Backgrounder

Published by The Heritage Foundation

No. 1699
October 27, 2003

Better Intelligence Sharing for Visa Issuance and Monitoring: An Imperative for Homeland Security

James Jay Carafano, Ph.D., and Ha Nguyen

Since the September 11, 2001, attacks on New York and Washington, D.C., providing intelligence support for the issuance and monitoring of visas to keep these documents out of the hands of terrorists has been a top priority for the Bush Administration and Congress. A number of legislative initiatives have set out the requirements for an effective, integrated, objective system, but it will be years before this system is in place.

In the meantime, Congress needs a more effective committee structure to oversee the complex information technology and human capital programs required to support the new system. In addition, the Administration needs to institute organizational changes and establish appropriate measures of effectiveness to ensure that the current system operates as efficiently as possible.

On Terrorism's Front Line

In the global war waged by terrorists, visas can be deadly weapons. One ready means available to enemies wishing to enter the United States is the nonimmigrant visa, which can be obtained from any of the 211 American consulates around the world. The length of stay varies depending on the type of visa. Travelers holding nonimmigrant visas represent the overwhelming majority of individuals entering the U.S. During fiscal year 2000, a record 33.7 million visitors, students,[1] and temporary work through U.S. borders.[2]

Nonimmigrant visas are ideal for supporting attacks that require brief or repeated trips to the

- Since the September 11 attacks, providing intelligence support for visa issuance and monitoring to keep these documents out of the hands of terrorists has been a top priority for the Bush Administration and Congress.
- During fiscal year 2000, a record 33.7 million visitors, students, and temporary workers passed through U.S. borders.
- Both houses of Congress should establish permanent committees to oversee homeland security.
- The intelligence community should focus on ensuring that intelligence databases are interoperable and shared between agencies.
- The Office of Visa Services should be transferred to the Department of Homeland Security

This paper, in its entirety, can be found at:
www.heritage.org/homelanddefense/bg1699.cfm

Produced by the Homeland Defense Project

Published by The Heritage Foundation
214 Massachusetts Ave., NE
Washington, DC 20002–4999
(202) 546-4400 heritage.org

United States. In fact, all of the September 11 hijackers entered the United States in this manner. The 19 terrorists received a total of 23 visas from five different consular posts over a four-year period.[3]

Entry can be more difficult for individuals on a terrorist watch list or from countries with suspected terrorist ties, but these safeguards have been far from perfect. For example, Sheik Omar Abdel Rahman, convicted of conspiracy in the 1993 bombing of the World Trade Center, was on the State Department watch list but managed to obtain a tourist visa under an assumed name.

Terrorists can also enter the United States through the permanent immigration system, obtaining a "green card" to live in the country or become a naturalized citizen. Each year, approximately 900,000 foreigners enter the U.S. in this manner because they have a relative in the United States, possess a specialized job skill, are seeking asylum as a refugee, or have won a visa lottery[4] that admits about 50,000 a year. One study of 28 known militant Islamic terrorists found that 17 of them were in the country legally, either as permanent residents or as naturalized citizens.[5]

The prevalent use of identity theft and false travel documents makes the current system particularly vulnerable to abuse. In 2001, officials at border crossing points seized over 100,000 falsified documents. Over 50 percent of these documents were border crossing cards, alien registration cards, and fraudulent visas and passports.[6]

Such materials have been used by terrorists. For example, one of the perpetrators of the 1993 World Trade Center bombing entered the country with a doctored passport.[7] Thus, intelligence is critical not only to keep suspected terrorists from legitimately obtaining and using passports, but also to prevent them from easily using falsified documents to travel into the United States.

Legislating Better Counterterrorism Tools

Before September 11, the ability of the United States to counter the threat of visa-carrying terrorists had long been hamstrung by weaknesses in the system for issuing visas and green cards, lapses in port of entry and border control screening, and lax enforcement of immigration laws. Three major reasons primarily account for these shortfalls: poor performance by and lack of resources for immigration services, inadequate collaboration among state and federal agencies, and insufficient cooperation by foreign governments.

After September 11, significant attention was paid to addressing these shortfalls. In particular, legislation directed major changes in the intelligence support system for visa issuance and monitoring. Three legislative initiatives sought to strengthen the visa system.

