

# TOP PRIORITIES FOR IMPROVING INTELLIGENCE AND LAW ENFORCEMENT CAPABILITIES

*A Report of the Working Group on Intelligence and Law Enforcement*<sup>1</sup>

Daniel W. Fisk, Working Group Rapporteur

Since the deadly terrorist attacks on America on September 11, questions have intensified about the ability of government agencies to gather and communicate actionable intelligence. Federal, State, and Local officials widely recognize that more resources must be focused on improving intelligence so that all levels of government, including emergency and first responders, can more effectively deter, stop, apprehend, and respond to those who would harm Americans.

- 
1. The Working Group on Intelligence and Law Enforcement includes Louis Dupart, Esq., Partner, Fleischman & Walsh, Washington, D.C.; Carmel Fisk, former Minority Counsel, Subcommittee on International Law, Immigration, and Refugees, Committee on the Judiciary, U.S. House of Representatives; Thomas Frazier, President, The Frazier Group, Baltimore, Md., former Chief of Police, Baltimore, Md.; Major General Bob Harding, USA (Ret.), Executive Vice President for Operations, Innovative Logistics Techniques, Inc., McLean, Va.; Alvin James, Anti-Money-Laundering Practice Leader, Ernest & Young; Dr. Mark M. Lowenthal, SRA International, Inc., Fairfax, Va.; N. John MacGaffin III, President, MacGaffin & Miller, Inc., Washington, D.C.; Ambassador David C. Miller, Jr., Chairman, MacGaffin & Miller, Inc., Washington, D.C.; Dr. William J. Olson, Minority Staff Director, International Narcotics Control Caucus, U.S. Senate; and The Honorable Robert S. Warshaw, Warshaw & Associates, Inc., Sylva, N.C., former Chief of Police, Rochester, N.Y. The following individuals also contributed to elements of this report in an advisory capacity: Christopher Barton, Chief Counsel, Permanent Select Committee on Intelligence, U.S. House of Representatives; the Honorable Edward J. Derwinski, former senior member of the House Committee on Foreign Affairs; Robert Filippone, Deputy Chief of Staff, Select Committee on Intelligence, U.S. Senate; John Mackey, Investigative Counsel, Committee on International Relations, U.S. House of Representatives; David A. Martin, Doherty Professor of Law, University of Virginia, and former General Counsel, Immigration and Naturalization Service; David Muhlhausen, Policy Analyst, Center for Data Analysis, The Heritage Foundation; and Robert Rector, Senior Research Fellow, The Heritage Foundation.

The capabilities of and relationships between law enforcement agencies (LEAs) and the Intelligence Community have received sustained attention over the past few years, including a comprehensive review in 1995 by the House Permanent Select Committee on Intelligence and its report, *Intelligence Community in the 21st Century*; the 1996 Brown–Rudman Commission; and more recent reviews by the Hart–Rudman, Bremer, and Gilmore Commissions.<sup>2</sup> Many of the excellent recommendations made by these commissions and studies have yet to be fully implemented, though after September 11, the Administration and Congress sought to address some of the bureaucratic problems exposed by the attacks in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (P.L. 107–56) and the FY 2002 Intelligence Authorization Act (P.L. 107–108).

Indeed, September 11 sent a powerful message to decision-makers that much more needs to be done to protect the homeland, and quickly. They now recognize that no single action, law, or institution—no one-step remedy—can possibly combat all of the threats facing the United States and its citizens. A multifaceted approach to homeland security is necessary. Building on the recommendations of earlier commissions and post-September 11 legislative efforts, the Working Group on Intelligence and Law Enforcement has identified the top priorities for improving the ability of both law enforcement agencies across America and the Intelligence Community to protect the American people from terrorist attacks.

- **Priority #1: Require the Office of Homeland Security to direct the assessment of threats to critical assets nationwide.** Since September 11, a number of State and Local governments, along with various Federal government agencies, have begun to develop their own vulnerability assessments. This is an important step in helping government officials determine what homeland assets critical to the nation’s economy and security are vulnerable and whether the responsible agencies and institutions are organized and equipped to protect them. A first step in this process should be the development of a uniform methodology for assessing the risk and the threat to vulnerable targets.
- **Priority #2: Rapidly improve information-gathering capabilities at all levels of government.** For Federal, State, and Local LEAs, a first line of defense against terrorism and other threats to the homeland is access to timely, reliable, and actionable information from both foreign and domestic sources. Rapidly enhancing government’s ability to acquire and analyze this information is vital to homeland security.

---

2. The status of recommendations made by previous commissions and studies that remain unimplemented may be found in the table at the end of this chapter. The status of post-September 11 legislative efforts may be found in the Appendix.

- **Priority #3: Improve intelligence and information sharing among all levels of government with homeland security responsibilities.** The need for better sharing and dissemination of information to all levels of government was starkly evident in the aftermath of September 11. Improved LEA–Intelligence Community cooperation has far more to do with changing bureaucratic cultures than revising statutes or regulations. Creating an all-source information fusion center and a cooperative structure for the sharing of information collected is critical to an effective homeland security policy.
- **Priority #4: Strengthen the visa approval and border security mechanisms.** The first line of defense against terrorists today often involves a determination by a consular officer or Immigration and Naturalization Service (INS) inspector that an alien should or should not be allowed to enter the United States. Legally entering the United States was remarkably easy for the September 11 terrorists. The visa approval and entry–exit processes must be strengthened, as should the ability of LEAs to enforce existing immigration laws against aliens who are in violation of those and other laws. Consular officers must have more information upon which to make a visa decision. At the same time, the Secretary of State should leverage the approval of a waiver as permitted by the Visa Waiver Program to enhance the anti-terrorism cooperation of other countries. Mechanisms to enforce immigration laws against aliens who violate the terms of their visas or who enter the country without inspection also should be strengthened.
- **Priority #5: Reduce the opportunities for identity theft and fraud in state identity document systems.** False documents continue to be a major problem, and the terrorists involved in the September 11 attacks showed that they will exploit those States with systems most liable to fraud. Any State that continues to run a document system subject to fraud and abuse places the lives of all Americans in jeopardy. Current procedures for the issuance of identity documents, including driver’s licenses, birth certificates, and death certificates, must be tightened and a mechanism developed to deter and prevent identity theft.
- **Priority #6: Create a mechanism to monitor recent anti–money-laundering initiatives to obstruct the financing of terrorism.** Many of the deficiencies in pre-September 11 efforts to obstruct the financing of terrorist activities were addressed in the PATRIOT Act. But the financial services area is dynamic, and those who seek to harm the United States will continue to attempt to circumvent the regulatory structures currently established. To anticipate how those who would threaten the United States could skirt the existing anti–money-laundering restrictions, the Secretary of the Treasury should create a mechanism to evaluate how current laws could be circumvented.

