. Following the experience of the Reconstruction era, Congress enacted a law, which codified this aversion stating that “it shall not be lawful to employ any part of the Army of the United States, as a posse comitatus, or otherwise, for the purpose of executing the laws, except in such cases and under such circumstances as such employment of said force may be expressly authorized by the Constitution or by act of Congress.” Through DoD directives, the law was extended so that the provisions of the “Posse Comitatus Act”, Title 18 of the U.S. Code (USC), Section 1385 would apply not only to the Army and the Air Force but to the Navy and the Marine Corps as well. Through Congressional exceptions, omission, specific directives and interpretation, the law does allow for limited exceptions for domestic use of the National Guard (both in its state and federal capacity) to deal with natural disasters and threats to civic order, but even in the latter case, the deployment of the guard has often been controversial.

Even in areas where the military role is less controversial (e.g., protecting the United States from attack by foreign military forces), the U.S. military had not played a major part especially in the years leading up to 9/11. Defense of American airspace against foreign aircraft atrophied with the end of the Cold War, and while there was growing interest in defending against ballistic missile attacks beginning with President Reagan, little thought or attention went into the possibility of developing systems (both warning and response) to attacks by other means (including “air breathing” threats like cruise missiles). The agency with the greatest focus on threats to U.S. shores from abroad was the Coast Guard, which, although nominally a military service, operated largely as a civilian agency within the Department of Transportation, rather than the DoD, and

²⁴ See “U.S. Intel Chief Defends Info Sharing Efforts,” *UPI*, April 17, 2006 and U.S. Government Accountability Office, “The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information” (March 2006).

concerned itself primary with drug interdiction (as well as maritime safety, etc.). Coast Guard capabilities remained relatively modest throughout the 1990s.

Nonetheless, the United States military possesses a number of unique capabilities that make it an attractive candidate for homeland security missions. The military is highly responsive and deployable on short order, has an extraordinary ability to plan and execute complex operations, and possesses some specialized skills and equipment that would be costly to duplicate on a civilian level (either within a national agency or especially state by state or locality by locality). As a result, in the 1990s, the military (particularly the Guard and Reserve) began to take on certain missions related to homeland security, including important roles in major national events that posed potential security risks (e.g. the Atlanta Olympics) and specialized operations (responding to nuclear emergencies, along with the Department of Energy).

9/11 dramatically brought home the problems of failure to consider adequately the role of the military in homeland security and its integration with domestic agencies and activities. The 9/11 Commission painstakingly documented the ineffective efforts to interdict the hijacked aircraft once the terrorists' intention became clear – a multi-dimensional failure that included lack of integrated communications, poor or undefined procedures, and sheer lack of capacity to mount a timely operation.

Not surprisingly, therefore, the military moved rather quickly to compensate for these deficiencies, beginning with the deployment of 24-hour air caps around New York and Washington. By April 2002 the need to address direct attack on the homeland was consolidated into a new military command, Northern Command (NORTHCOM), which went into effect in October 2002 and took over command and control of the Pentagon's homeland defense efforts, which had earlier been coordinated among four different commands with North American Aerospace Command (NORAD), Joint Forces Command, Pacific Command and Southern Command having separate responsibilities for various elements of the effort. NORTHCOM was also given the responsibility to coordinate military support to civil authorities including in the course and the aftermath of a crisis. But these efforts developed in considerable isolation from the evolving mechanism for coordinating homeland security operations — in 2002 a Pentagon official

put it very bluntly stating that “We don't tell the Office of Homeland Security about recommendations, only about decisions.”²⁵ This was due in large measure to the insistence (by both military and civilian DoD leaders) that operations had to be handled through the traditional military chain of command, from the uniformed services to the President through the Secretary of Defense (the same argument that has led to excluding civilian national security agencies from participating in the planning and execution of war operations).

The continued problems of integrating the military and civilian roles in protecting the homeland could be seen in the Cessna incursion in restricted Washington, DC airspace in May 2005. This episode demonstrated that there remain two conflicting lines of authority – Customs and Border Protection through DHS, and the military through the Secretary of Defense – to interdict threats. DHS Secretary Chertoff reportedly has recommended resolving this problem in part by transferring Customs authority to the Coast Guard, which reports both through DHS and the Secretary of Defense.