First, the USA PATRIOT Act requires the Federal Bureau of Investigation to share information in its National Crime Information Center with immigration services and the U.S. Department of State.[8] This gives consular officers who issue visas and federal

1. In addition, 28 countries are part of the U.S. Visa Waiver Program, allowing their citizens to enter the U.S. for 90 days without a visa. For a list of countries and program details, see U.S. Department of State, Bureau of Consular Affairs, "Visa Waiver Program (VWP),"at *travel.state.gov/vwp.html* (October 16, 2003).
2. Immigration and Naturalization Service, "Temporary Admissions Fiscal Year 2000," p. 4, at *www.immigration.gov/graphics/shared/aboutus/statistics/00yrbk_TEMP/Temp2000.pdf*.
3. U.S. General Accounting Office, *Border Security: Visa Process Should be Strengthened as an Antiterrorism Tool*, GAO–03–132NI, October 2002, p. 6.
4. Hesham Mohamed Hadayet, who shot and killed two people and wounded three at a Los Angeles airport ticket counter on July 4, 2002, initially came to the United States on a six-month tourist visa. His application for permanent residence status was denied, but he was allowed to remain in the country because his wife was granted permanent residency status through the U.S. State Department's Diversity Lottery Program.
5. Steven A. Camarote, *The Open Door: How Militant Terrorists Entered and Remained in the United States, 1993–2001* (Washington, D.C.: Center for Immigration Studies, 2001), p. 19.
6. U.S. General Accounting Office, *Identity Theft: Prevalence and Links to Alien Illegal Activity*, GAO–02–830T, June 25, 2002, p. 7.
7. U.S. Department of Justice, *The Potential for Fraud and INS's Efforts to Reduce the Risks of the Visa Waiver Program*, Inspection Report I–99–10, March 1999.

agents at border inspection points the means to check the criminal history of a visa applicant or bearer. It also instructs the Attorney General and the Secretary of State to develop a biometric[9] standard for verifying the identity of visa applicants and bearers of visas and passports, as well as querying law enforcement databases.[10]

Second, the Homeland Security Act of 2002 abolished the Immigration and Naturalization Service and transferred its functions to the Department of Homeland Security (DHS). Responsibility for providing immigration-related services and benefits was assigned to the DHS's Bureau of Citizenship and Immigration Services (BCIS). The DHS's Bureau of Customs and Border Protection assumed the border security functions of the Immigration and Naturalization Service, along with monitoring all U.S. borders and points of entry, and incorporated the Customs Service (previously part of the Department of Treasury).

While the State Department's consular offices retained responsibility for issuing visas, the DHS is charged with promulgating regulations governing visa issuance and training consular officers. As a result of the reorganization, the DHS has become the primary customer for intelligence in support of visa issuance and monitoring, having responsibility for monitoring the border and oversight of Department of State visa programs.

Third, a number of provisions in the Enhanced Border Security and Visa Entry Reform Act affect intelligence sharing and visa issuance and monitoring. Key measures include:

- Requiring law enforcement and intelligence agencies to make a maximum effort to share information relevant to admissibility and deportability of aliens with State and the BCIS.
- Directing the BCIS to integrate all of its data systems into Chimera, an interoperable, interagency system. This provision assigns the DHS primary responsibility for developing an overarching information architecture to share immigration and intelligence data. The law also calls for creating an eight-member commission to oversee the system.
- Requiring the implementation of an integrated entry and exit database[11] containing arrival and departure information from machine-readable visas, passports, and other travel and entry documents. The use of machine-readable documents will greatly facilitate the ability to query intelligence databases.[12]