## **PRIORITY #1: REQUIRE THE OFFICE OF HOMELAND SECURITY TO DIRECT AN ASSESSMENT OF THREATS TO CRITICAL ASSETS NATIONWIDE.**

Since September 11, Federal, State, and Local governments have intensified efforts to identify vulnerable assets within their respective jurisdictions. These useful exercises will not necessarily be uniform in their methodology or compiled in one accessible database so that jurisdictions with overlapping responsibilities could coordinate their homeland security policies. Recognizing that not all potential targets can be protected at all times, a nationwide threat assessment of potential critical targets would provide a database to policymakers, first responders, and other agencies and officials with responsibility for homeland defense to facilitate protection and early warning by prioritizing what needs to be protected, under what circumstances, and by whom. This assessment should be matched with intelligence on the capabilities of those who would seek to harm the United States.

**Key Step #1. The Director of the Office of Homeland Security (OHS) should establish the methodology for conducting Federal, State, and Local threat assessments to ensure general uniformity of findings.** The Director of the OHS should establish the methodology that government entities will follow in assessing risks to people and infrastructure in their jurisdictions to ensure the compatibility of the information transmitted to OHS. To avoid compounding an already complicated coordination system, the basic format of these assessments should have the following elements:

**Identify the Critical Targets.** To be able to respond appropriately when a national alert about terrorism is announced, government officials with homeland security responsibilities, working with other relevant agencies and private entities, must first identify the critical targets within their jurisdictions that are or could be at risk, such as communication, utility, and transportation nodes and facilities; emergency-response facilities, bridges, and tunnels; and targets with significant political or symbolic value, such as national monuments and certain government buildings.

**Assess the Threat.** Next, relevant government entities should assess the threat to each critical target that has been identified. This assessment should include:

1. The type of threat or threats to each critical infrastructure (for example, explosives, cyberterrorism, biological or chemical attack, or a combination of these types). Since the nature of the threat is dynamic, the process of threat assessment must be continuous. In addition to actual targets, the assessment should include an inventory of facilities that could be used to develop chemical and biological agents and the sources of supply for such facilities, existing as well as potential.

2. The level of threat or the probability of attack on each target. Some facilities are likely targets at all times; others are at variable risk depending on the circumstances.
3. Potential threats from people or groups in a given area, including changes in demographics or patterns of behavior of groups that may threaten homeland security (such as an increase in activity by gangs with state or national reach). This assessment should identify which assets these individuals or groups are likely to target and whether agencies in the area have the ability to identify those groups.

**Track the Materials Sought by Terrorists.** Finally, a system should be developed to track the flow and supply of sensitive materials critical to the development and manufacture of chemical or biological agents and radioactive devices.<sup>3</sup>

**Key Step #2. The OHS Director should establish a national strategy to protect the homeland based on the national assessments.** A national strategy for homeland defense must include prevention (requiring both detection and deterrence); preparedness; crisis management; and consequence management. Before a national strategy can be finalized and resources allocated effectively, however, critical assets identified in the national assessments must be prioritized according to three fundamental characteristics: the potential for loss of life if attacked, the impact an attack would have on the economy, and the ability of the nation to function both domestically and internationally. Additional elements of the strategy should include how agencies should respond and who should be designated as points of contact should an emergency occur.

Recent legislation requires the President to designate a senior Department of Justice (DOJ) official as the coordinator for all Justice Department activities to combat domestic terrorism, including State and Local grant programs.<sup>4</sup> It is expected that this position will be the Deputy Attorney General for Combating Terrorism. This statutory requirement effectively makes the DOJ the most significant agency for Federal homeland security efforts within the United States and will necessitate that the OHS Director coordinate the development of the national strategy with the Department of Justice.

**Key Step #3. The Office of Homeland Security should develop a national alert and warning system.** The President should direct the OHS Director, working with Federal agencies and State and Local governments, to develop a warning system for threats to the homeland. Such a system should specify the methods of communica-

---

3. For a discussion of the development of an early warning system to detect chemical, biological, or other attacks, see Priority #1 in the chapter on Civil Defense.

4. As required by Section 612 of Public Law No. 107-77.

tion and provide a threat assessment based on a grading system similar to the Defense Readiness Conditions (DEFCON) system used by the U.S. Department of Defense (DOD). The DEFCON system ranks threats based on the severity of the situation at hand (DEFCON 1 to DEFCON 5). Military commanders are required to take certain actions with each DEFCON warning level.

A similar system for homeland defense would help avoid miscommunications about threats. Threat levels should be assigned by determining, at a minimum, the apparent imminence of the threat and the credibility of the source. Other factors should be considered as deemed necessary by the OHS Director.