The traditional justifications for insulating military operations are the unique “expertise” of the military in war fighting and the need for operational secrecy to assure mission success. However, these rationales have limited applicability in the context of “homeland” security. Unlike military operations abroad, it is impossible to identify a “theater of operations” over which the military could have exclusive control dealing with threats on the territory of the United States, as the Cessna episode so vividly demonstrated. Moreover, to the extent that secrecy is a factor in homeland security activities, it is equally applicable to the operational activities of all the agencies involved in counter-terrorism, such as the FBI, and does not therefore provide a justification for disparate treatment of the military.

To some extent, DoD recognizes the need to integrate at least some of its activity into the planning and operational activities of other homeland security agencies, while seeking to preserve its traditional approach to insulating military operations. It has tried to square this circle by differentiating between the functions of “homeland security,” which it considers a national team effort that it is a part of, and “homeland defense, the

²⁵ Peter F. Verga, special assistant to the secretary of defense for domestic security, in Elizabeth Becker, “Big Visions for Security Post Shrink Amid Political Drama,” *New York Times* 3 May 2002:1.

principal responsibility of NORTHCOM, with limited coordination with civilian agencies. This latter function along with its civil support mission – which consists of activities where DoD personnel would operate in support of civilian agencies through the provision of specialized capabilities (rapid transport, specialized equipment) in the case of “consequence management assistance, such as would occur after a terrorist event employing a weapon of mass destruction”²⁶ – is considered to fall within the ambit of “homeland security.”

Not surprisingly, the DoD has sought to limit its civil support mission for a variety of reasons, many of them quite compelling, others rooted more in culture than in sound policy.²⁷ At a time of great strain on military personnel and high, unforeseen need for deploying Guard and Reserve personnel abroad in connection with operations in Iraq and Afghanistan, the Pentagon has been reluctant to give the Guard and Reserve major roles in assuring homeland security. Absent a dramatic increase in the number of active duty personnel this rationale is sound. There is little point in building a homeland security strategy around personnel who might be unavailable when needed, and under current deployment demands, for many communities that danger is real. Moreover, while the Guard and Reserve provide a pool of disciplined, healthy individuals who are used to training for stressful operations, these qualities are not so unique as to militate strongly in favor of using the Guard and Reserve instead of, for example, trained police and fire auxiliary personnel.

Nonetheless, there remains room for considerable improvement and DoD could have other specific roles in homeland security as well. It possesses robust communications networks that DHS and other agencies may need to employ in the event of catastrophic attacks that leave normal communications infrastructure nonfunctional.²⁸ Its technology development efforts are also potentially quite useful to the homeland security mission in a broader sense. For example, unmanned aerial vehicles are already

²⁶ “Homeland Defense vs Homeland Security,” US Northcom, 2005, 24 May 2005, Available: <http://www.northcom.mil/index.cfm?fuseaction=s.homeland>; “Who We Are—Civil Support,” US Northcom, 2005, 24 May 2005, Available: http://www.northcom.mil/index.cfm?fuseaction=s.who_civil

²⁷ Last year it was reported that “DOD is considering whether some of its civil support functions “should be migrated into the civilian community”. See “DoD Mulls Shifting Homeland Defense Responsibilities to Others,” *Homeland Defense Watch* Vol. 3 No. 8 (19 Apr. 2004).

²⁸ Adrian A. Erckenbrack and Aaron Scholer, “The DoD Role in Homeland Security,” *Joint Forces Quarterly*, no. 35 (October 2004), p. 35.

used in border surveillance at times; aerostats could be as well. Unmanned aerial systems might also help with monitoring of key infrastructure. There could also be much improvement in the coordination of DoD and civilian homeland security activities. The integration of the HSC into the NSC should contribute to this result, as the Pentagon is more comfortable with coordination through the established NSC processes than through a more civilian policy council like the HSC.

Another serious problem is arising in the field of counter-terrorism intelligence collection and operations where there is a seam between the civilian agencies – both domestic (FBI) and foreign (CIA) – and the military, as the Pentagon begins to expand (in number, scope and geographic reach) its use of human intelligence sources. These difficulties occur in both the domestic and foreign context. Overseas, the Pentagon is contemplating a significant expansion of its intelligence gathering role, not only in connection with the “hot” battlefield (e.g. Iraq and Afghanistan) but also as part of the so-called “global war on terror” in virtually any part of the world where terrorists might operate. The Pentagon has increased its intelligence missions and personnel, raising concerns about overlap with other agencies’ functions and questions about whether some of these related initiatives are appropriate for military personnel.²⁹ Press accounts have detailed the creation of the Strategic Support Branch, which “deploys small teams of case officers, linguists, interrogators and technical specialists alongside newly empowered special operations forces.” The reports indicate that the unit, created to provide the Secretary of Defense with expanded independent human intelligence operational tools, had been operating in Iraq, Afghanistan, and “emerging target countries.”³⁰ Thus in the overseas context, the contemplated military role would not be limited to intelligence collection but would extend to intelligence operations as well. While this enhanced role has been endorsed by the 9/11 Commission, which stated that “[l]ead responsibility for directing and executing paramilitary operations, whether clandestine or covert, should shift to the Defense Department”³¹ and the Defense Science Board, which called for the establishment of “a more robust Defense human intelligence (HUMINT) capability than

²⁹ Pincus, “CIA, Pentagon Seek to Avoid Overlap.”