8. The National Criminal Investigation Center (NCIC) is a computerized index of criminal justice information that is maintained by the FBI and available to federal, state, and local law enforcement and other criminal justice agencies. The database includes the agency's Interstate Identification Index (criminal history information); Wanted Persons File; Missing Persons File; Unidentified Persons File (to cross-reference unidentified bodies against records in the Missing Persons File); Foreign Fugitive File; and Violent Gang/Terrorist File (used to identify criminal gangs and their members to local, state, and federal law enforcement). The database also includes the U.S. Secret Service (now part of the Department of Homeland Security) Protective File, which maintains names and other information on individuals who are believed to pose a threat to the President. The law directs the agency to share information in the Interstate Identification Index and the Wanted Persons File as well as other files as agreed to by the Attorney General and the agency.
9. Biometrics are methods of identifying a person based on a physiological or behavioral characteristics, including the person's face, fingerprints, hand geometry, handwriting, iris, retina, vein, and voice.
10. The Enhanced Border Security and Visa Reform Act of 2002 reduces from two years (as enacted in the USA PATRIOT Act) to 15 months the period after which the President must certify biometric standards for identifying aliens seeking admission into the U.S. and from 18 months to one year the period after which the President must first report to the Congress on the progress in implementing the use of biometrics.
11. The entry-exit database will be the United States Visitor and Immigration Status Indicator Technology program (U.S.–Visit) established by the Homeland Security Act of 2002. It will be an automated entry-exit system that relies on numerous information sources, including biometrics, to identify and determine whether an individual should be admitted to the country. Through numerous processes such as scanning of machine-readable passports, individual interviews, and the fingerprinting of non-immigrant travelers, U.S.–Visit is intended to track a person's immigration and visa status and alert authorities to expired visas. The collected information can then be checked against federal databases and watch lists.

- Directing the Secretary of State to establish a terrorist lookout committee at each mission tocoordinate efforts in identifying suspected terrorists. The Department of State must train consular officers in visa screening, coordinate with law enforcement and intelligence agencies, obtain unclassified law enforcement and intelligence information on suspected terrorists, and disseminate this information to consular officers.
- Requiring consular and immigration officials to report the loss or theft of a U.S. or foreign passport within 72 hours of notification, using an electronic data reporting system.[13]

Together, these measures establish a comprehensive framework for employing intelligence and law enforcement information against terrorists using U.S. visas, green cards, and passports or passports from visa-waiver countries.[14]

The system, however, is not currently in place. Implementation will require information technology and human capital programs that are still on the drawing boards, and it is unclear whether the Administration is making sufficient progress in all areas. For example, according to an August 2003 report on the implementation of the Enhanced Border Security and Visa Entry Reform Act, 12 out of 21 deadlines established in the legislation have been missed.[15]

It is also unclear whether congressional oversight is adequate to ensure that the complex array of initiatives and programs reach fruition. Congress's track record for ensuring adequate funding and establishing improvements in this area is less than stellar. Several of the requirements established by post–September 11 legislation are not even new initiatives. For example, Congress called for the establishment of an entry-exit system in 1996.[16]

Part of the problem is that no single congressional committee in either chamber has primary responsibility for overseeing intelligence and information sharing in support of visa issuance and monitoring. Each of the key acts affects a wide cross section of government agencies, and congressional oversight is fragmented. For example, oversight of the USA PATRIOT Act falls under the Intelligence and Judiciary Committees of the House and Senate, while the Homeland Security Act falls largely under the House Select Committee on Homeland Security, which currently has no counterpart in the Senate.

While both chambers debate how best to organize their committee structures to oversee homeland security over the long term, intelligence sharing for visa issuance and monitoring is a pressing issue that should not wait for more protracted discussion on congressional reform.[17] The threat of terrorists carrying visas is imminent and needs to be—and can be—addressed right now.

Both houses should establish permanent homeland security committees with exclusive oversight of the Homeland Security Act and the visa issuance and monitoring provisions in the PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act, particularly in the area of intelligence sharing. These committees should place special emphasis on information technology and human capital needs, which are critical to the success of the system. They should also oversee all appropriations for visa issuance and monitoring programs.

