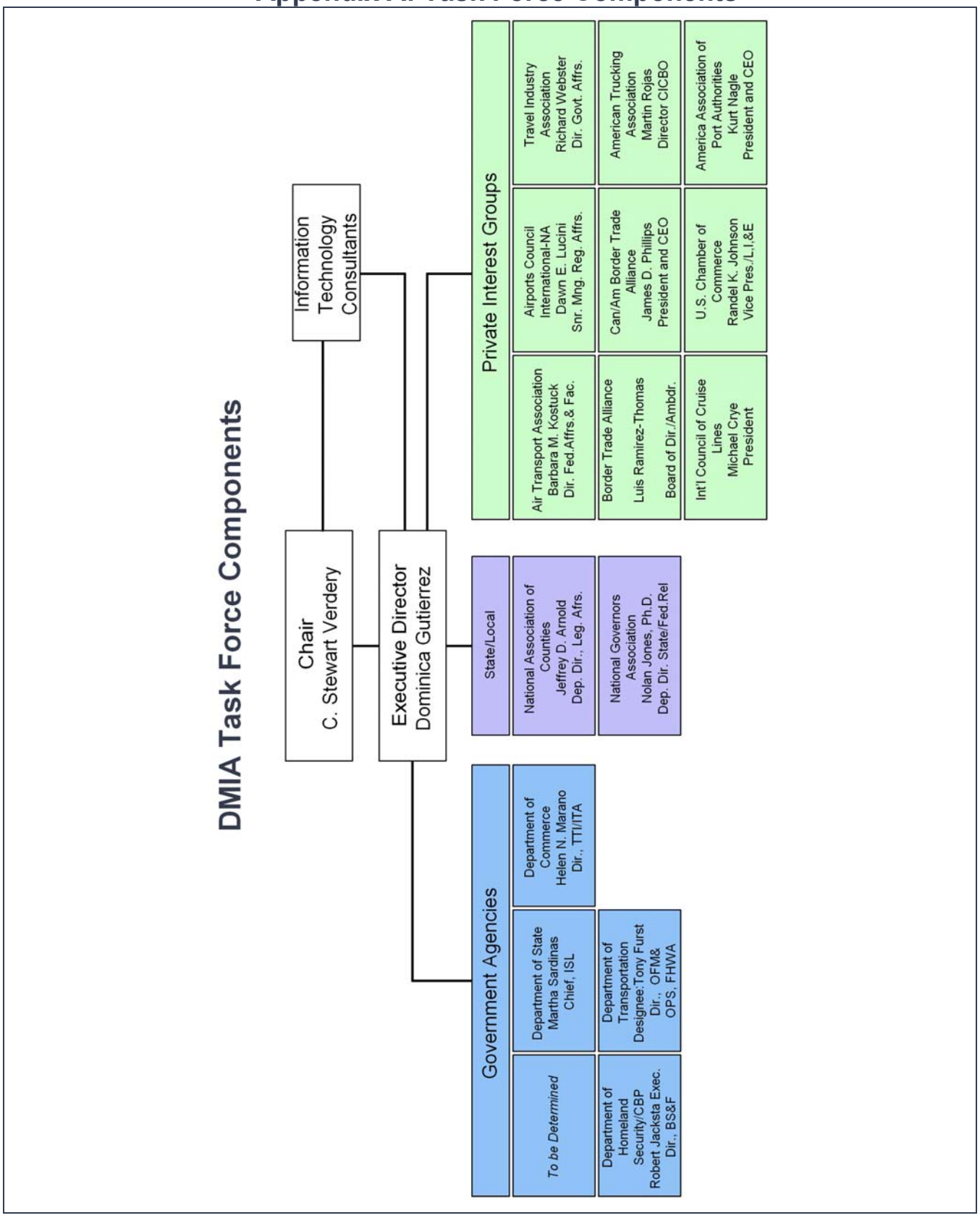
Appendix A: Task Force Components



The Canadian/American Border Trade Alliance (Can/Am BTA): The Canadian/American Border Trade Alliance, formed in 1992, is a transcontinental, bi-national, broad-based organization with participation from all 27 states (Washington to Maine including Alaska) on or near the U.S./Canada Border and the Canadian Provinces. Can/Am BTA participants include members from border trade, border crossing and transportation segments including producers, shippers, brokers, mode transportation providers, bridge and tunnel operators, chambers of commerce, business and trade corridor associations and economic development and government agencies. The combined network involves over 60,000 companies and organizations in their individual memberships. The Can/Am BTA acts, as one of its prime focuses, to resolve issues, problems and needs border-wide to achieve appropriate border crossing practices, policies and resources at the U.S./Canada borders.

American Trucking Associations: The American Trucking Associations is the national trade association of the trucking industry. American Trucking Associations is a federation of affiliated state trucking associations, conferences, and other organizations that together include more than 37,000 motor-carrier members, representing every type and class of motor carrier in the country. American Trucking Associations represents an industry that employs nearly 10 million people, providing one out of every 14 civilian jobs. This includes the more than 3 million truck drivers who travel over 400 billion miles per year to deliver to Americans 86 percent of their transported food, clothing, finished products, raw materials, and other items.

American industrial and commercial enterprises are able to compete more effectively in the global marketplace due to the benefits of safe and efficient trucking. Truck transportation is the most flexible mode for freight shipment, providing door-to-door service to every city, manufacturing plant, warehouse, retail store, and home in the country. Trucks are the only providers of goods to 75 percent of American communities. Five percent of the nation's gross domestic product, roughly $600 billion, is created by truck transportation. Actions that affect the trucking industry's ability to move its annual 8.9 billion tons of domestic freight and our international operations with Canada and Mexico have significant consequences for our country's economic wellbeing.

U.S. Chamber of Commerce: The U.S. Chamber of Commerce is the world's largest business federation, representing more than 3 million businesses and organizations of every size, sector, and region, including membership of international corporations and businesses. The Chamber has membership in all 50 states and 95 American Chambers of Commerce (AmChams) abroad. Through this federation, the Chamber is engaged at all levels of government on border issues, through its state and local chambers at the local levels, nationally in Washington, D.C., and internationally through our AmChams and involvement in multilateral meetings and conferences, including interactions with all of the major embassies in Washington and U.S. embassies and consulates around the world. Chamber members sit on many task forces and advisory councils to local, state, and federal governments, including the DMIA Task Force, and the Chamber chairs the Americans for Better Borders coalition of over 80 member organizations and companies that helped craft the Data Management Improvement Act, the Enhanced Border Security and Visa Entry Reform Act, and other significant border-related legislation.

Airports Council International-North America (ACI-NA): ACI-NA was first established as the Airport Operators Council in 1947, today it is the "Voice of Airports" representing local, regional, and state governing bodies that own and operate commercial airports throughout the U.S. and Canada. ACI-NA is the largest of six worldwide regions of Airports Council International (ACI), based in Geneva, Switzerland. ACI's other regions include Europe, Asia, Pacific, Africa and Latin America/Caribbean.

The mission of ACI-NA states that ACI-NA shall identify, develop and advance common policies and programs for the enhancement and promotion of airports and their managements that are effective, efficient and responsive to consumer and community needs. One of the premier airport associations, ACI-NA offers the pre-eminent North American airports a forum for the exchange of ideas and information. Its staff is headquartered in Washington, DC, and Ottawa, Canada, providing ACI-NA with direct access to the federal government, industry partners, and related aviation associations.

As a member association, ACI-NA helps its members develop common positions and communicate them among the government, the press, and the general public. We are recognized as the authoritative voice of airports, and represent airports that carry 98 percent of all passenger traffic and almost all cargo traffic throughout North America. Over 380 aviation-related businesses are also associate members of ACI-NA.

Air Transport Association of America, Inc.: Founded in 1936, the Air Transport Association of America, Inc., is the oldest and largest airline trade association in the U.S. Its U.S. members account for 95 percent of the passenger and cargo traffic carried by U.S. scheduled airlines. The Air Transport Association serves its member airlines and their customers by: assisting the airline industry in continuing to provide the world's safest system of transportation; transmitting technical expertise and operational knowledge among member airlines to improve safety, service, and efficiency; advocating fair airline taxation and regulation worldwide, ensuring a profitable and competitive industry; and by developing and coordinating industry actions that are environmentally beneficial, economically reasonable, and technologically feasible.