³⁰ Barton Gellman, “Secret Unit Expands Rumsfeld’s Domain,” *Washington Post*, January 23, 2005, p. A01.

³¹ National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York, NY: W.W. Norton & Co, 2004) 415.

exists today,”³² there is reason to be concerned about this approach including lack of coordination on sensitive operations with the State Department and the CIA; imperfect Congressional oversight of covert military operations; lack of expertise in the military for these operations; potential lack of legal protection for military personnel acting covertly; and the possible negative foreign policy implications of an exposed covert operation.³³

Our study has found that it is uncertain whether the DNI has the authority to resolve the respective roles of the CIA and the military for covert intelligence collection and operations.³⁴ The Office of the DNI and the Pentagon have been working toward resolving some of these issues. Recently, the CIA and the Pentagon also drafted an MoU to “deconflict” and coordinate their operations, which is awaiting approval.³⁵ While the Robb-Silberman Commission suggested the creation of a Human Intelligence Directorate more generally, on covert action specifically, their recommendations were classified, but reports indicate that their suggestion to shift planning of covert operations out of the CIA’s hands was rejected, with the administration stating clearly that the “CIA also will strengthen its management of covert action.”³⁶ With the creation of the NCS, the CIA has been given authority to coordinate all human intelligence operations overseas and develop common rules and standards. Along with one deputy to oversee the HUMINT work of the CIA and another to oversee that of the intelligence community as a whole, the NCS will also have a “covert action executive” who will coordinate covert

³² Defense Science Board, *Report of the Defense Science Board 2003 Summer Study on DoD Roles and Missions in Homeland Security, Volume 1*, November 2003, p. 20; the DSB also stated that the Secretary of Defense “should accelerate the ongoing transformation of the Defense HUMINT Service, with particular attention to ensuring that the nation has the global coverage and sustained foreign presence that is needed in regions ripe and important” in its *2004 Summer Study on Transition to and From Hostilities* released in December 2004.

³³ For a more detailed analysis of the problems associated with military covert operations outside the “hot” battlefield, see Jennifer D. Kibbe, “A Loophole for Covert Operations,” *Fort Worth Star-Telegram* 8 Aug. 2004 and our forthcoming book *Erasing the Seams: An Integrated, International Strategy to Combat Terrorism*.

³⁴ The act merely says, “The Director of National Intelligence, in consultation with the Secretary of Defense and the Director of the Central Intelligence Agency, shall develop joint procedures to be used by the Department of Defense and the Central Intelligence Agency to improve the coordination and deconfliction of operations that involve elements of both the Armed Forces and the Central Intelligence Agency consistent with national security and the protection of human intelligence sources and methods.”

³⁵ Pincus, “CIA, Pentagon Seek to Avoid Overlap.”

³⁶ See “President Bush Administration Actions to Implement WMD Commission Recommendations,” June 29, 2005 (www.whitehouse.gov/news/releases/2005/06/20050629-5.html [July 6, 2005]). On rejection of the recommendation, see Douglas Jiehl, “Bush to Create New Unit in F.B.I. for Intelligence,” *New York Times*, June 30, 2005, p. 1.

operations.³⁷ However, while the authority to coordinate (but not direct operations) has been assigned, it has not been clarified—for example, it is not quite clear who will resolve disputes between the agencies (and how) or whether that individual will have the ability and not just the authority to do so. It also is not clear which authority (Title 50 or Title 10) governs. The ambiguities need to be resolved and authorities need to be made clear. In cases of disagreement that cannot be resolved by the office of the NCS director, the DNI and the newly established Joint Intelligence Community Council should be given oversight responsibility. Even in cases in which the military is the most suitable instrument for conducting clandestine and covert operations, appropriate safeguards comparable to those in Title 50 should be applied.