12. The act also requires countries participating in the Visa Waiver program to employ machine-readable passports that are tamper-proof and employ biometric identifiers.
13. The act also requires countries in the Visa Waiver program to report the theft of blank passports issued by the country in a timely manner.
14. See footnote 1.
15. NumbersUSA, "Implementation Deadlines in the Enhanced Border Security and Visa Entry Reform Act (H.R. 3525)," updated August 9, 2003, at *www.numberusa.com/hottopic/deadlines.htm* (September 8, 2003).
16. Rosemary Jenks, "The Enhanced Border Security and Visa Entry Reform Act of 2002, A Summary of HR 3525," Center for Immigration Studies *Backgrounder*, June 2002, p. 3.
17. For one comprehensive recommendation, see Michael Scardaville, "The New Congress Must Reform Its Committee Structure to Meet Homeland Security Needs," Heritage Foundation Backgrounder No. 1612, November 12, 2002, at *www.heritage.org/Research/HomelandDefense/bg1612.cfm*.

The Current System

While Congress must organize itself better to partner with the executive branch in addressing the long-term threat of terrorists with visas, the Administration must continue to improve the intelligence sharing process. This is no easy task. The current process is a hodge-podge of legacy information systems and post–September 11 policy changes and organizational tinkering.

As the system operates today, providing intelligence support for visa issuance begins with TIPOFF. Established in 1987, TIPOFF is run through the Department of State's Bureau of Intelligence and Research as a clearinghouse for sensitive intelligence information provided by other agencies. It includes full biographic records on approximately 85,000 terrorist names, photos, fingerprints, and other source documentation.[18]

TIPOFF receives highly classified intelligence data, sensitive law enforcement information, and diplomatic reports from the U.S. intelligence community through a variety of classified and unclassified communications networks.[19] In addition, the State Department maintains Visas Viper, a dedicated telegraphic channel for reporting information on known and suspected terrorists directly to the TIPOFF staff.[20]

In turn, declassified information on suspected terrorists (e.g., name, date, and place of birth, nationality, and passport number)[21] is made available as a terrorist watch list.[22] In addition to name records, including over 12 million related to terrorist and criminal activity[23] provided by the intelligence community and the Drug Enforcement Agency, TIPOFF data are entered into the Consular Lookout and Support System (CLASS),[24] which consular officers use to run checks before issuing a visa.[25]

While the DHS is responsible for overall supervision of the immigration system, the CLASS database and day-to-day consular affairs are managed by the Department of State. Even though the DHS has specific oversight and training responsibilities, bifurcating authority for consular operations between two departments creates the potential for gaps in visa operations and effective intelligence sharing.

18. Ambassador Francis X. Taylor, "Testimony to the Joint Congressional Intelligence Committee Inquiry," Select Committee on Intelligence, U.S. Senate, and Permanent Select Committee on Intelligence, U.S. House of Representatives, October 1, 2002, at *www.state.gov/s/ct/rls/rm/13891.htm*.
19. The members of the U.S. intelligence community are the Department of State, Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, National Reconnaissance Office, National Imagery and Mapping Agency, Army Intelligence, Air Force Intelligence, Navy Intelligence, Marine Corps Intelligence, Coast Guard Intelligence, Department of the Treasury, Department of Energy, Federal Bureau of Investigation, and Department of Homeland Security.
20. Ambassador Francis X. Taylor, "Testimony to the Joint Congressional Intelligence Committee Inquiry."
21. For a list of the data in the TIPOFF, see U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO–03–322, April 15, 2003, p. 16.
22. Watch lists, also referred to as lookout, target, or tip-off lists, contain information on known or suspected domestic and international terrorists and criminals. They are used by federal, state, and local agencies to identify, monitor, and apprehend suspects. U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated*, p. 40.
23. U.S. General Accounting Office, *Border Security: Visa Process Should be Strengthened as an Antiterrorism Tool*, GAO–03–132NI, October 2002, p. 26.
24. *Ibid.*, p. 11. In addition to CLASS, the State Department has special clearance procedures and interagency name check requirements for visa applicants from certain countries. *Ibid.*, p. 12.
25. Consular offices also have access to the Consolidated Consular Database, which includes records of five-year visa applications (approvals and denials). TIPOFF also periodically exports declassified biographic data to the Foreign Terrorist Tracking Task Force. On October 29, 2001, the President directed the Attorney General, with assistance from the Secretary of State, the Director of Central Intelligence, and others, to create this task force to ensure that the federal agencies coordinate programs to (1) deny entry into the United States of aliens associated with, or suspected of being engaged in or supporting, terrorist activity and (2) locate, detain, prosecute, or deport those already present in the United States. See Office of the President, Homeland Security Presidential Directive–2, October 29, 2001, at *www.fas.org/irp/offdocs/nspd/hspd-2.htm*.