Border Trade Alliance (BTA): Since 1986, the Border Trade Alliance has been a leading authority on international trade and commerce throughout North America. The organization is a grassroots, non-profit organization that provides a forum for discussion and advocacy on border issues as varied as customs procedures, immigration, infrastructure, and the environment. A network of public and private sector representatives from the United States, Mexico and Canada, the BTA's core values include a commitment to improving the quality of life in border communities through trade and commerce and a commitment to work as a community-based grassroots organization.

National Association of Counties (NACo): NACo, the only national organization that represents county governments in the United States. With its headquarters on Capitol Hill, NACo is a full-service organization that provides an extensive line of services including legislative, research, technical, and public affairs assistance, as well as enterprise services to its members. The association acts as a liaison with other levels of government, works to improve public understanding of counties, serves as a national advocate for counties and

provides them with resources to help them find innovative methods to meet the challenges they face.

National Governors Association (NGA): NGA is the collective voice of the nation's governors and one of Washington, D.C.'s, most respected public policy organizations. NGA provides governors and their senior staff members with services that range from representing states on Capitol Hill and before the Administration on key federal issues to developing policy reports on innovative state programs and hosting networking seminars for state government executive branch officials. The NGA Center for Best Practices focuses on state innovations and best practices on issues that range from education and health to technology, welfare reform, and the environment. NGA also provides management and technical assistance to both new and incumbent governors.

American Association of Port Authorities (AAPA): Founded in 1912, the American Association of Port Authorities is a trade association representing the interests of 150 public ports in the Western Hemisphere. Our membership also consists of 300 sustaining members. On behalf of its U.S. members, AAPA is active in Washington partnering with Congress, the Federal Government and other trade associations to advance the interests of public ports. U.S. ports serve vital national interests by facilitating the flow of trade and cruise passengers and supporting the mobilization and deployment of U.S. troops. In the next twenty years, U.S. overseas international trade, 95% of which enters or exits through the nation's ports, is expected to double. As the link between the land and the water, ports continue to update and modernize their facilities not only to accommodate this growth, but also to ensure homeland security.

International Council of Cruise Lines (ICCL): The International Council of Cruise Lines (ICCL) is a non-profit trade association that represents the interests of 15 passenger cruise lines in North America and abroad, and a growing number of cruise industry strategic business partners.

The ICCL participates in the regulatory and policy development process and promotes all measures that foster a safe, secure and healthy cruise ship environment. Under the direction of the chief executives of its member lines, the ICCL advocates industry positions to key local, state, federal authorities, the International Maritime Organization (IMO) and the International Labor Organization (ILO) to develop and strengthen guidelines and regulations. At the federal level, we work closely with many agencies, including the State Department, Commerce Department and various agencies at the Department of Homeland Security, (DHS), which now include the U.S. Coast Guard, the Transportation Security Administration (TSA), and Customs and Border Protection. The ICCL actively monitors international shipping policy and develops recommendations to its membership on a wide variety of issues.

Each year the ICCL commissions an economic study that demonstrates the cruise industry is a significant contributor to the U.S. economy. In the years ahead, it is projected that the cruise industry will continue to grow, providing opportunities for U.S. industries and employees to benefit from the expansion of this business.

Assisted by a staff in Arlington, VA, the ICCL's members include the largest passenger cruise lines that call on hundreds of ports in the U.S. and abroad. The ICCL Associate Members represent the industry suppliers and strategic business partners. Each year the ICCL's overnight cruise ship operators carry more than 10 million passengers on over 100 ships.

Travel Industry Association of America (TIA): TIA has been in existence since 1941. It is a Washington, DC based, non-profit association that represents and speaks for the common interests and concerns of all components of the U.S. travel industry. TIA is a recognized leader in promoting and facilitating increased travel to and within the United States in order to make America the world's number one tourism destination. TIA is the authoritative and recognized source of research, analysis and forecasting for the entire industry and its primary spokesperson to the domestic and international media. TIA's mission is to represent the whole of the U.S. travel and tourism industry to promote and facilitate increased travel to, and within, the United States.

U.S. Department of Commerce (DOC): The DOC promotes job creation, economic growth, sustainable development and improved living standards for all Americans by working in partnership with business, universities, communities and workers to build for the future and promote U.S. competitiveness in the global marketplace by strengthening and safeguarding the nation's economic infrastructure. The DOC keeps America competitive with cutting-edge science and technology and an unrivaled information base providing effective management and stewardship of the nation's resources and assets to ensure sustainable economic opportunities.

U.S. Department of Transportation (DOT): The DOT was established by an act of Congress on October 15, 1966, the DOT's first official day of operation was April 1, 1967. The mission of DOT is to serve the United States by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future.

Americans depend on safe, efficient, and secure transportation systems. Whether we travel on roads, boats, rails, or in the air, we rely on our transportation systems to get us where we need to go. These same systems play a supporting role in our national economic well being, making it possible to move goods from place to place -- ensuring our continued success in the global marketplace. The DOT works in tandem with our transportation systems by providing leadership and guidance on behalf of the public.

U.S. Department of State (DOS): The Executive Branch and the Congress have constitutional responsibilities for U.S. foreign policy. Within the Executive Branch, the Department of State is the lead U.S. foreign affairs agency, and the Secretary of State is the President's principal foreign policy adviser. The Department advances U.S. objectives and interests in shaping a freer, more secure, and more prosperous world through its primary role in developing and implementing the President's foreign policy. The Department also supports the foreign affairs activities of other U.S. Government entities including the Department of Commerce and the Agency for International Development. It also provides an array of important services to United States citizens and to foreigners seeking to visit or immigrate to the U.S.

Appendix B: Legislation and Regulation(s) Affecting Border Management

The following is a list of legislative and regulatory mandates that have helped shape the mission and role of the DMIA Task Force, followed by the complete text of the DMIA.

North American Free Trade Agreement (NAFTA), Public Law 103-182, Signed December 18, 1993

Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104-208, Signed September 30, 1996

Data Management Improvement Act (DMIA), Public Law 106-215, Signed June 15, 2000

The Visa Waiver Permanent Program Act (VWPPA), Public Law 106-396, Signed October 30, 2000

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), Public Law 107-56, Signed October 26, 2001

Aviation and Transportation Security Act, Public Law 107-71, Signed November 11, 2001

The Enhanced Border Security and Visa Entry Reform Act of 2002 (BSA), Public Law 107-173, Signed May 14, 2002

Trade Act of 2002, Public Law 107-210, Signed August 6, 2002

The 24-Hour Rule, 67 FR (Federal Register) 66318 (RIN 1515-AD11)
Published in the Federal Register, October 31, 2002 to be effective December 2, 2002

Maritime Transportation Security Act (MTSA), Public Law 107-295, Signed November 25, 2002

Homeland Security Act, Public Law 107-296, Signed November 25, 2002

Immigration and Naturalization Service Data Management Improvement Act of 2000

Pub. L. 106-215 Immigration and Naturalization Service Data Management Improvement Act of 2000

106th Congress
June 15, 2000
114 Stat. 337

———————

[H.R. 4489]

An Act

To amend section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Immigration and Naturalization Service Data Management Improvement Act of 2000”.

SEC. 2. AMENDMENT TO SECTION 110 OF IIRIRA.

(a) IN GENERAL- Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1221 note) is amended to read as follows:

“SEC. 110. INTEGRATED ENTRY AND EXIT DATA SYSTEM.

“(a) REQUIREMENT- The Attorney General shall implement an integrated entry and exit data system.

“(b) INTEGRATED ENTRY AND EXIT DATA SYSTEM DEFINED- For purposes of this section, the term `integrated entry and exit data system' means an electronic system that--

“(1) provides access to, and integrates, alien arrival and departure data that are--

“(A) authorized or required to be created or collected under law;

“(B) in an electronic format; and

“(C) in a data base of the Department of Justice or the Department of State, including those created or used at ports of entry and at consular offices;

“(2) uses available data described in paragraph (1) to produce a report of arriving and departing aliens by country of nationality, classification as an immigrant or nonimmigrant, and date of arrival in, and departure from, the United States;

“(3) matches an alien's available arrival data with the alien's available departure data;

“(4) assists the Attorney General (and the Secretary of State, to the extent necessary to carry out such Secretary's obligations under immigration law) to identify, through on-line searching procedures, lawfully admitted nonimmigrants who may have remained in the United States beyond the period authorized by the Attorney General; and

“(5) otherwise uses available alien arrival and departure data described in paragraph (1) to permit the Attorney General to make the reports required under subsection (e).