Warnings should be disseminated geographically. Only States or regions in danger should be warned of an impending attack. There is no reason to have the entire country at a high state of alert if information narrows the geographic scope of where an attack could occur. Nationwide warnings should be issued only when intelligence is credible that an attack is imminent but the potential targets are numerous or non-specific. For example, the threat may be to a nuclear power plant, but the intelligence does not specify which one.

The program should be managed by the OHS through an interagency command-and-control center similar to the one created to handle the “Year 2000” (Y2K) threat to computers and computerized systems. The OHS Director should be responsible for determining the threat level and communicating it to lead agencies and governors. Governors should be responsible for sharing that information, not only with the Commander of the State’s National Guard and the emergency services department head, but also with Local officials, the public, and private industry, as appropriate. Lead agencies should be responsible for communicating the threat level to the private sector when conditions warrant.

## **PRIORITY #2: RAPIDLY IMPROVE INFORMATION-GATHERING CAPABILITIES AT ALL LEVELS OF GOVERNMENT.**

The Second Gilmore Commission report, issued in December 2000, noted that “‘foreign’ terrorism and ‘domestic’ terrorism may not be easily distinguished.” This conclusion was dramatically and tragically proved accurate on September 11. Acquiring reliable, timely, and actionable intelligence is the first line of defense against future acts of terrorism.

**Key Step #1. The President should direct the OHS Director to establish a national intelligence coordinating group to develop a national intelligence strategy, including the establishment of resource allocation and targeting priorities. The OHS Director should establish a Homeland Security Intelligence Coordinating**

Group (HSICG) at the Assistant Secretary level for this purpose. Disputes about policy or operations should be referred to a Deputy-level committee, a procedure currently used for the resolution of interagency disputes on other national security issues. The HSICG should be chaired by OHS and include representatives from the U.S. Departments of State, Defense, Justice, Treasury, and Transportation, and the Intelligence Community. The OHS Director should work with the Director of Central Intelligence (DCI) to ensure that a strategy exists to integrate homeland security intelligence into the work of the existing interagency mechanisms to determine targeting priorities.

In addition, to ensure adequate input from State and Local agencies, designees with security clearances from the following groups should be invited to participate on a regular basis: the International Association of Chiefs of Police, the National Sheriffs Association, and, as appropriate, other police executive organizations. On a case-by-case basis, designees with security clearance should also be invited to participate from the National Governors' Association, the U.S. Conference of Mayors, the National League of Cities, the National Association of Counties, and the International City Managers Association. The initial intelligence-sharing strategy should be finalized within 90 days of the first HSICG meeting.

**Key Step #2. The Administration should strengthen foreign intelligence–collection capabilities.** Recent legislation requires the DCI to lift the guidelines which hinder the recruitment of foreign agents (Section 403 of the Intelligence Authorization Act for Fiscal Year 2002). While this reform is an essential step to increasing foreign intelligence, other steps need to be taken:

**Recruitment of More Officers with Non-Official Cover.** To re-energize the Central Intelligence Agency's Non-Official Cover (NOC) program, the DCI should direct the recruitment of officials willing to operate under non-official cover, a group that offers the CIA a unique capability for gathering intelligence. This program has suffered from bias from full-time Directorate of Operations (DO) officers and from a lack of sustained funding. More officers who are willing to pursue this career path should be recruited, and the resources needed to sustain a vigorous NOC program should be provided.

**Recruitment of Officers for the Directorate of Operations.** The DCI should accelerate the recruitment of CIA DO officers who have diverse, multiethnic, multilingual backgrounds. The primary threat to the American people today is from more diverse peoples and groups from more regions than during the Cold War struggle against the Soviet Union.

**Development of Foreign Liaison Relationships.** The development of liaison relationships between U.S. and foreign LEAs should be enhanced through the International Law Enforcement Academy (ILEA) program. ILEAs now exist in

Thailand, for Southeast Asia, and Hungary for training for law enforcement officials from Eastern and Central Europe. An ILEA will open shortly in the United Arab Emirates (UAE) to train law enforcement officials from the Middle East.

**Key Step #3. The Administration should increase the sources of domestic information available to Federal agencies with homeland defense responsibilities.** Cabinet Secretaries with law enforcement responsibilities should hold LEA officials accountable for both the quality of their intelligence collection and their ability to collect evidence to develop a case for prosecution. The Attorney General should direct the Director of the Federal Bureau of Investigation (FBI) and the Administrator of the Drug Enforcement Administration (DEA) to measure and rate their Special Agents in Charge (SACs), and make promotion decisions, based on the SACs' ability to collect intelligence equal to making cases. The Secretary of the Treasury should do the same for law enforcement entities under his control, and the Secretary of Transportation should do the same for the U.S. Coast Guard.

**Key Step #4. State and Local LEAs should enhance information-collection efforts.** An effective homeland security structure must capitalize on the presence and potential of State and Local law enforcement agencies and personnel. The involvement of approximately 17,000 state and local police departments<sup>5</sup> is critical to a comprehensive homeland defense effort. "Community policing" offers a valuable potential for citizen involvement in homeland defense and for information gathering.

**Re-establish State and Local LEA intelligence units.** State and Local governments should re-establish LEA intelligence units, many of which were abolished in the 1970s following allegations of police harassment of certain groups. The U.S. Attorney General and State Attorneys General should establish frameworks for dealing with documented sustained abuses.

**Enhance Citizen Cooperation in Local Efforts.** Local police departments should include citizens' assessments of local threats and vulnerabilities through the Police–Citizen Interaction Committee (PCIC) mechanism—a formal platform for regular precinct-level meetings with citizens to discuss problems and solutions of interest to the community. Implementing community policing tactics, like PCICs, should not require federal funding.