Transferring the Office of Visa Services to the DHS. While the Homeland Security Act of 2002 gave the Secretary of the DHS exclusive authority to issue regulations and administer the visa program, consular officers remained part of the Department of State.[26] This was a mistake. For the DHS to fulfill its responsibilities in the visa process, and because of the national security aspect of visa approvals, the Bureau of Consular Affairs' Office of Visa Services should be placed under the DHS. Moving the Visa Office to the DHS would enable the DHS to focus on tightening, improving, and more broadly utilizing the visa function to meet the exigencies of homeland security.[27]

Under the current system, after approving or denying a visa request, consular officers notify the DHS via a separate information system. Information entered into the CLASS system is also entered into the Interagency Border Inspection System (IBIS),[28] along with data from 20 other federal agencies. IBIS is maintained by the Bureau of Customs and Border Protection in the DHS's Border and Transportation Security Directorate. It is used to identify aliens who are suspected of criminal or terrorist activity, have outstanding arrest warrants, or have been previously deported. In addition to watch list information, IBIS includes other data such as information on lost U.S. passports, lost or stolen visas, and missing blank foreign passports.

As a backup, visa data, including watch list information and revocations, are also faxed and cabled from the Department of State to the Bureau of Customs and Border Protection. These data are entered into the National Automated Immigration Lookout System II (NAILS), a legacy mainframe computer system that can also be used to send out watch list information. TIPOFF data are shared with NAILS through updates on diskettes and then transferred to IBIS.[29]

CLASS and IBIS provide only extracts from actual classified databases. Consular officers and border officials must submit the visa applicant's or holder's fingerprints to the FBI's National Crime Information Center to get an individual's full criminal history.[30] In addition, if an applicant is flagged by CLASS or during an interview with an applicant, the consular office prepares a Visas Condor cable, which is sent to the FBI and CIA for name checks.[31]

The system described above operates on information systems that have been around for a decade or more. Some of these systems cannot talk to each other.[32] The reliability of current technologies is also an issue. For example, a computer worm recently infected the CLASS system, requiring shutdown of the entire computer network.[33] Training and personnel management are also problems. The U.S. General Accounting Office has concluded that the DHS lacks a human capital strategy for implementing an entry-exit system.[34]

26. Homeland Security Act of 2002, Section 428(b)(1).

27. John J. Tkacik, Jr., "Why the Department of Homeland Security Should Control Visas," Heritage Foundation *Backgrounder* No. 1569, July 12, 2002, at *www.heritage.org/Research/NationalSecurity/BG1569.cfm*.

28. The backbone of IBIS is the Treasury Enforcement Communications System (TECS), a legacy system developed by the U.S. Treasury Department. This is a computer system developed to identify individuals and businesses suspect of violating federal law.

29. See Jayson P. Ahern, Assistant Commissioner, Bureau of Customs and Border Protection, statement before the Subcommittee on National Security, Emerging Threats and International Relations, Committee on Government Reform, U.S. House of Representatives, June 18, 2003, p. 5, and U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated*, p. 26.

30. The FBI can also conduct fingerprint-records searches using its own Automated Biometric Fingerprint Identification System (IDENT), which it maintains to identify and track aliens who were repeatedly apprehended trying to enter the United States illegally and those aliens who are suspected of criminal activity, have outstanding arrest warrants, or were previously deported.

31. For example, all male applicants over 16 from countries that are designated as state sponsors of terrorism require interviews, must complete a supplemental visa application, and must be reported via a Visas Condor cable. U.S. General Accounting Office, *Border Security: Visa Process Should be Strengthened as an Antiterrorism Tool*, pp. 21–22. Cables are also sent to the Department of Defense and National Security Agency for information.