“(c) CONSTRUCTION-

“(1) NO ADDITIONAL AUTHORITY TO IMPOSE DOCUMENTARY OR DATA COLLECTION REQUIREMENTS- Nothing in this section shall be construed to permit the Attorney General or the Secretary of State to impose any new documentary or data collection requirements on any person in order to satisfy the requirements of this section, including--

“(A) requirements on any alien for whom the documentary requirements in section 212(a)(7)(B) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(7)(B)) have been waived by the Attorney General and the Secretary of State under section 212(d)(4)(B) of such Act (8 U.S.C. 1182(d)(4)(B)); or

“(B) requirements that are inconsistent with the North American Free Trade Agreement.

“(2) NO REDUCTION OF AUTHORITY- Nothing in this section shall be construed to reduce or curtail any authority of the Attorney General or the Secretary of State under any other provision of law.

“(d) DEADLINES-

“(1) AIRPORTS AND SEAPORTS- Not later than December 31, 2003, the Attorney General shall implement the integrated entry and exit data system using available alien arrival and departure data described in subsection (b)(1) pertaining to aliens arriving in, or departing from, the United States at an airport or seaport. Such implementation shall include ensuring that such data, when collected or created by an immigration officer at an airport or seaport, are entered into the system and can be accessed by immigration officers at other airports and seaports.

“(2) HIGH-TRAFFIC LAND BORDER PORTS OF ENTRY- Not later than December 31, 2004, the Attorney General shall implement the integrated entry and exit data system using the data

described in paragraph (1) and available alien arrival and departure data described in subsection (b)(1) pertaining to aliens arriving in, or departing from, the United States at the 50 land border ports of entry determined by the Attorney General to serve the highest numbers of arriving and departing aliens. Such implementation shall include ensuring that such data, when collected or created by an immigration officer at such a port of entry, are entered into the system and can be accessed by immigration officers at airports, seaports, and other such land border ports of entry.

“(3) REMAINING DATA- Not later than December 31, 2005, the Attorney General shall fully implement the integrated entry and exit data system using all data described in subsection (b)(1). Such implementation shall include ensuring that all such data are available to immigration officers at all ports of entry into the United States.

“(e) REPORTS-

“(1) IN GENERAL- Not later than December 31 of each year following the commencement of implementation of the integrated entry and exit data system, the Attorney General shall use the system to prepare an annual report to the Committees on the Judiciary of the House of Representatives and of the Senate.

“(2) INFORMATION- Each report shall include the following information with respect to the preceding fiscal year, and an analysis of that information:

“(A) The number of aliens for whom departure data was collected during the reporting period, with an accounting by country of nationality of the departing alien.

“(B) The number of departing aliens whose departure data was successfully matched to the alien's arrival data, with an accounting by the alien's country of nationality and by the alien's classification as an immigrant or nonimmigrant.

“(C) The number of aliens who arrived pursuant to a nonimmigrant visa, or as a visitor under the visa waiver program under section 217 of the Immigration and Nationality Act (8 U.S.C. 1187), for whom no matching departure data have been obtained through the system or through other means as of the end of the alien’s authorized period of stay, with an accounting by the alien’s country of nationality and date of arrival in the United States.

“(D) The number of lawfully admitted nonimmigrants identified as having remained in the United States beyond the period authorized by the Attorney General, with an accounting by the alien's country of nationality.

“(f) AUTHORITY TO PROVIDE ACCESS TO SYSTEM-

“(1) IN GENERAL- Subject to subsection (d), the Attorney General, in consultation with the Secretary of State, shall determine which officers and employees of the Departments of Justice and State may enter data into, and have access to the data contained in, the integrated entry and exit data system.

“(2) OTHER LAW ENFORCEMENT OFFICIALS- The Attorney General, in the discretion of the Attorney General, may permit other Federal, State, and local law enforcement officials to have access to the data contained in the integrated entry and exit data system for law enforcement purposes.

“(g) USE OF TASK FORCE RECOMMENDATIONS- The Attorney General shall continuously update and improve the integrated entry and exit data system as technology improves and using the recommendations of the task force established under section 3 of the Immigration and Naturalization Service Data Management Improvement Act of 2000.

“(h) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to carry out this section such sums as may be necessary for fiscal years 2001 through 2008.”

(b) CLERICAL AMENDMENT- The table of contents of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 is amended by amending the item relating to section 110 to read as follows:

“Sec. 110. Integrated entry and exit data system.”.

SEC. 3. TASK FORCE.

(a) ESTABLISHMENT- Not later than 6 months after the date of the enactment of this Act, the Attorney General, in consultation with the Secretary of State, the Secretary of Commerce, and the Secretary of the Treasury, shall establish a task force to carry out the duties described in subsection (c) (in this section referred to as the “Task Force”).

(b) MEMBERSHIP-

(1) CHAIRPERSON; APPOINTMENT OF MEMBERS- The Task Force shall be composed of the Attorney General and 16 other members appointed in accordance with paragraph (2). The Attorney General shall be the chairperson and shall appoint the other members.

(2) APPOINTMENT REQUIREMENTS- In appointing the other members of the Task Force, the Attorney General shall include--

(A) representatives of Federal, State, and local agencies with an interest in the duties of the Task Force, including representatives of agencies with an interest in--

(i) immigration and naturalization;

(ii) travel and tourism;

(iii) transportation;

(iv) trade;

(v) law enforcement;

(vi) national security; or

(vii) the environment; and

(B) private sector representatives of affected industries and groups.

(3) TERMS- Each member shall be appointed for the life of the Task Force. Any vacancy shall be filled by the Attorney General.

(4) COMPENSATION-

(A) IN GENERAL- Each member of the Task Force shall serve without compensation, and members who are officers or employees of the United States shall serve without compensation in addition to that received for their services as officers or employees of the United States.

(B) TRAVEL EXPENSES- The members of the Task Force shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of service for the Task Force.

(c) DUTIES- The Task Force shall evaluate the following:

(1) How the Attorney General can efficiently and effectively carry out section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1221 note), as amended by section 2 of this Act.

(2) How the United States can improve the flow of traffic at airports, seaports, and land border ports of entry through--

(A) enhancing systems for data collection and data sharing, including the integrated entry and exit data system described in section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1221note), as amended by section 2 of this Act, by better use of technology, resources, and personnel;

(B) increasing cooperation between the public and private sectors;

(C) increasing cooperation among Federal agencies and among Federal and State agencies; and

(D) modifying information technology systems while taking into account the different data systems, infrastructure, and processing procedures of airports, seaports, and land border ports of entry.

(3) The cost of implementing each of its recommendations.

(d) STAFF AND SUPPORT SERVICES-

(1) IN GENERAL- The Attorney General may, without regard to the civil service laws and regulations, appoint and terminate an executive director and such other additional personnel as may be necessary to enable the Task Force to perform its duties. The employment and termination of an executive director shall be subject to confirmation by a majority of the members of the Task Force.

(2) COMPENSATION- The executive director shall be compensated at a rate not to exceed the rate payable for level V of the Executive Schedule under section 5316 of title 5, United States Code. The Attorney General may fix the compensation of other personnel without regard to the provisions of chapter 51 and subchapter III of chapter 53 of title 5, United States Code, relating to classification of positions and General Schedule pay rates, except that the rate of pay for such personnel may not exceed the rate payable for level V of the Executive Schedule under section 5316 of such title.

(3) DETAIL OF GOVERNMENT EMPLOYEES- Any Federal Government employee, with the approval of the head of the appropriate Federal agency, may be detailed to the Task Force without reimbursement, and such detail shall be without interruption or loss of civil service status, benefits, or privilege.

(4) PROCUREMENT OF TEMPORARY AND INTERMITTENT SERVICES- The Attorney General may procure temporary and intermittent services for the Task Force under section 3109(b) of title 5, United States Code, at rates for individuals not to exceed the daily equivalent of the annual rate of basic pay prescribed for level V of the Executive Schedule under section 5316 of such title.

(5) ADMINISTRATIVE SUPPORT SERVICES- Upon the request of the Attorney General, the Administrator of General Services shall provide to the Task Force, on a reimbursable basis, the administrative support services necessary for the Task Force to carry out its responsibilities under this section.

(e) HEARINGS AND SESSIONS- The Task Force may, for the purpose of carrying out this section, hold hearings, sit and act at times and places, take testimony, and receive evidence as the Task Force considers appropriate.