**Regular Assessments of Local Threat Sources.** The Attorney General—through the FBI Director and the relevant SAC or U.S. Attorney—should request State and Local LEAs to submit annual assessments of the events, activities, or changes in demographics or patterns of behavior of groups in their jurisdiction (for example,

---

5. U.S. Department of Justice, Federal Bureau of Investigation, *Crime in the United States 2000: Uniform Crime Reports*, p. 1.

an increase in activity by gangs with state or national reach) that may threaten homeland security.

**Key Step #5. The DCI and Secretary of Defense should direct the strengthening of measurement and signature intelligence (MASINT) capabilities.** MASINT (and biometrics) by nature is a security discipline. It detects, identifies, and—most important—can be used to verify data from other intelligence sources. Its systems, for example, detect disturbances of earth (tunnels) and differences in gradient and ambient temperatures (spotting people and things, differentiating between “real” and “fake,” etc.). MASINT is perfectly designed to assist against any number of asymmetric threats; it is already in use for many important conventional aspects of the war against terrorism.

MASINT must be integrated into intelligence systems to alert or trigger intelligence-collection platforms or sensors (known as “cueing” and “cross-cueing”) for the targeting of other intelligence platforms and assets. Although this process has started at the Defense Intelligence Agency (DIA), it is in its infancy and is not getting the attention it deserves from DOD. The Defense Department is primarily treating MASINT and biometrics as an “information-automation-technology” discipline, having assigned as executive agent for MASINT the U.S. Army under the Director for Information, Systems, Command, Control, Communications, and Computers (DISC4).

**Key Step #6. The DCI and Secretary of Defense should maximize the capabilities of DOD’s Information Dominance Center (IDC) for the near term, and explore merging it into the CIA Counter Terrorism Center (CTC) in the long term.** The IDC (formerly called the Land Information Warfare Activity) at Fort Belvoir, Virginia, already performs the automated data-mining and cross-cueing of intelligence from the CIA, the National Security Agency (NSA), the Defense HUMINT Service (DHS), the National Imagery and Mapping Agency (NIMA), and the Counter-Intelligence Analysis Center. The Counter Terrorism Center (CTC), based in the CIA Directorate of Operations, focuses primarily on analyzing CIA DO–collected HUMINT. In the near term, retraining CTC analysts or reorienting the CTC mission to handle the work of the IDC is unnecessary. Under present circumstances, the IDC and the CTC should continue their operations and do what they do best. Over the longer term, the DCI and Secretary of Defense, working with the relevant congressional committees, should review the possible folding of the IDC into the CTC to form an all-source Intelligence Community intelligence center.

**PRIORITY #3: IMPROVE INTELLIGENCE AND INFORMATION-SHARING AMONG ALL LEVELS OF GOVERNMENT WITH HOMELAND SECURITY RESPONSIBILITIES.**

The Second Gilmore Commission report emphasized that “more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats.” The critical element of improved law enforcement–Intelligence Community cooperation has more to do with changing bureaucratic cultures than revising statutes or regulations.

**Key Step #1. The OHS Director, working with relevant Cabinet officials, should create a Federal-level fusion center for collecting intelligence and law enforcement information.** The President should direct the OHS Director, working with the Attorney General, the Secretary of the Treasury, the Secretary of Transportation, and the DCI, to create an all-source Federal-level information fusion center to which all information relevant to homeland defense is sent and from which information can be accessed by Federal agencies, and State and Local LEAs with homeland defense responsibilities, as required on a need-to-know basis.

**Key Step #2. The OHS Director should create a structure for sharing and disseminating information among Federal, State, and Local agencies.** The OHS Director, through the new Homeland Security Intelligence Coordinating Group, should develop a mechanism for sharing and disseminating information among government agencies.

**Cooperative Structure.** The OHS Director and HSICG should review the structure developed for Federal-State-Local cooperation in counternarcotics efforts. Both the High-Intensity Drug Trafficking Area (HIDTA) Program and the Justice Department’s Organized Crime Drug Enforcement Task Force (OCDETF) provide models for cross-government information sharing regarding terrorism-related threats to the homeland. The HSICG should explore the reconfiguration and expansion of the HIDTA Program into a “Drugs and Domestic Preparedness” structure, while remaining sensitive to the efficacy of this program in addressing the illegal drug problem and without deflecting the focus of the HIDTA program and the OCDETF mechanism away from combating the illegal drug trade.

As currently implemented, the HIDTA provides enhanced coordination and joint efforts among Federal, State and Local LEAs in order to reduce drug trafficking in critical regions of the United States. HIDTA provides a coordination umbrella for Federal, State, and Local law enforcement anti-drug efforts through an

outcome-focused, strategy-driven approach developed collectively by LEAs in the HIDTA region.

**Background Checks.** Each State and Territorial governor (56 jurisdictions) should designate the senior official responsible for homeland security within that specific jurisdiction to be cleared for security information on a need-to-know basis. This official should be cleared by the FBI Director and DCI for access, as required or needed, to national security information and as the principal point of contact between State and Local LEAs and Federal agencies. Under current law, both the CIA and FBI Directors have the authority to grant a security clearance for access to classified information based on national security needs. In some circumstances, the Director of the CIA or FBI, respectively, in coordination with the governor and mayor, may determine that a senior city official should also be granted a security clearance. Determinations of the need and extent of security clearances for State, Local, and Territorial officials should be reviewed on a routine basis.

**Federal Liaison.** The Director of OHS and the Attorney General each should appoint a senior official with both Federal and State or Local LEA experience as liaison and point of contact for State and Local officials and Federal agencies involved in homeland security. The Justice Department's Office of Domestic Policy (in the Office of Justice Programs) provides funding to State and Local agencies for training, equipment, and exercises. This office provides a basis for a liaison mechanism within the Department of Justice; however, there remains value in designating a senior Justice official who has direct communication with the Attorney General as a liaison for State and Local agencies. Further, the State and Local Advisory Group (SLAG) that had been established to advise the Attorney General should be resurrected to advise both the Attorney General and the OHS Director on how the Federal government can be more responsive to State and Local first-response agencies. The SLAG could be an important basis for creating grassroots support for homeland defense initiatives.