32. U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated*, p. 19.

Measuring Effectiveness. To ensure that current capabilities continue to improve, the intelligence community and congressional oversight committees should establish measures of effectiveness in order to identify problems requiring immediate attention and evaluate progress in fixing them. Since integrating systems is intended to facilitate the flow, use, accuracy, and timeliness of intelligence, measures of effectiveness should focus on determining how quickly, accurately, and reliably information is moving through the processes that support visa issuance and monitoring, how well-trained consular and border officials are in using the data available, and whether the information is correct.

One measure of effectiveness should be the time elapsed between the report of a lost or stolen passport or revoked visa and notification of local, state, and federal officials. The measure should also be used to identify breakdowns in the information sharing process. These data should be collected jointly by the State Department and DHS and made available to Congress along with analysis that both identifies obstacles to greater efficiencies and makes recommendations on how they can be overcome.

Another measure of effectiveness should gauge the reform of consular affairs operations. The DHS, as part of its responsibility for visa issuance, should establish criteria for evaluating the effectiveness of screening visa applicants and applications as a counterterrorism tool. It should assess consular staffing levels and the staff's skill level, language proficiency, and training in interviewing and screening techniques in light of the technological tools available and current screening policies.

A third measure of effectiveness should be the number of "false-positives," or instances in which the system incorrectly flags an individual as a suspected terrorist or criminal. In addition, the quickness and efficiency of correcting errors—allowing individuals wrongly placed on watch lists and denied visas to rectify the situation—should be monitored. Both the State Department and DHS should collect this information and work with a civilian advisory group of concerned stakeholders to help create a system that catches terrorists but does not, at the same time, impinge upon the rights of individuals and legitimate travel and commerce.

In addition, the proposed select congressional committees should require reporting of the number of false-positives and the reasons behind them, and should regularly assess improvement in the use of intelligence in support of visa issuance and monitoring.

Recent Innovations in Intelligence Sharing

In the past year, the Administration has undertaken two major initiatives for improving the current system. The first is the establishment of the Terrorism Threat Integration Center (TTIC) on May 1, 2003.

The TTIC is designed to be a central location where all terrorist-related intelligence, both foreign and domestic, is gathered, coordinated, and assessed. It is composed of elements of the FBI, CIA, Department of Defense, Department of Homeland Security, Department of State, and other intelligence agencies. According to the Administration, the TTIC will:

- Optimize the use of terrorist threat-related information, expertise, and capabilities to conduct threat analysis and inform collection strategies;
- Create a structure that ensures information sharing across agency lines;
- Integrate terrorist-related information collected domestically and abroad in order to form the most comprehensive threat picture possible; and
- Provide terrorist threat assessments for the national leadership.[35]

The TTIC has recently developed a secure Web site to provide access to top-secret information to government officials from all agencies involved in

33. CBSNEWS.com, "Virus Shuts Down U.S. Visa System," September 26, 2003, at *www.cbsnews.com/stories/2003/09/24/tech/main574860.shtml*.

34. U.S. General Accounting Office, *Risks Facing Key Border and Transportation Security Program Need to Be Addressed*, GAO–03–1083, September 2003, p. 7.

the war against terrorism. It will soon have a Web site with secret and law-enforcement–sensitive information that will give access to a much broader community of analysts. Eventually, TTIC Online will have "sensitive but unclassified" information that will allow more information sharing with state and local officials and the private sector.[36] Currently, the Director of the TTIC reports directly to the Director of Central Intelligence (DCI).

The second initiative is creation of the Terrorist Screening Center (TSC) under the FBI to consolidate all terrorist watch lists into a single function and give around-the-clock access to local, state, and federal authorities. The TSC will bring together databases that include the State Department's TIPOFF, the FBI's Violent Gang and Terrorist Offender's File, and the DHS's many transportation security lists. Once established, the TSC will make it easier for consular officers to determine whether a visa applicant is a potential terrorist. The main source of the TSC's information will be the TTIC. An interagency group has been established to draft standards for placing an individual on the watch list, and the TSC is expected to be functional by December 1, 2003.

As part of these new initiatives, TIPOFF's database portion will move under the TTIC while the support functions for consular offices will move to the TSC. The TTIC will forward all terrorist-related information from the intelligence community to the TSC. Department of State officials from the Consular Affairs support part of TIPOFF will be assigned to the TSC to provide the full level of support to the Bureau of Consular Affairs.[37]

Placing the TTIC and TSC in different locations, especially under the DCI and FBI, has raised numerous concerns about whether it would indeed optimize intelligence sharing. It is deeply troubling that the DHS, as *the primary consumer* of intelligence for visa enforcement, does not have primary control over the mechanisms for fusing and disbursing information.