(f) OBTAINING OFFICIAL DATA- The Task Force may secure directly from any department or agency of the United States information necessary to enable it to carry out this section. Upon request of the Attorney General, the head of that department or agency shall furnish that information to the Task Force.

(g) REPORTS-

(1) DEADLINE- Not later than December 31, 2002, and not later than December 31 of each year thereafter in which the Task Force is in existence, the Attorney General shall submit a report to the Committees on the Judiciary of the House of Representatives and of the Senate containing the findings, conclusions, and recommendations of the Task Force. Each report shall also measure and evaluate how much progress the Task Force has made, how much

work remains, how long the remaining work will take to complete, and the cost of completing the remaining work.

(2) DELEGATION- The Attorney General may delegate to the Commissioner, Immigration and Naturalization Service, the responsibility for preparing and transmitting any such report.

(h) LEGISLATIVE RECOMMENDATIONS-

(1) IN GENERAL- The Attorney General shall make such legislative recommendations as the Attorney General deems appropriate--

(A) to implement the recommendations of the Task Force; and

(B) to obtain authorization for the appropriation of funds, the expenditure of receipts, or the reprogramming of existing funds to implement such recommendations.

(2) DELEGATION- The Attorney General may delegate to the Commissioner, Immigration and Naturalization Service, the responsibility for preparing and transmitting any such legislative recommendations.

(i) TERMINATION- The Task Force shall terminate on a date designated by the Attorney General as the date on which the work of the Task Force has been completed.

(j) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to carry out this section such sums as may be necessary for fiscal years 2001 through 2003.

SEC. 4. SENSE OF THE CONGRESS REGARDING INTERNATIONAL BORDER MANAGEMENT COOPERATION.

It is the sense of the Congress that the Attorney General, in consultation with the Secretary of State, the Secretary of Commerce, and the Secretary of the Treasury, should consult with affected foreign governments to improve border management cooperation.

Approved June 15, 2000.

Appendix C: Minimum Documentary Requirements for Entry to U.S.

DOCUMENTARY REQUIREMENTS (Minimum)			
APPLICANT	**COMING FROM CONTIGUOUS TERRITORY**[59]	**COMING FROM WESTERN HEMISPHERE**[60]	**COMING FROM EASTERN HEMISPHERE**[61]
US CITIZENS[62]	• Verbal declaration or • Proof of citizenship.	• Verbal declaration or • Proof of citizenship.	• Valid passport
Lawful Permanent Residents (passport and visa not required) **Outside the US for less than 1 year.**	• Permanent Resident Card, I-551; or • Expired I-551 with Notice of Action, I-797, indicating card has been extended; or • Expired I-551 presented by USG employee if 1) is a civilian or military employee in possession of official orders; or 2) is the spouse or child of the employee and is preceding or accompanying, or following to join employee or serviceperson within four months of his return to the US; or • Temporary Residence Stamp (ADIT stamp) in passport or I-94; or • Reentry permit, I-327; or • Refugee Travel Document, I-571.	• Permanent Resident Card, I-551; or • Expired I-551 with Notice of Action, I-797, indicating card has been extended; or • Expired I-551 presented by USG employee if 1) is a civilian or military employee in possession of official orders; or 2) is the spouse or child of the employee and is preceding or accompanying, or following to join employee or serviceperson within four months of his return to the US; or • Temporary Residence Stamp (ADIT stamp) in passport or I-94; or • Reentry permit, I-327; or • Refugee Travel Document, I-571.	• Permanent Resident Card, I-551; or • Expired I-551 with Notice of Action, I-797, indicating card has been extended; or • Expired I-551 presented by USG employee if 1) is a civilian or military employee in possession of official orders; or 2) is the spouse or child of the employee and is preceding or accompanying, or following to join employee or serviceperson within four months of his return to the US; or • Temporary Residence Stamp (ADIT stamp) in passport or I-94; or • Reentry permit, I-327; or • Refugee Travel Document, I-571.

[59] Canada and/or Mexico
[60] North America, Central America, South America
[61] Europe, Asia, Australia, Africa, Oceania.
[62] No US Passport required when subject is traveling:

- With a Valid Merchant Marine ID or Air Crewman ID card.
- Member of the US Armed Forces on active duty.
- Under twelve years old, with evidence of U.S.C. at time of entering, and included in the foreign passport of parent.
- Has been authorized by the Secretary of State with waiver of passport requirement.

DOCUMENTARY REQUIREMENTS (Minimum)			
APPLICANT	**COMING FROM CONTIGUOUS TERRITORY**	**COMING FROM WESTERN HEMISPHERE**	**COMING FROM EASTERN HEMISPHERE**
Lawful Permanent Residents (passport and visa not required) **Outside the US for less than 2 years.**	• Reentry permit, I-327; or • Refugee Travel Document, I-571; or • Immigrant visa (SB-1 IV)	• Reentry permit, I-327; or • Refugee Travel Document, I-571; or • Immigrant visa (SB-1 IV)	• Reentry permit, I-327; or • Refugee Travel Document, I-571; or • Immigrant visa (SB-1 IV)
Lawful Permanent Residents **Outside the US for more than 2 years. (*Passport Required unless otherwise noted.)***	• Immigrant Visa (SB-1)	• Immigrant Visa (SB-1)	• Immigrant Visa (SB-1)
American Indian born in Canada with 50%[63] American Indian Blood	• Must be able to prove status. • Exempt from all passport and visa requirements. • Exempt from all grounds of inadmissibility.		
NATO	Armed services personnel entering under NATO STATUS OF FORCES AGREEMENT (SOFA) and armed services personnel attached to NATO allied headquarters in the US are *visa and passport exempt.*		
Canadian Citizen	• Oral declaration and ID; or • Proof of citizenship	• Oral declaration and ID; or • Proof of citizenship • Crewmembers: no I-95	• Valid passport • Crewmembers: I-95 (*The following nonimmigrant classifications require a passport and visa: E1, E-2, K-1, K-2, K-3, K4. See INA Section 101(a).)*

[63] Tribal card without % is unacceptable.

DOCUMENTARY REQUIREMENTS (Minimum)			
APPLICANT	**COMING FROM CONTIGUOUS TERRITORY**	**COMING FROM WESTERN HEMISPHERE**	**COMING FROM EASTERN HEMISPHERE**
British Subjects with Residence in Bermuda or Canada[64]*	• Passport with nonimmigrant visa (NIV): I-94 • Crewmember: I-95	• Passport with NIV: I-94 • Crewmember: I-95	• Passport with NIV: I-94 • Crewmember: I-95
British Overseas Territory Citizens of Bermuda	• Oral declaration and ID; or • Proof of citizenship	• Oral declaration and ID; or • Proof of citizenship • Crewmembers: no I-95	• Valid passport • Crewmembers: I-95 (*The following nonimmigrant classifications require a passport and visa: E1, E-2, K-1, K-2, K-3, K4. See INA Section 101(a).)*
Canadian Landed Immigrant **with** British Common Nationality or a citizen of Ireland[65]*	• Passport with NIV: I-94 • Crewmember: I-95	• Passport with NIV: I-94 • Crewmember: I-95	• Passport with NIV: I-94 • Crewmember: I-95
Canadian Landed Immigrant **without** Common Nationality[66]*	• Passport with NIV: 1-94 • Crewmember: I-95	• Passport with NIV: I-94 • Crewmember: I-95	• Passport with NIV: I-94 • Crewmember: I-95
Mexican Citizen	Border Crossing Card (DSP-150), No I-94 required if in US < 72 hours and/or within 25 miles of the southern land border; or Passport with NIV.	• Passport and Border Crossing Card (DSP-150) as B1/B2 lieu visa, I-94 required. • PP with NIV.	• Passport and Border Crossing Card (DSP-150) as B1/B2 lieu visa, I-94 required; or • PP with NIV.

64 Exempt NIV under the Visa Waiver Program (VWP) when traveling for business or tourism.
65 Exempt NIV under the VWP when traveling for business or tourism.
66 Exempt NIV under the VWP when traveling for business or tourism.
*Effective March 17, 2003.