**Handling National Security Information.** To further facilitate the sharing of information, in selected instances, the Attorney General or Secretary of the Treasury, as required, should delegate authority to the SAC of the relevant Federal agency to deputize State and/or Local law enforcement officials as Special U.S. Marshals to handle classified information. The designation of these officers or units should be done in consultation, as required, with the appropriate governor, mayor, and state or metropolitan police chief. The FBI uses this arrangement in conducting investigations under its Violent Crime Task Force structure.

**Key Step #3. Federal officials should increase support for State and Local LEA information efforts.** An essential objective of any homeland defense strategy must include initiatives to bolster the preparedness of State and Local governments, especially

LEAs and other first responders, and to reassure the public that State and Local authorities can function separate and apart from the federal umbrella, even as they horizontally cooperate with their federal colleagues.

**Funding Support.** Congress, in recently enacted appropriations, has bolstered funding for the Justice Department's Office of Domestic Preparedness (ODP) to train State and Local agencies to prepare for terrorist actions and to equip specially designed State and Local units to cooperate with Federal agencies on homeland security operations. To help ensure that funding is not wasted, the ODP should (1) set minimum standards for preparedness for States and localities receiving federal assistance and (2) evaluate their performance. If States and localities do not meet the minimum standards, their federal assistance should be discontinued. Funding for equipment can be established as a matching grant program.

**Training Support.** The Attorney General should direct the FBI Director to implement a core course curriculum on terrorism at the FBI's National Academy at Quantico and the National Executive Institute for State and Local officials. The PATRIOT Act (Section 908) requires the Attorney General, in consultation with the DCI, to provide appropriate training to State and Local officials "who encounter, or may encounter in the course of a terrorist event, foreign intelligence in the performance of their duties." The Attorney General and Director of the FBI should provide instruction for these State and Local officials in the handling of classified and other national security material through the existing Regional Community Policing Institute structure in place in 30 localities.

#### **PRIORITY #4: STRENGTHEN THE VISA APPROVAL PROCESS AND BORDER SECURITY MECHANISMS.**

All of the 19 terrorists who organized and implemented the September 11 hijackings and attacks in New York and Washington entered the United States legally, having been approved for visas by U.S. consular officials and permitted entry by INS inspectors. However, some of these terrorists remained in the United States illegally after their visas had expired. The lack of timely, all-source intelligence for the vetting of visa applicants, the general ease of obtaining a visa, and the limited resources for dealing with those who violate the terms of their visa combined to give the terrorists an advantage in gaining access to the United States.

The Department of State (Bureau of Consular Affairs), the INS, and the U.S. Customs Service (USCS) play critical roles in determining who and what enters the United States. September 11 illustrated that the U.S. government has limited capacity to separate and distinguish legitimate travelers from those who may have the goal of attacking the American people. The steps that must be taken to

strengthen the visa approval system and entry–exit mechanisms and to ensure that overstays are reduced include the following.

### **STRENGTHENING THE VISA APPROVAL PROCESS AND ENTRY–EXIT VERIFICATION MECHANISMS**

**Key Step #1. The President, through the OHS Director, should mandate the creation of a comprehensive, Federal-level lookout database accessible to officials involved in border security.** Decisions made by consulates and the INS are only as good as the information available to their officers. One can expect those with beliefs inimical to the United States to hide their true beliefs, associations, and intended actions to help them gain entry to the country.

The recently approved USA PATRIOT Act does not ensure the sharing of data by all agencies with information that may be relevant to visa/entry decisions. Many Intelligence Community agencies with relevant information and the agencies under the authority of the Secretary of the Treasury (such as the U.S. Customs Service and the Internal Revenue Service) and under the Secretary of Transportation (such as the U.S. Coast Guard) are not required to share information with those responsible for making consular decisions.

The PATRIOT Act (Section 403) mandates that the Attorney General and FBI Director provide the State Department (Consular Affairs) “access to the criminal history record information contained in the National Crime Information Center’s Interstate Identification Index (NCIC–III), the Wanted Persons File, and to any other files maintained by the National Crime Information Center...” Before enactment of the PATRIOT Act, there was some sharing of information among the State Department, the INS, Customs, and the DEA, but the information exchange was not comprehensive. The creation of a comprehensive lookout database is essential to preventing potential terrorists from entering the United States.

**Key Step #2. Congress should repeal the requirement that INS inspectors clear passengers on international flights within 45 minutes of each flight’s arrival.** Before September 11, airlines had complained about long waits for inspections at international ports of entry at airports, such as New York’s JFK and those in Newark and Miami. Instead of finding a way to spread the arrival times of international flights, the airline and travel industry lobbied Congress to require that “adequate” inspections to clear international flights through the primary point of inspection be accomplished within 45 minutes of arrival. Congress should repeal this “45-minute” rule (Section 286[g] of the Immigration and Naturalization Act, or INA).

**Key Step #3. Congress should amend the Visa Waiver Program.** Congress should amend the Visa Waiver Program (8 U.S.C. 1187) to:

1. Make aliens from countries designated as “not fully cooperating with U.S. antiterrorism efforts” ineligible for the Visa Waiver Program, which permits citizens of qualifying countries to travel to the United States for tourism or business for 90 days without obtaining a U.S. visa;
2. Deny participation in the program to those countries that do not have adequate controls over their own official identity and travel documents, including passports; and
3. Require that all countries that want to remain in the Visa Waiver Program upgrade their passport systems to include a digitized, machine-readable fingerprint and a facial photo and provide an electronic database to the INS, so that the identity of the alien passport holder can be verified by an INS inspector at a port of entry.