4) Difficulties arising from problems in gaining international cooperation

It is widely accepted that the United States has a compelling need for international cooperation in fighting terrorism. President George Bush, for example, has emphasized that “the wars of the 21st century are going to require incredible international cooperation. . . . We need to cooperate.”³⁸ Much of the threat emanates from abroad, and with limited exceptions, the United States cannot operate unilaterally either to collect the necessary intelligence or undertake the operations necessary to thwart or eliminate that threat. Prior to 9/11, the principal linkages between U.S. intelligence agencies and their foreign counterparts were almost exclusively “bilateral” in two important senses.³⁹ First, the sharing was largely between the United States and individual countries (there is some exception in the case of collaboration on technical intelligence between the United States, the United Kingdom, Canada, and Australia and within NATO), and second, sharing was between homologous entities (SIGINT or signals intelligence agencies with other SIGINT agencies; human intelligence agencies with liaison services, law enforcement with law enforcement). These bilateral relations were largely a function of differing

³⁷ Bill Gertz, “Covert Action Operations to Remain in CIA's control: 9/11 Panel's Suggestion of Pentagon Role Rejected,” *Washington Times*, October 14, 2005, A13.

³⁸ George W. Bush, “Moment of Truth for World in Iraq,” press conference with President Bush, Prime Minister Tony Blair, President Jose Maria Aznar, and Prime Minister Jose Manuel Durao Barroso, Azores, Portugal, March 16, 2003.

³⁹ Occasionally in the 1990s, information was shared with multilateral organizations, but this was often ad hoc, for very specific assignments.

degrees of trust, a reflection of the prevailing Cold War emphasis on information security rather than sharing.

While these special relationships have intensified in many cases since 9/11, sharing structures remain fragmented and stovepiped. There is a limited degree of sharing of cross-community assessments (for example, from the United Kingdom's Joint Intelligence Committee), but the barriers to sharing raw intelligence across the full range of analysts remain high. Moreover, in the transatlantic context, there are serious problems in sharing with Europe as a result of the fragmented nature of the European system itself. While the European Union (EU) as an entity and the European Council and Commission have important responsibilities and authorities that affect counterterrorism across the EU (for example, ports, the "Schengen" border information system), intra-European information sharing (apart from bilateral sharing) is weak, and the new EU institutions developed to address the deficiencies revealed by the Madrid bombing (such as the office of the "coordinator for the fight against terrorism") are understaffed and undersupported by the member states. Some intra-EU collaboration is possible on the strategic level through the EU's Joint Situation Centre (SitCen), which could provide an avenue of cooperation and exchange with the United States.

As with sharing among U.S. agencies and actors, there is a need to reassess the balance of risks and benefits from enhanced sharing with partners abroad. It is self-evident that in the face of the current jihadist terrorist threat, intelligence collected by foreign agencies is indispensable, a fact that was underscored by the crucial role of liaison agency intelligence in foiling the plots to attack U.S. embassies abroad in 1998 and 2001 as well as potential attacks associated with the millennium celebrations. Yet without adequate methods of sharing, it will be impossible to "connect the dots" between information held by the United States and by others.⁴⁰ Improved sharing is also needed to build a greater sense of reciprocity, which is critical to effective long-term intelligence

⁴⁰ See Written Statement for the Record of the Director of Central Intelligence before the National Commission on Terrorist Attacks upon the United States," March 24, 2004 (www.9-11commission.gov/hearings/hearing8/tenet_statement.pdf [July 6, 2005]). See also Samuel L. Berger, testimony before the National Commission on Terrorist Attacks upon the United States," March 24, 2004 (www.9-11commission.gov/hearings/hearing8/berger_statement.pdf [July 6, 2005]).

relationships. While security remains a legitimate concern, many of the tools to protect the security of information in the U.S. context could be applied to international sharing.

There are a number of other aspects to this problem. One is the lack of clarity regarding which agency in the United States has responsibility for interaction with foreign partners. As mentioned above, in the case of intelligence the CIA, FBI, DoD, and even some state and local agencies have a presence abroad. Add to that the Department of Homeland Security, which has a full-time attaché to the European Union, and the State Department, in its traditional role as diplomatic liaison, and the arena seems crowded. Their activities lack coordination, and that lack is likely to cause confusion in the minds of international partners and continued stovepiping of information. While there have been indications that the CIA and DoD have been working to resolve this issue, it is not clear that the FBI and DHS are coordinating their activities with the other agencies. The Intelligence Reform Act does give the DNI some coordinating authority, which some consider ambiguous, but the statute is being interpreted broadly, which might serve to alleviate the problem.