DOCUMENTARY REQUIREMENTS (Minimum)			
APPLICANT	**COMING FROM CONTIGUOUS TERRITORY**	**COMING FROM WESTERN HEMISPHERE**	**COMING FROM EASTERN HEMISPHERE**
Mexican (citizen) Crewmember on a commercial airplane belonging to a Mexican company	Visa not required if crewmember is employed on an aircraft belonging to a Mexican company authorized to engage in commercial transportation in the U.S. Passport is required.		
Mexican with diplomatic or official passport	No visa requirements as long as bearer is entering the US for 6 months as a visitor in the US. Spouse and dependents under 19 years old who have the same documents and accompany official at the time of entry are also visa and I-94 exempt.		
Mexican citizen entering the US pursuant to **International Boundary & Water Commission Treaty**	No visa and No passport requirement as long as individual is working directly or indirectly on construction, operation, and maintenance of works in the US in accordance with the Treaty.		
Citizens of Freely Associated States (Marshall Islands and Federated States of Micronesia), formerly the Trust Territory of the Pacific Islands.	• Proof of citizenship required. • Exempt passport and visa requirements.		
Transit Without Visa[67] **Please note that this program was suspended on August 2, 2003**	Passport and US NIV are not required as long as individual is being transported in immediate and continuous transit through the US in accordance with INA 238(D). Individual **must be admissible under immigration laws** and meet qualifications.		
Visa Waiver Program[68]	Passport requirement with return/onward ticket or proof of economic solvency.		

[67] Citizens from the following countries **MUST** HAVE A VISA: Afghanistan, Angola, Bangladesh, Belarus, Bosnia-Herzegovina, Burma, Burundi, Central African Republic, China, Colombia, Congo, Cuba, India, Iran, Iraq, Libya, Nigeria, North Korea, Pakistan, Sierra Leone, Somalia, Sri Lanka, Sudan, and Yugoslavia.
The following citizens may use the in-transit lounge if their carrier has an approved in-transit lounge agreement in approved POE: Bangladesh, India, Pakistan, and Sri Lanka.

[68] Nationals of the following countries are in the VWP: Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, United Kingdom.

SPECIAL CLASSES
Adjacent Islands[69]: Passport requirement, but no visa requirement for nationals and residents under the following conditions: 1. **Bahamian National or British subject residents of the Bahamas**: A visa is not required if, prior to boarding a carrier to the US, the passenger is pre-inspected in the Bahamas and determined to be admissible by the Bureau of Customs and Border Protection (CBP). 2. **British subject residents of the Cayman Islands or of the Turks and Caicos Islands**: A visa is not required if they come directly from the above islands to a US POE and present a current certificate from the Clerk of the Court showing no criminal record. 3. **National of Great Britain, France, the Netherlands, and nationals of adjacent Caribbean Islands that are independent countries**: A visa is not required if passenger is national of Great Britain, France, the Netherlands, Antigua, Barbados, Grenada, Jamaica, or Trinidad &Tobago; resides in British, French, or Dutch territories located in the adjacent islands; and is proceeding to the US as an agricultural worker or has a valid certificate from the Department of Labor granting employment in the US Virgin Islands. 4. **Nationals and residents of the British Virgin Islands traveling to the US Virgin Islands**: A visa is not required. 5. **Nationals and residents of the British Virgin Islands traveling to the US**: A visa is not required as long as individual is pre-inspected in St. Thomas and determined to be admissible by the CBP.

SPECIAL CLASSES
Guam Visa Waiver Program[70]**:** No visa requirement as long as: • Possess a valid, unexpired passport • Entry into Guam is for 15 days or less • Is a visitor for business or pleasure • Arrives in a signatory carrier • Holds a round trip ticket with a confirmed departure date not exceeding 15 days from date of admission Possess a completed and signed Guam Visa Waiver Information Form (I-736) and I-94.

[69] Anguilla, Antigua, Aruba, Bahamas, Barbados, Barbuda, Bermuda, Bonaire, British Virgin Islands, Cayman Islands, Curacao, Dominica, Dominican Republic, Grenada, Guadeloupe, Haiti, Jamaica, Marie-Galante, Martinique, Miquelon, Montserrat, Saba, St. Barthelemy, St. Christopher, St. Eustatius, St. Kitts-Nevis, St. Maarten, St. Pierre, St. Vincent and the Grenadines, Trinidad and Tobago, Turks and Caicos and the other British, French, and Netherlands territories or possessions bordering on the Caribbean Sea.

[70] Citizens of the following countries participate in the GVWP: Australia, Brunei, Indonesia, Japan, Malaysia, Nauru, New Zealand, Papua New Guinea, Singapore, Solomon Islands, South Korea, Taiwan (Applies to travel that begin in Taiwan to Guam with no layovers except in a US territory enroute AND are in possession of a Taiwan National Identity Card and a valid Taiwan passport with a valid reentry issued by the Taiwan Foreign Ministry of Foreign Affairs.

Appendix D: Select Organizations and Programs

Agriculture and Quarantine Inspection (AQI)

After a long and distinguished history in the U.S. Department of Agriculture (USDA), approximately 2,600 employees from Animal and Plant Health Inspection Service (APHIS)/Plant Protection and Quarantine (PPQ), Agriculture Quarantine and Inspection (AQI) force became part of DHS' Border and Transportation Security's Bureau of Customs and Border Protection (CBP) on March 1, 2003.

APHIS' efforts to protect American agriculture have long been the first line of defense against the introduction of foreign plant and animal pests and diseases at our Nation's Ports-of-Entry (POE). This critical mission will now be carried out by DHS. Since September 11, 2001, APHIS continues to be on heightened alert against both intentional and unintentional threats to agricultural resources. Creating a consolidated border inspection organization allows for unprecedented information sharing, streamlined services, cross training among specialists, and innovative techniques that weren't previously possible when border inspection was the responsibility of three separate agencies.

To assist DHS in this effort, APHIS/PPQ Beagle Brigade has also moved to the new department within CBP. These highly trained detector dogs sniff the baggage and vehicles of international travelers as they arrive in the United States to identify prohibited agricultural products. APHIS will maintain responsibility for training new members of the Beagle Brigade as well as their handlers. In addition, APHIS will continue to train all CBP Agriculture Specialists in the science of pest and disease detection.

While some safeguarding responsibilities have been transferred to DHS, APHIS will continue to play an important role in preserving America's agricultural resources. In this role, APHIS will work to strengthen and expand its pest detection programs as well as its partnerships with States, industry, and academic institutions. In the event of an agri–terror attack on our homeland, DHS and APHIS will work as partners to safeguard America's food and agricultural resources. DHS will lead the team of first responders to contain and manage the threat while APHIS provides crucial scientific and diagnostic expertise. This expertise will be critical in managing a potential disease outbreak as well as assisting DHS in its investigative and intelligence–gathering efforts to find those responsible for the terrorist attack. Today's world presents new threats to U.S. agriculture, and this partnership creates a stronger line of defense to protect our Nation's agricultural resources.

United State Coast Guard (USCG)

On March 1, 2003 the U.S. Coast Guard became a part of DHS. It remains intact as an organization and reports directly to the Secretary, DHS. The USCG's homeland security mission is more visible today, but it is just as important as it was when the USCG first began protecting our national sovereignty 211 years ago.

In the wake of the September 11 terrorist attacks, the USCG immediately mobilized more than 2,000 reservists in the largest homeland defense and port security operation since World War II. The USCG has increased its vigilance, readiness, and patrols to protect the country's 95,000 miles of coastline, including the Great Lakes and inland waterways.

As part of Operation Noble Eagle[71], the USCG is at a heightened state of alert protecting more than 361 ports and 95,000 miles of coastline, America's longest border. The USCG continues to play an integral role in maintaining the operations of our ports and waterways by providing a secure environment in which mariners and the American people can safely go about the business of living and working freely.

The USCG's homeland security role includes:

- Protect ports, the flow of commerce, and the marine transportation system from terrorism;
- Maintain maritime border security against illegal drugs, illegal aliens, firearms, and weapons of mass destruction;
- Ensure that we can rapidly deploy and resupply our military assets, both by keeping USCG units at a high state of readiness, and by keeping marine transportation open for the transit assets and personnel from other branches of the armed forces;
- Protect against illegal fishing and indiscriminate destruction of living marine resources, prevention and response to oil and hazardous material spills, both accidental and intentional; and
- Coordinate efforts and intelligence with federal, state, and local government agencies.

Federal Bureau of Investigations (FBI)

On July 26, 1908, then-Attorney General Charles J. Bonaparte appointed an unnamed force of Special Agents to be the investigative force of the Department of Justice. The FBI evolved from this small group.