**Key Step #4. The Secretary of State should accelerate the development and deployment of technology for biometric travel documents for aliens and U.S. citizens.** The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA, P.L. 104-208), the Immigration and Naturalization Service Data Management Improvement Act of 2000 (P.L. 106-15), and the PATRIOT Act of 2001 (P.L. 107-56) all contain provisions regarding the upgrading of technologies to produce and/or read biometric travel documents—visas for aliens and passports for U.S. citizens. The Secretary of State should direct the Assistant Secretary of State for Consular Affairs to expedite the development and issuance of a new tamper-proof and fraud-proof U.S. passport and visa system to deter and minimize the use of fraudulent or stolen U.S. documents by terrorists. The new documents should include a machine-readable fingerprint and a facial photo, in the case of U.S. passports, matched to a computer record of all valid U.S. passport holders. The Border Crossing Card (BCC) to facilitate travel between the United States and Mexico should be continued.

**Key Step #5. The Attorney General, working with the Secretary of the Treasury as appropriate, should strengthen the entry process and explore the development of an exit monitoring mechanism.** A system should be developed and given adequate resources to address the exit as well as the entry of aliens. Developing a comprehensive entry–exit system presents enormous challenges, but this does not render it impossible or not worth exploring. It does mean that the objective should be accomplished in structured, incremental steps.

Initially, the Attorney General should direct the INS Commissioner and the Chief of the Border Patrol to expand the INS Automated Biometric Identification

System (IDENT system) to all Border Patrol stations and inspection locations. The IDENT system currently is used to identify aliens who have been apprehended for violations of the immigration laws. Apprehended aliens' photographs and fingerprints (prints of the left and right index fingers) are entered into an electronic database. Using this information, a person who subsequently gives a different name may still be tracked in the system, including the number of times he or she has been apprehended and the outcome of each apprehension (removal, release, etc.).

Further, the OHS Director, the Attorney General, the Secretary of the Treasury, and the DCI should continue efforts to expand and increase the integration of the U.S. Customs Service, which is tasked with combating illegal entries of people and goods, into all aspects of border security to ensure coordination of all relevant Federal agencies. Currently, uniformed USCS inspectors and plainclothes investigators are present at all the points of entry to combat smuggling, among other illegal activities.

## **STRENGTHENING LEAS' ABILITY TO ENFORCE IMMIGRATION OR OTHER LAWS AGAINST ALIENS WHO VIOLATE THEM**

**Key Step #1. Congress should amend the Immigration and Naturalization Act (INA) and other laws to strengthen the monitoring of visa holders and the removal of visa violators.**

**Reporting on the Status of Non-Immigrant Visa Holders.** Congress should amend the INA to require those who sponsor a non-immigrant visa holder to report on the status of the sponsored alien, such as affirming under penalty of law that the alien is abiding by the terms of his visa. To enhance efforts to track aliens and prevent overstays, those who sponsor a non-immigrant visa should report on the alien's status annually, or as soon as there is a change in the alien's status. This would help INS develop a more effective and useful database of aliens still in the United States. INS investigative resources should also be increased to ensure that the agency is able to follow up on this information when it finds an alien in violation of the time limit on the visa.

**Limiting the Use of Voluntary Departure.** Congress should amend Section 240B of the INA to eliminate voluntary departure as an option during removal proceedings before an immigration judge. Voluntary departure allows an alien who is ineligible to remain in the United States (for example, because he entered illegally or overstayed a visa) to leave without having an order of deportation entered against him and put in his record. This "voluntary departure" option allows aliens to avoid the consequences of a deportation order, such as being barred for 10 years from receiving another visa. Under this amendment, INS would still be able to grant voluntary departure to aliens who are not placed in removal proceedings (required to

go before an immigration judge) or in removal proceedings where the INS counsel agrees to terminate proceedings in order to grant a voluntary departure.

Voluntary departures benefit aliens rather than expedite the process of removing them. Unless there are disincentives with teeth, aliens will continue to overstay and otherwise violate their visa conditions. Tightening the availability of voluntary departure is one way to show that the Federal government is serious about its immigration laws and the consequences of violating them. Such measures help to constrict the universe of aliens who overstay or otherwise violate the conditions of their visas. Eliminating the availability of “voluntary departure” in removal proceedings might also streamline the process, effectively eliminating an issue for appeals.

**Putting the Burden of Proof on Violators of Visas.** Congress should amend Section 236(a) of the INA with new language to make it unmistakably clear that, in bond re-determination hearings before immigration judges (cases involving aliens who have been charged with violating immigration laws), aliens charged with violations of the law have the burden of proving that they are neither a danger to the community nor a flight risk.

This should apply to all aliens detained by INS pending removal proceedings, whether or not the grounds upon which their removal is sought are criminal. The presumption should be that anyone detained by INS pending removal proceedings meets one or both of the above requirements, with the presumption open to rebuttal by the respondent; rebuttal evidence should be more than unsubstantiated statements by the respondent. In cases requiring mandatory detention (such as aliens certified as terrorists by the Attorney General under Section 236A of the INA, as amended by Section 412 of the PATRIOT Act) and criminal aliens per Section 236(c) of the INA, the presumption would not be open to rebuttal. This would not change the existing obligation of the INS to prove that the respondent is an alien and is subject to a ground of inadmissibility or deportability; nor would it prevent the respondent from rebutting the INS’s evidence of alienage or the charges of an immigration violation.

**Increasing Access to Court Documents.** Federal courts should be required to make available to INS all court documents relevant to immigration removal proceedings. Criminal court documents are essential in supporting many of the charges in immigration hearings regarding an alien’s removability. Some courts and LEAs are less than helpful in supplying the documentation necessary to prove that an alien has been engaged in activities that violate the terms of his or her visa or that would make that individual ineligible for immigration relief or benefits.