The DHS was created to be the main center for data sharing and analysis for homeland security, but it has not been given the tools to exploit U.S. intelligence and law enforcement resources. In the end, the current arrangement leaves the DHS as little more than just another intelligence end user, competing with other members of the national security community to ensure that its priority requirements are met.

Both the FBI and CIA directors have pledged to provide any support that the new agency requires.[38] But such assurances, although well-intended, fail to address how agencies with competing demands and priorities will allocate scarce resources, particularly during periods of national crisis when the United States is engaged in active operations overseas and faces a significant terrorist threat at home.[39] Placing the TTIC and the TSC outside the DHS only exacerbates this problem.

As serious as this problem is, however, it is also susceptible of solution. Specifically:

1. **Both the Terrorist Threat Integration Center and the Terrorist Screening Center should be placed under one interagency center and report directly to the Secretary of the Department of Homeland Security.**

Placing the TSC under the FBI and having the TTIC report to the DCI overlooks the fact that the

35. U.S. Department of State, International Information Programs, "Fact Sheet: Bush to Create Terrorist Threat Integration Center," January 28, 2003, at *usinfo.state.gov/topical/pol/terror/03012806.htm*.

36. John Brennan, Director, Terrorist Threat Integration Center, "Information Sharing and Coordination for Visa Issuance: Our First Line of Defense for Homeland Security," testimony before the Committee on the Judiciary, U.S. Senate, September 23, 2003.

37. *Ibid*.

38. George J. Tenet, testimony before the Committee on Governmental Affairs, U.S. Senate, June 27, 2002, and Robert S. Mueller III, testimony before the Committee on Governmental Affairs, U.S. Senate, June 27, 2002.

39. The lack of robust intelligence mechanisms for the Department of Homeland Security was evident in the enabling legislation. See James Jay Carafano, "Prospects for the Homeland Security Department: The 1947 Analogy," Center for Strategic and Budgetary Assessments *Backgrounder*, September 12, 2002, at *www.csbaonline.org/4Publications/Archive/B.20020912.Prospects_for_the_/B.20020912.Prospects_for_the_.htm*.

main functions of both agencies are to *coordinate, analyze, and disseminate* intelligence data—unlike the FBI and CIA, whose principal functions are to conduct law enforcement and gather intelligence, respectively.

TTIC and TSC functions more rightly fall under the intelligence role assigned to the DHS. Giving the DCI (and effectively the CIA)[40] and the FBI control over these two centers may complicate information sharing and reinforce barriers between intelligence producers and consumers. Moreover, since most of the information available at the TSC will come from the TTIC, both should be placed under the same interagency organization with oversight by a single federal authority to assure close cooperation and uninhibited flow of information between the two centers.

The structure for intelligence sharing between agencies should be based on a consumer- driven model. The DHS was designed as the biggest consumer of intelligence information and has the most at stake in terms of intelligence sharing and dissemination, particularly in the areas of visa issuance and monitoring. Thus, the TTIC and the TSC should be placed under the DHS both to ensure the best possible establishment and operation of these centers and to make certain that the DHS has the tools and ability to fulfill its responsibilities.

Emphasizing the DHS as the main intelligence coordination and analysis agency will also preempt the need for an independent domestic intelligence agency. In the aftermath of the September 11 attacks, many policymakers proposed creating a domestic agency to collect information and investigate people within the United States.[41] However, this policy recommendation would not have resolved any of the intelligence sharing loopholes; it would simply have created yet another layer of bureaucracy in the intelligence process.

Furthermore, such an agency could pose a serious threat civil liberties because it might be used to spy on American citizens, unconstrained by the legal constraints and judicial oversight that constrain domestic law enforcement agencies. Placing the TTIC and the TSC under the DHS not only addresses the need for better intelligence sharing, but also facilitates better protection of civil liberties.