The mission of the FBI is to uphold the law through the investigation of violations of federal criminal law; to protect the United States from foreign intelligence and terrorist activities; to

[71] Operation Noble Eagle refers to U.S. military operations associated with homeland defense and civil support to federal, state and local agencies in the United States, and includes the increased security measures taken after the September 11 terrorist attacks. The operation involves joint agency coordination and cooperation to ensure our nation and borders are protected from future attacks.

provide leadership and law enforcement assistance to federal, state, local, and international agencies; and to perform these responsibilities in a manner that is responsive to the needs of the public and is faithful to the Constitution of the United States.

September 11, 2001 terrorist attacks had a profound impact on the responsibilities of the FBI. The U.S. PATRIOT Act granted new provisions to address the threat of terrorism. The FBI was given responsibility for protecting the American people against future terrorist attacks. On May 29, 2002, Attorney General John Ashcroft issued revised investigative guidelines to assist the FBI's counter terrorism efforts.

To support the FBI's change in mission and to meet newly articulated strategic priorities, the FBI reengineered its structure and operations to closely focus on prevention of terrorist attacks, countering foreign intelligence operations against the U.S., and on addressing cyber crime-based attacks and other high-technology crimes. In addition, the FBI remains dedicated to protecting civil rights, combating public corruption, organized crime, white-collar crime, and major acts of violent crime. The FBI has also strengthened its support to federal, county, municipal, and international law enforcement partners and has dedicated itself to upgrading its technological infrastructure to successfully meet each of its priorities.

United States Border Patrol (USBP)

The USBP, established by an Act of Congress in response to increasing illegal immigration, was officially established on May 28, 1924. As mandated by this Act, the small border guard in what was then the Bureau of Immigration was reorganized into the USBP. The initial force of 450 officers was given the responsibility of combating illegal entries and the growing business of alien smuggling. Today, the USBP has approximately 10,400 agents. The USBP is the mobile uniformed law enforcement arm of DHS. In March of 2003, the USBP began a new chapter in its history by becoming part of the new CBP.

While the USBP has changed dramatically since its inception over 75 years ago, its primary mission remains unchanged: to detect and prevent the illegal entry of aliens into the U.S. There is a direct linkage between the activities of the USBP between POEs and the POEs themselves. Together with other law enforcement officers, the USBP helps maintain borders that work – facilitating the flow of legal immigration and goods while preventing the illegal trafficking of people and contraband. The USBP is specifically responsible for patrolling the 6,000 miles of Mexican and Canadian international land borders and 2,000 miles of coastal waters surrounding the Florida Peninsula and the island of Puerto Rico. Agents work around the clock on assignments, in all types of terrain and weather conditions. Agents also work in many isolated communities throughout the U.S.

All USBP agents spend 19 weeks in training at the U.S. Border Patrol Academy in Glynco, Georgia, or Charleston, South Carolina, which is a component of the Federal Law Enforcement Training Center. Agents are taught immigration law, statutory authority, police techniques, and Spanish. Upon graduation, they spend an additional 24 weeks in on-the-job training, which includes weekly intensive instruction in immigration law and Spanish.

The primary mission of the USBP is the detection and apprehension of illegal aliens and smugglers of aliens at or near the land border. This is accomplished by maintaining surveillance, following up leads, responding to electronic sensor alarms and aircraft sightings, and interpreting and following tracks. Some of the major activities include maintaining traffic checkpoints along highways leading from border areas, conducting city patrol and transportation check, and anti-smuggling investigations. Since 1994, the USBP has made more than 11.3 million apprehensions nationwide, more than the current combined populations (2000 U.S. Census data) of Iowa, Missouri, and Kansas.

The USBP also works closely with state and local law enforcement counterparts, often being the only law enforcement presence in remote areas. Special teams of USBP agents also conduct search and rescue operations in remote areas.

United States Department of State (DOS)

The Department of State manages the United States' international relations, which includes the issuance of international travel documents: passports to U.S. citizens and visas to certain foreign nationals to come to the U.S.

Passport Systems

All domestic passport agencies are equipped with the modern photo-digitized Travel Document Issuance System (TDIS-PD). All passports issued by the domestic passport agencies incorporate the use of printed digital photos and related security devices resulting in greatly improved passport security. TDIS-PD is currently being upgraded with a newer more powerful database (Microsoft's SQL) and capability to integrate with posts abroad, which will allow DOS posts to transfer data electronically for domestic issuance of overseas passport applications. The Passport Records Imaging System Management (PRISM) system permits electronic storage of high-resolution digital color images of passport applications and Consular Reports of Birth Abroad. The decentralized version of PRISM allows users to immediately retrieve electronic records within minutes of passport issuance.

A companion system, the Passport Information Electronic Retrieval System (PIERS), provides a direct electronic index to the PRISM passport application images to DOS Consular Officers and Diplomatic Security agents abroad and passport agencies and passport headquarters staff. Currently, digital color images of passport records from 1996 to the present are stored on PRISM. A back scan project to digitally image paper records of passport applications issued between 1994 and 1998 is underway. Once this project is completed, passport records including photographs will be available for all currently valid passports. DOS expects to complete the project in 2004. In addition, an index record of passport issuances back to 1978 is available.

The Passport Lookout Tracking System (PLOTS) contains an index as well as digital images of approximately 150,000 passport fraud and law enforcement lookouts, and is available worldwide to consular officers and other authorized officials.

Visa Systems

The modernized Nonimmigrant Visa (NIV) System produces a tamper-resistant, machine-readable visa that includes the applicant's photograph, and features a seamless interface with both the DOS' name check system (CLASS) and the Consular Consolidated Database (CCD). In February 2003, DOS deployed the latest release of nonimmigrant visa software with enhanced data collection (25 new data elements) and improved scanning and photo-capture features.

The latest immigrant visa software facilitates data sharing with the Social Security Administration, which is used to provide social security numbers for new immigrants. The Immigrant Visa system is under re-designed to produce an immigrant visa that includes a digitized photo and machine-readable format, which will be piloted in early 2004.

Consular Consolidated Database (CCD)

All visa system activity abroad is replicated and stored in the CCD. All consular posts abroad have access to the CCD, a global database of visa records making it possible to instantly verify U.S. visa issuance or refusal from anywhere in the world.

DOS currently shares issued visa records with DHS inspectors at all Ports-of-Entry, and subsequently with DHS field offices that have access to the Interagency Border Inspection System (IBIS). Recent upgrades to the CCD's interagency connectivity make it technically ready to share visa records, in near real-time, throughout the U.S. government.

Name checks

The Consular Lookout and Support System (CLASS) is the primary automated screening tool for consular officers issuing passports and visas, and CLASS routinely processes over 100,000 name checks daily. CLASS contains linguistic-based algorithms (Arabic, Russian/Slavic, Hispanic) used in querying its data. An Asian algorithm is in the linguistic design stage. CLASS has a database containing over 14 million visa subject lookouts and 3.6 million passport subject lookouts. In 2003, while adding eight million FBI lookouts, DOS upgraded hardware to keep response time efficient.

Biometrics

Changes in the law in regard to biometrics are having significant effects on DOS' travel document issuance. Section 303(b) of the Border Security Act stipulates that by October 26, 2004, the Secretary of State shall issue only visas that use biometric identifiers. Section 303(c) of the Border Security Act establishes certain requirements for travelers from Visa Waiver Program (VWP) countries by which they will need to have passports that incorporate biometric identifiers that comply with standards of the International Civil Aviation Organization (ICAO).

Biometric Passport

At its May 2003 meetings, ICAO adopted facial recognition as the globally interoperable biometric to facilitate machine-assisted identity confirmation at U.S. and other borders. The objective is to ensure that such passports can be "read" by similar equipment worldwide, that they are being used by the person to whom the passport was issued, and that the passport has not been altered. ICAO also provided that fingerprint and iris images could be included in the passport to supplement facial recognition as additional biometrics, at the discretion of the issuing country.

Although the Border Security Act does not specify that U.S. passports must incorporate biometric identifiers, DOS believes that biometrics stored in travel documents provide added security to the authentication of passport data and can enhance the processing and verification of identity of persons at borders. Therefore, DOS has adopted the ICAO standard for use in the U.S. passport and has assembled an interdisciplinary committee to solve the problems inherent in issuing a biometrically enabled passport, consisting of experts from the Bureau of Consular Affairs, the Department of Homeland Security, the Government Printing Office and other offices.

DOS plans to initially produce a small number of biometrically enhanced passports in fiscal year 2005, with the goal of converting the entire U.S. passport process during fiscal year 2006.