Problems associated with the lack of coordination extend to policy development as well. A recent example was the dispute over the Transportation Security Act of November 2001, which stated that airlines had to provide U.S. authorities with detailed information on all passengers before arrival at a U.S. port of entry through the passenger name record (PNR), which includes information on the passenger's name, date of birth, method of payment, and meal preferences. This announcement was seen as a unilateral imposition of rules, and European airlines found themselves in a difficult situation. Compliance with the rules would require them to provide what the European Union considers sensitive information on their passengers within fifteen minutes of departure to the United States and would require them to defy EU privacy protection laws. There were concerns in the EU about the kind of information that was required, retention periods, and the resistance of U.S. authorities to limiting the use of data collected to the counterterrorism realm.

European airlines were stuck in the middle. Noncompliance with the U.S. law would likely result in fines, delays, and possible flight cancellations. In March 2003, the

EU and the United States reached an interim agreement that allowed the kind of access that the Act required while a more permanent agreement could be reached. In December 2003, they finally reached an agreement, formalized in May 2004, that is to be in effect for three and a half years, at which point it is to be renegotiated. Under the agreement airlines can legally transfer PNR data on the basis of the DHS's promise to implement protections for the use, sharing, security, correction, and oversight of data that are sufficient to guard passenger privacy.

The uproar and objections that met the U.S. demand for passenger information could have been avoided or at least reduced had there been an integrated strategy—one that included a diplomatic element before, not after, the fact—that had taken into account broader transatlantic interests in counterterrorism cooperation. Similar problems have arisen from U.S. requirements concerning armed sky marshals, though there are indications that the problems were not as bad because both sides have learned some lessons since the PNR case.

It is apparent that the United States needs to integrate its diplomatic strategy with its homeland security strategy—and not leave diplomacy to post facto efforts to gain support for domestic decisions reached without regard for the consequences to international cooperation. Coordination needs to take place both at the national level and in the field. This is a powerful argument for integrating the responsibilities of the HSC into the NSC3, as well as for enhancing the chief of mission's role in embassies with regard to the full spectrum of U.S. counterterrorism agencies.

5) Failure to consolidate terrorist watch lists across agencies operating domestically and internationally

The problem of the foreign/domestic divide has also been evident in the various watch lists maintained by different federal agencies. In the aftermath of the 9/11 attacks, there were numerous calls for the consolidation of these lists, spurred on by a key lapse that contributed to the attacks having taken place – the CIA's failure to notify immigration authorities and the FBI in time that it had placed two individuals on its terrorist watch list, who as a result were allowed into the U.S. and subsequently formed

part of the group that hijacked and crashed a plane into the Pentagon. In April 2003, a Government Accounting Office (GAO) report estimated that 9 agencies had a dozen different watch lists. Agencies had little, if any, access to each other's watch lists. There were few guidelines and standards on what criteria would determine how and why someone got placed on a list or how they could be removed from it.

Some progress has been made since then – the Terrorist Screening Center (TSC) that became operational in December 2003 has made efforts to consolidate information into a single master list but according to the GAO, the project has been characterized by inordinate delays and the TSC has still not completed the integration. Ten of the 12 databases have been consolidated according to the TSC but they have yet to include available biometric information into the database;⁴¹ many agencies still cannot access the list directly; there are doubts about the accuracy of the data that is in the system; and there are still no specific guidelines on what gets an individual placed on this list. The efforts have been hampered by technical and administrative difficulties and continued hesitation on the part of various agencies to share information. This leads to problems like the flap last year over two flights originating in Europe being diverted when Customs and Border Protection (CBP) detected passengers on the flight manifests who matched individuals on the various watch lists that names are run against, only to find that they were false hits. Since CBP officials take almost an hour to run the names on each flight against these lists and airlines are only required to provide the manifests 15 minutes before the flights take off, detections usually occur after the flight has already taken off.⁴² Though some of these problems might be alleviated by the NCTC, which feeds the TSC counter-terrorism information from various agencies whose work it coordinates, much still needs to be done in terms of integrating the watch lists, standardizing criteria, ensuring accuracy and specifying guidelines and procedures.

⁴¹ Secretary of Homeland Security Michael Chertoff recently pointed out the benefits of having this information: “Right now we are using the most primitive kind of screening in many respects, meaning we screen for bad names. And of course, names are not the best way of identifying people. They're certainly not as good as biometrics.”

⁴² Sara Kehaulani Goo, “No-Fly Gaps Irk Airlines, DHS” *Washington Post* 25 May 2005: A03.