Judges have been known to seal court documents so that a criminal conviction cannot be used by INS in removal hearings where such documents are needed to prove the elements of the criminal activity that render an alien subject to deportation or ineligible for immigration benefits or relief. For example, a Pre-Sentencing

Investigation is the report of a court-appointed official to the judge on the facts of the crime committed; this report is used by the judge to determine the sentence to be imposed on the defendant. Such reports, which contain details of the criminal activity for which the alien was convicted, can be critical to the enforcement of immigration laws. They may detail the age of the victim, the relationship of the victim to the alien, or the amount of loss to the victim, information that may be essential to proving an alien's removability but which may not be included in the record of conviction. In the case of credit card fraud, the conviction documents may not specify the amount of the victim's loss, but the loss must be known in order to determine the immigration consequences of this crime. Cooperation in providing conviction and related documents should be encouraged for all Local, State, and Federal LEAs and courts as part of a concerted effort to improve respect for and enforcement of immigration laws.

**Key Step #2. The Attorney General should direct the implementation of comprehensive procedures for handling immigration cases that have national security aspects or involve classified documents.** For example, the Attorney General could designate one judicial location where such cases should be considered, provide for special training of potential trial attorneys in the handling of classified information, and require trial attorneys in these cases, as well as immigration judges, interpreters, bailiffs, and necessary support personnel, to have a security clearance. The suitable location should be one where defense attorneys are readily available.

**Key Step #3. The Attorney General should direct Federal LEAs to work with State and Local LEAs to develop a standardized, comprehensive format for criminal "rap sheets."** These sheets should be made available to the INS in a reliable secure format for enforcement purposes—both for determining eligibility for benefits and for use in removal proceedings.

## **PRIORITY #5: REDUCE THE OPPORTUNITIES FOR IDENTITY THEFT AND FRAUD IN STATE IDENTITY DOCUMENT SYSTEMS.**

The September 11 atrocities showed that terrorists will use fraudulently obtained identification to blend in and move through society undetected. It also proved that they will exploit those States with systems most liable to fraud. Any State that continues to run a document system subject to fraud and abuse places the lives of all Americans in jeopardy. The creation of a fraud-proof driver's license and identification card system would make it far more difficult for terrorists to enter the country unlawfully and to move about freely. The new system would also limit the growing problem of identity theft.

Currently, state-issued identity cards suffer from three deficiencies:

1. They are easily counterfeited.
2. There is little effort to determine whether the information the applicant provides is true.
3. There is often little or no effort to determine whether the card applicant is in the United States lawfully.

The present state identity card system should be reformed in the following manner:

**Key Step #1. State governments, working with the National Governors' Association, the U.S. Conference of Mayors, the OHS Director, and the Department of Justice, should initiate programs to improve certificates of identity, including the development of new tamper-proof documents.** States need to develop mechanisms to determine that the recipients of driver's licenses and other state-issued certificates of residency are indeed valid, legal recipients.

States should not issue certificates of identity or residence except to individuals who provide (a) proof of citizenship or (b) a valid passport and a tamper-proof document demonstrating their lawful presence in the United States. In ascertaining citizenship, states should not accept birth certificates and Social Security cards at face value, since these documents are easy to counterfeit or obtain fraudulently. Instead, the issuing Department of Motor Vehicles should check the authenticity of the information on any document with the agency that issued it; there should be a mechanism to determine whether the same name, birth date, and Social Security number have been used to obtain a driver's license for another individual living elsewhere. There should be an automatic cross-check of death records to bar terrorists and other criminals from attempting to assume the identities of deceased individuals.

States should require aliens who apply for a driver's license to provide a passport and valid tamper-proof U.S. visa. The alien's immigration status, registration number, and permitted length of stay should be included on the license and in the electronic file.

States should redesign all driver's licenses and identity cards to be machine-readable and to include a digitized photograph that can be electronically matched against a duplicate photo in a central DMV electronic file. Police and other organizations seeking to verify identities would use scanning machines to compare the picture and other information on the card with the matching electronic data. The FBI Director also should cooperate in the creation of tamper-proof driver's licenses and identity documents.

The new fraud-proof driver's licenses should be used in all circumstances in which current driver's licenses are used to confirm an individual's identity. These include boarding an airplane, entering a secure or sensitive area, renting or purchasing a vehicle, opening a bank account, and in police traffic stops. In addition, the Federal government or the States might require that fraud-proof identification be used in other transactions, such as renting a hotel room or buying rail or bus tickets. This would further hamper the ability of terrorists to move about the country unlawfully.

**Key Step #2: State governments, working in cooperation with the Federal government, should strengthen existing mechanisms for recording all domestic documents (such as birth certificates, death certificates, and driver's licenses).** Electronic data from the 50 state DMVs should be pooled so that the authenticity of a driver's license from one state can be confirmed when the license is used in another state. The entire system should be checked automatically for attempted duplicate entries: instances in which two different persons have attempted to use the same name, date of birth, and Social Security number.

**Key Step #3. The OHS Director, in coordination with the Chairman of the Federal Trade Commission, the Attorney General, and State governments, should develop a mechanism to enhance the Federal-level mechanism to deter and obstruct identity theft.** An enhanced nationwide registry should be established for those who have had documents containing sensitive personal information lost or stolen, such as a passport, driver's license, credit card, or other documents containing such personal information. Individuals who have been victimized by the theft of such documents normally report such losses to local law enforcement authorities, banks, and credit card companies and credit bureaus. A national registry of these cases would provide additional protection against identity theft.

The Identity Theft and Assumption Deterrence Act of 1998 (P.L. 105-318) made identity theft a federal crime and mandated that the Federal Trade Commission (FTC) establish procedures to "log and acknowledge the receipt of complaints" of the victims of identity theft and to refer complaints to "appropriate law enforcement agencies for potential law enforcement action" (Section 5). As currently implemented by the FTC, the victim of identity theft must report to the relevant local LEA, banks, and the major credit bureaus before the FTC refers the complaint to the Department of Justice. This current structure should form the basis for an expanded registry with an active interface with law enforcement in situations of identity theft.