Biometric Visa

In order to meet the October 26, 2004, deadline, DOS will undertake an unprecedented global biometric enrollment program for visa applicants. The enrollment will initially be of two fingerprints plus a photograph. Visa-issuing posts in Mexico have been taking visa applicant fingerprints since 1998 for the issuance of Border Crossing Cards through a joint program with the legacy Immigration and Naturalization Service and now with the Department of Homeland Security. The Border Crossing Card program has provided valuable experience for fingerprinting of visa applicants and related issues.

Transportation Safety Administration (TSA)

The Aviation and Transportation Security Act recognized the importance of security for all forms of transportation and related infrastructure elements. This cannot be accomplished by the TSA in isolation and requires strengthened partnerships among Federal, State and local government officials, and the private sector to reduce vulnerabilities and adopt the best practices in use today.

On February 17, 2002, TSA assumed the aviation security screening responsibilities previously performed by the airlines' for over 30 years and is responsible for day-to-day Federal security screening operations for passenger air transportation and intrastate air transportation. This includes: the non-intrusive and if warranted intrusive screening of airport passengers, their luggage, airport employees, and all others needing to pass through security checkpoints.

Infrastructure protection of critical assets such as pipelines and more than 10,000 Federal Aviation Administration facilities is another key mission of the TSA. Along with rail and highway bridges, many other national assets are critical to our economic and national security and vital for the free and seamless movement of passengers and goods throughout the country.

The U.S. transportation system is vast, enabling the free movement of millions of passengers each day. The system includes:

- More than 367 maritime ports, 1,000 commuter rail stations, 429 federalized airports and 600 central bus stations;
- Over 130 million passengers who commute by ferry, and more than six million passengers who take overnight cruise line voyages;
- More than 23 million passengers who ride on Amtrak trains, 61 million passengers who ride on local commuter rails, and over 85 million passengers who ride the Long Island Railroad; and
- An estimated 860 million passengers who ride on over 44,000 over-the-road motor coaches and inner city buses each year.

Canine Units

The Canine programs of legacy U.S. Customs, INS, Agricultural Quarantine Inspection, and the U.S. Border Patrol are now part of CBP. The primary mission of the Canine Units is to detect and prevent terrorists and terrorist weapons from entering the U.S. Legacy U.S. Customs, Agriculture, and INS canine units are deployed within the POE while the U.S. Border Patrol canines are deployed between POEs.

Program Background of Canine Units

The legacy USCS has approximately 700 Canine Enforcement Officers (CEO) including officers in training. 571 CEOs with a detector dog are stationed at 73 POEs to include Hawaii and Puerto Rico, as well as two pre-clearance stations. This total includes 16 anti-terrorism teams (10 explosive teams at 5 locations and 6chemical teams at 3 locations). The current journeyman grade for all CEOs is GS-11. The Canine Enforcement Training Center (CETC) is located in Front Royal, Virginia, and has a capacity of training 180 teams annually with a staff of 40. The average length of the training course is 13 weeks.

The USBP has approximately 334 Border Patrol Agents with a detector dog with an additional 108 teams to be trained in fiscal year 2003. These agents are assigned to 69 stations (includes northern/southern borders & coastal stations). The current journeyman grade is GS-11. The Border Patrol National Canine Facility (NCF) is located in El Paso, TX, and has a capacity of training 120 canine teams with a current staff of nine. The average length of the training course is 11 weeks, with all detector dogs being trained to detect concealed humans and narcotics.

The Inspections Program of legacy INS has 36 canine teams assigned to 15 locations with an additional 15 new inspectors being trained in fiscal year 2003. Legacy INS detector dogs and canine inspectors are also trained at the USBP NCF in El Paso, TX. The legacy INS canine program mission is enhancing their law enforcement efforts to detect concealed humans, as

well as narcotics. The canine budget remains at the headquarters level and is estimated at $866,000 for fiscal year 2003. This budget is for the training of 15 new inspector teams and 5 replacement detector dogs. The canine program's policies and procedures are the same as USBP's.

The Animal & Plant Health Inspection Service (APHIS) has 139 approved Plant Protection & Quarantine (PPQ) Canine Office positions. The current journeyman grade is GS-9. Seventy five detector dog teams are currently deployed at POEs, 38 teams are waiting to be trained at National Detector Dog Training Center (NDDTC) and 26 canine officer vacancies were transferred to DHS. These officers are assigned to select international airports, land borders, mail facilities and cargo areas throughout the U.S. The APHIS Detector Dog program averages about 85,000 seizures of prohibited agricultural products a year. APHIS dogs are housed at USDA approved kennels which meet stringent guidelines. Dogs are procured from "shelters," "rescue groups" and "private donations." APHIS dogs are retired at nine years of age.

All APHIS canine officers are qualified as PPQ Officers (Biology degree or 24 related course credits) and receive New Officer Training (NOT) in Frederick, MD, prior to their canine training. The APHIS NDDTC is located in Orlando, Florida. The NDDTC has a current staff of 12; instructors have degrees or extensive training in detection work and animal behavior. The NDDTC's operating budget for fiscal year 2002 was $1.5 million, which includes all leasing of three facilities. The average length of the training course is 10 weeks with all the detector dogs being trained on 5 basic odors. Additional odors are introduced for detector dogs working in specific ports. Some dogs have been known to recognize nearly fifty odors during their six to nine year careers. The training center conducts 10 scheduled classes of 4 students per class annually (40 teams). They also conduct approximately 10 replacement classes per year.

Appendix E: Acronyms

ACRONYM	DESCRIPTION
AAPA	American Association of Port Authorities
ABI	Automated Broker Interface
ACI-NA	Airports Council International—North America
ACE	Automated Commercial Environment
ACS	Automated Commercial System
ADIS	Arrival Departure Information System
AES	Automated Export System
AIS	Automatic Identification System
AmChams	American Chambers of Commerce
AMO	Air and Marine Operations
AMS	Automated Manifest System
APHIS	Animal and Plant Health Inspection Service
API	Advance Passenger Information
APIS	Advance Passenger Information System
AQI	Agriculture Quarantine Inspection
ARS	Pre-Arrival Review System
ASAC	Aviation Security Advisory Committee
ATR	Airport Technical Requirements
ATSA	Aviation Transportation and Security Act of 2001
BCS	Border Cargo Selectivity
BLM	Border Liaison Mechanism
BOTA	Bridge of the Americas
BSA	Enhanced Border Security and Visa Entry Reform Act
BSPC	Border Station Partnership Council
BRASS	Border Release Advanced Selectivity System
BTS	Border and Transportation Security
CADD	Computer Aided Design and Development
CANACAR	Camara Nacional del Autotransporte de Carga
Can/Am BTA	Canadian/American Border Trade Alliance
CBP	U.S. Customs and Border Protection
CCD	Consular Consolidated Database
CEO	Canine Enforcement Officer
CETC	Canine Enforcement Training Center
CHCP	Cargo Handling Cooperative Program
CL	Computational Linguistics
CLAIMS	Computer-Linked Application Information Management System
CLASS	Consular Lookout and Support System
CLIA	Cruise Lines International Association
COAC	Commercial Operations Advisory Committee
CODIS	Combined DNA Index System
COTS	Commercial-Off-The-Shelf

ACRONYM	DESCRIPTION
CSA	Customs Self-Assessment
CSI	Container Security Initiative
CTA	Canadian Trucking Alliance
C-TPAT	Customs-Trade Partnership Against Terrorism
CVPC	Commercial Vehicle Processing Center
DCL	Dedicated Commuter Lane
DHS	Department of Homeland Security
DIHS	Division of Immigration Health Services
DMIA	INS Data Management Improvement Act of 2000
DNA	Deoxyribonucleic Acid
DOC	U.S. Department of Commerce
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
DOT	U.S. Department of Transportation
DSV	Dynamic Signature Verification
EID	Enforcement Integrated Database
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FAMS	Federal Air Marshal Service
FAST	Free and Secure Trade
FBI	Federal Bureau of Investigation
FCCA	Florida-Caribbean Cruise Association
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FIRST	Frequent Importer Release System
FIS	Federal Inspection Services
FLETC	Federal Law Enforcement Training Center
FPS	Federal Protective Service
FROB	Freight Remaining on Board
GSA	General Services Administration
GIS	Geographic Information System
GPS	Global Positioning System
HRSA	Health Resources and Services Administration
IAFIS	Integrated Automated Fingerprint Identification System
IATA/CAWG	International Air Transport Association/Control Authorities Working Group
IBET/IMET	Integrated Border and Marine Enforcement Teams
IBIS	Interagency Border Inspection System
ICAO	International Civil Aviation Organization
ICCL	International Council of Cruise Lines
ICE	Bureau of U.S. Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
IFTWG	Intermodal Freight Technology Working Group