2. **The intelligence community should focus on ensuring that intelligence databases are interoperable and shared between agencies rather than on merging watch lists.**

The intelligence failures prior to September 11 were caused by a lack of communication and intelligence sharing among agencies. Many have called for the creation of a consolidated watch list as the solution to better intelligence sharing.[42] However, such an attempt would waste time and effort without addressing the root cause of the problem—that agencies need to share relevant counterterrorism information.

Thus, in reforming the way in which intelligence sharing is conducted, the focus should be on making the watch lists interoperable while not stripping them of their individual tasks. An efficient interagency intelligence sharing system will facilitate the flow of terrorist-related information while addressing the multi-functionality needs of each agency.

3. **Data-mining technology is a potentially powerful tool and should be explored.**

Data-mining technologies could be particularly useful for the TTIC and the TSC in developing terrorist watch lists.[43] In the 2004 Defense Appropriations bill, Congress cut all funding for research and

40. The position of DCI has virtually no staff and no budget or administrative authority over any federal agency.

41. Larry M. Wortzel, "Americans Do Not Need a New Domestic Spy Agency to Improve Intelligence and Homeland Security," Heritage Foundation Executive Memorandum No. 848, January 10, 2003, at *www.heritage.org/Research/HomelandDefense/EM848.cfm.*

42. See U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated.*

43. Data mining involves identifying patterns and anomalies from the observation of vast data sets. Both government and industry have spent millions developing these technologies. It has been used by both commercial and government agencies to combat fraud and money laundering. Usama Fayyad *et al.*, "From Data Mining to Knowledge Discovery in Databases," *Artificial Intelligence*, Fall 1996, p. 2. It has been widely proposed that data mining systems be applied to homeland security for a host of purposes. See, for example, Homeland Security Act of 2002, Section 201.

development of the Defense Advanced Research Projects Agency's Terrorism Information Awareness program, but concerns that data-mining technology will be abused are based on speculation. Existing oversight and implementation structures could be modified to control the use of such new technology.

If successfully developed and applied within the confines of the law, these technologies could offer numerous benefits to U.S. counter-terrorism efforts. Data-mining research and development should be encouraged, and Congress should support and closely monitor the study of this potential technological breakthrough.[44]

Conclusion

Better intelligence sharing for the visa issuance process is a crucial aspect of the war on terrorism. Through legislation like the USA PATRIOT Act and the Administration's organizational initiatives such as the TTIC and the TSC, the Administration and Congress have laid out a road map for achieving better intelligence sharing.

To ensure that these efforts are put into practice:

- Both houses of Congress should establish permanent homeland security committees. These committees should have exclusive oversight of the Homeland Security Act, visa issuance and monitoring provisions in the USA PATRIOT Act, and the Enhanced Border Security and Visa Entry Reform Act, particularly in the area of intelligence sharing.
- The Office of Visa Services in the Bureau of Consular Affairs should be moved from the Department of State to the Department of Homeland Security.
- Federal agencies and congressional oversight committees should establish measures of effectiveness in order to identify problems requiring immediate action and evaluate progress in fixing them.
- The Terrorist Threat Integration Center and the Terrorist Screening Center should be placed under one interagency center and report directly to the Secretary of the DHS.
- The intelligence community should focus on ensuring that intelligence databases are interoperable and shared among agencies rather then on integrating watch lists.
- Data-mining technology, a potentially powerful tool, should be researched and developed.

—James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security, and Ha Nguyen is Research Assistant for Homeland Security, in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.[45]

44. See Paul Rosenzweig, "Proposals for Implementing the Terrorism Information Awareness System," Heritage Foundation *Legal Memorandum* No. 8, August 7, 2003, at *www.heritage.org/Research/HomelandDefense/lm8.cfm*, and Paul Rosenzweig, Michael Scardaville, and Ha Nguyen, "Senate Should Restore TIA Funding," Heritage Foundation *Web Memo* No. 315, July 17, 2003, at *www.heritage.org/Research/HomelandDefense/wm315.cfm*.

45. The authors would like to thank Dani Doane, John Tkacik, and Paul Rosenzweig for their contributions to this paper and to acknowledge Stephen Webber for his research.