## **PRIORITY #6: CREATE A MECHANISM TO MONITOR RECENT ANTI-MONEY-LAUNDERING INITIATIVES TO OBSTRUCT THE FINANCING OF TERRORISM.**

An oversight mechanism is needed to anticipate how those who threaten the United States may circumvent existing anti-money-laundering restrictions. Many of the deficiencies in pre-September 11 efforts to obstruct, if not stop, the financing of terrorist activities have been addressed in the International Money-Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Title III of the PATRIOT Act). This law represents a good advance in combating money laundering by terrorists and the sponsors of terrorism. Nevertheless, those who seek to harm the United States can still buy the best financial and legal advice available to help them circumvent current reporting and regulatory structures.

**Key Step.** The Secretary of the Treasury should direct the creation of a mechanism to evaluate how the current law to obstruct terrorists' finances could be circumvented. The Treasury Secretary should direct the Foreign Terrorist Asset Tracking Center, the Financial Crimes Enforcement Network (FinCEN), and the U.S. Customs Service, working with the Attorney General and the DCI, to establish a mechanism to anticipate how the current banking and financial restrictions can be circumvented by terrorists or sponsors of terrorism so that remedial steps can be taken.

## **CONCLUSION**

September 11 starkly demonstrated that attacks on the American homeland can come from unexpected sources using unexpected means. Enhancing the relationship between Federal law enforcement agencies and the Intelligence Community, as well as enhancing the relationship between Federal, State, and Local agencies, is essential to addressing the ongoing threats to the American people. The multifaceted approach should reflect the understanding that there is no one-size-fits-all remedy. The Administration, Congress, state officials, and the private sector have correctly turned their attention to the need to deter and prevent, and to respond to, future terrorist attacks.

The Federal government should foster the development of a uniform methodology for assessing America's vulnerabilities and the means to address those threats, including a national homeland security strategy, to ensure that resources are allocated to meet critical needs. It should take steps to improve the collection of information by Federal agencies and to enhance information sharing with State and Local officials. It must strengthen the visa approval process, the entry-exit system

for aliens traveling to and from the United States, and the ability of law enforcement to enforce existing immigration laws. And it should create a mechanism to monitor recent initiatives to obstruct money laundering by terrorists and their allies.

State and Local governments also have a role as the first responders. They should take immediate steps to identify the critical targets within their respective jurisdictions and assess the threat to those targets, sharing these assessments with Office of Homeland Security. They also should improve the information collection and analysis mechanisms of their respective law enforcement and/or first-responder agencies; designate State and Local officials to interact with their Federal counterparts; and eliminate the opportunities for fraud in state identity document systems. Such a multifaceted, broad-based approach will help assure Americans that government is doing its best to protect them from future terrorist attacks.

Table 5

### Status of Key Unimplemented Commission Recommendations for Improving Intelligence and Law Enforcement

Recommendation	Name of Commission	Status
<b>Intelligence Collection.</b> Expand multidisciplinary collection, specifically expanding research and development in signals intelligence (SIGINT) and measurement and signature intelligence (MASINT).	Gilmore Commission Bremer Commission	No known vehicle for the expansion of multidisciplinary collection efforts has yet been introduced.
<b>Language Capability.</b> Develop a larger pool of linguists and an interagency strategy for employing them.	Bremer Commission	The FBI has posted public recruitment for contract linguists. The CIA has added positions for language instructors on the employment site in nine languages.
<b>Intelligence-Sharing.</b> Improve the sharing and dissemination of intelligence information among Federal agencies and between State and Local agencies.	Gilmore Commission Bremer Commission National Defense Panel	On October 29, 2001, Federal officials announced the creation of the Foreign Terrorist Tracking Task Force (FTTF) to “enhance United States efforts to prevent terrorist activity.” Based on the New York Joint Terrorism Task Force, which began in 1980 with members of the NYPD and 11 FBI investigators, the FTTF now includes over 100 members from several agencies at both the state and local levels. There are 36 similar task forces nationwide.
<b>Intelligence Funding.</b> Fund intelligence capabilities at adequate and sustained levels.	Hart–Rudman Commission Bremer Commission	The Intelligence Authorization bill for FY 2002 (H.R. 2883) was signed by the President on December 28, 2001. It reportedly provides an increase in funding for FY 2002, although amounts are classified.
<b>Money Laundering and Financing of Terrorism.</b> Disrupt and halt the sources of financing for terrorist activities.	Bremer Commission	Executive Order 13224, issued on September 23, 2001, suspended the assets and bank accounts of individuals and organizations suspected of involvement in terrorism. Title III of the PATRIOT Act (P.L. 107–56) strengthens legal mechanisms to monitor and obstruct international money laundering by individuals or groups suspected of involvement in terrorism.
<b>Terrorist Deterrence.</b> Develop deterrence initiatives against those states that either sponsor terrorism directly or allow their territory to be used by terrorists; methods should include denial of participation in certain visa programs.	Bremer Commission	Since September 11, numerous pieces of legislation have been introduced in both houses of Congress to address deficiencies in immigration and border enforcement mechanisms. The general thrust of these proposed bills is, inter alia, to strengthen the visa approval and the inspection and admission processes and the monitoring of foreign visitors, especially foreign students; to require the sharing of information among law enforcement and intelligence agencies; and to fund the hiring of additional personnel. The House approved one of the bills, H.R. 3525, the Enhanced Border Security and Visa Entry Reform Act, on December 19, 2001. It would authorize the hiring and training of personnel, require interagency information sharing, restrict the use of visas, and strengthen admission and inspection mechanisms.