ACRONYM	DESCRIPTION
IIRIRA	Illegal Immigration Reform and Immigrant Responsibility Act of 1996
IMO	International Maritime Organization
IMTC	International Mobility and Trade Corridor Project
INA	Immigration and Nationality Act
INS	Immigration and Naturalization Service
INSPASS	INS Passenger Accelerated Service System
IP	Internet Protocol
ISIS	Integrated Surveillance Intelligence Systems
ISPS	International Ship and Port Facility Security
IT	Information Technology
ITDS	International Trade Data System
ITI	International-to-International
ITS	Intelligent Transportation System
IV	Immigrant Visa
JACC	Joint Agency Coordination Center
JCN	Justice Consolidated Network
JOCC	Joint Operation Control Center
JPAU	Joint Passenger Analysis Unit
JWC	Joint Working Committee
LANL	Los Alamos National Laboratories
LESC	Law Enforcement Support Center
MIA	Miami International Airport
MTSA	Maritime Transportation Security Act
MOU	Memorandum of Understanding
NAFTA	North American Free Trade Agreement
NATAP	North American Trade Automation Prototype
NAILS	National Automated Immigration Lookout System
NATO	North Atlantic Treaty Organization
NCAP	National Customs Automation Prototype
NCF	National Canine Facility
NCIC	National Crime Information Center
NDDTC	National Detector Dog Training Center
NIIS	Non-Immigrant Information System
NISC	National Infrastructure Security Committee
NIV	Non-Immigrant Visa
NNSA	National Nuclear Security Administration
NOT	New Officer Training
NSEERS	National Security Entry/Exit Registration System
NVOCC	Non-Vessel Operating Common Carriers
NWCA	North West Cruiseship Association
OSC	Operation Safe Commerce
PAPS	Pre-Arrival Processing System
PAU	Passenger Analysis Unit

ACRONYM	DESCRIPTION
PIERS	Passport Information Electronic Retrieval System
PIL	Primary Inspection Lane
PIP	Partners in Protection (Canadian Program)
PLOTS	Passport Lookout Tracking System
POE	Port of Entry
POLA	Port of Los Angeles
PPQ	Plant Protection and Quarantine
PSAP	Public Safety Answering Point
RCCL	Royal Caribbean Cruise Lines
RCMP	Royal Canadian Mounted Police
RNS	Release Notification System
RVS	Remote Video Surveillance
SCS	Sterile Corridor System
SCT	Mexican Secretariat of Communications and Transportation
SDE	Surveillance Decision Environment
SENTRI	Secure Electronic Network for Travelers Rapid Inspection
TBWG	Trans Border Working Group
TDIS-PD	Travel Document Issuance System-Photo Digitized
TEA-21	Transportation Equity Act for the 21st Century
TECS	Treasury Enforcement Communications System
TIA	Travel Industry of America
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Card
TWOV	Transit Without Visa
UCD	User-Centered Design
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
USBP	U.S. Border Patrol
USCG	U.S. Coast Guard
USCS	U.S. Customs Service
USDA	U.S. Department of Agriculture
USPHS	U.S. Public Health Service
US-VISIT	The United States Visitor and Immigrant Status Indicator Technology
VACIS	Vehicle and Cargo Inspection System
VWP	Visa Waiver Program
VWPPA	Visa Waiver Permanent Program Act
WAM	Workforce Analysis Model

Appendix F: IT Report Summary

The DMIA Task Force contracted with independent information technology (IT) consultants to provide a full report outlining how the automated systems currently function in relation to the border management processes and recommendations for a future border management system. The full report also outlines recommended enhancements to current systems that address the various needs of DHS and other relevant agencies and organizations.

Due to the sensitive nature of the information and findings in the full IT report, an IT Report Summary is included as an Appendix in this report. As necessary, the Task Force will brief appropriate officials on the complete IT findings.

INFORMATION TECHNOLOGY CONSULTANT ANALYSIS SUMMARY REPORT 2003

LA-UR-03-7940

Prepared by

Jorge H. Roman
Paula N. Morgan
Diane M. Gonzales
Teresa L. Roberts
Terry M. Helm
Robert Y. Parker
Randy E. Michelsen
Benny J. Martinez

Los Alamos National Laboratory

Abstract

The initial section of this report provides a brief background summary and describes the scope of the subject project. General descriptions of Information Technology systems follow. The next portion explains the evaluation methodology of existing Information Technology systems. This section closes with observations and findings of the analysis including recommendations for improving current implementations.

The second section of this report addresses a conceptualized Information Technology system. It begins with a generic description of traveler and cargo components including possible areas of additional functionality. Detailed discussions of the applications of biometric technologies follow. The next discussion focuses on emerging technologies applicable to future Information Technology system functionality. This section of the report closes with recommendations relative to future Border Management Information Technology systems.

Finally, the summary report offers some overall conclusions.

Section 1: Evaluation of Current Information Technology Systems

Introduction

The Immigration and Naturalization Service Data Management Improvement Act (DMIA) of 2000 created a Task Force to evaluate and make recommendations on how to improve the flow of traffic at United States (U.S.) airports, seaports, and land border Ports-of-Entry (POEs) while enhancing security. Statutory mandates include evaluations and recommendations on an electronic entry/exit system; enhancing information technology (IT) systems and data collection/sharing; facilities and infrastructure issues; and increasing cooperation between public and private sectors, among federal and state/local governments, and with affected foreign governments.

Federal agencies responsible for border enforcement, protection, and inspection at over 300 POEs are now a part of the new Department of Homeland Security (DHS). The DHS came into existence as an official cabinet-level department on January 24, 2003, and now includes legacy Immigration and Naturalization Services (INS), legacy U.S. Customs (USCS), U.S. Coast Guard (USCG), the Transportation Security Administration (TSA), and about 18 other federal agencies. Both the legacy INS and legacy USCS are now divided among the border, interior, and services functions within DHS—Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and Citizenship and Immigrations Services (CIS). During 2003, the Los Alamos technical team (referred to in this report as the team) looked at the border management responsibilities, from an IT perspective, of these and other federal government entities with a role in border management, including the Department of Justice (DOJ) and the Department of State (DOS).

This report analyzes border management functions and related efforts. The systems the report covers include both those that the DMIA Task Force identified in 2002 and those that the team identified during the 2003 reporting period. The team expanded the scope of effort to include additional agencies, bureaus, and systems for a broader assessment of the current border management systems. The team's goal during this reporting period was to research each of these systems to make high-level recommendations on the better use of technology.

The team based its observations in this report on what it has seen, read about, and reviewed. (Some of these observations are unique to a single system, and others apply to border management systems as a whole.) The team developed a set of questions designed to elicit the facts about each system. Team members conducted several different types of interviews, read written documentation about the systems, conducted Web searches, and went on fact-finding site visits to POEs and other locations to see demonstrations of the systems in operation.

The team analyzed the IT systems in each border management functional category using seven factors:

1. Purpose—why does the system exist and what does it do?
2. Feasibility—is the functionality needed?
3. Technological Obsolescence[1]—extensibility, maintenance burden, accessibility.
4. Interface—intercommunications with other systems.
5. Integration—knowledge integration.
6. Overlapped—functional duplication.
7. Biometrics—robustness hierarchy.

These factors support the report's IT recommendations and conclusions for border management and focus on the security impact of each system. In a layered approach, a system's time relationship to protecting the borders determines its security impact; that is, the closer the system is to preventing an unwanted event, the greater the impact. Critical systems are in the final protective ring of border management.

Scope

This report concentrates on the technical analysis of the aggregated systems and attempts to relate them to the border management systems studied in 2002 as well as to incorporate the new areas of study mentioned above. It examines IT systems and related efforts such as enterprise architecture, infrastructure planning efforts, implementation projects, and agreements and standards.

The team's recommendations focus on interfaces among the various systems and the processes that encompass the border management domain (Figure 1):

TSA—Transportation workers identification and infrastructure security at POEs
U.S. Coast Guard—Commercial vessels
Legacy U.S. Customs—Cargo systems/travelers
Legacy Immigration and Naturalization Service Functions—Travelers
Department of State functions—Consular Affairs/visa issuance and documents
Department of Justice, Federal Bureau of Investigation (FBI)—Criminal records

[1] For an explanation of the term technological obsolescence, please see page 9.

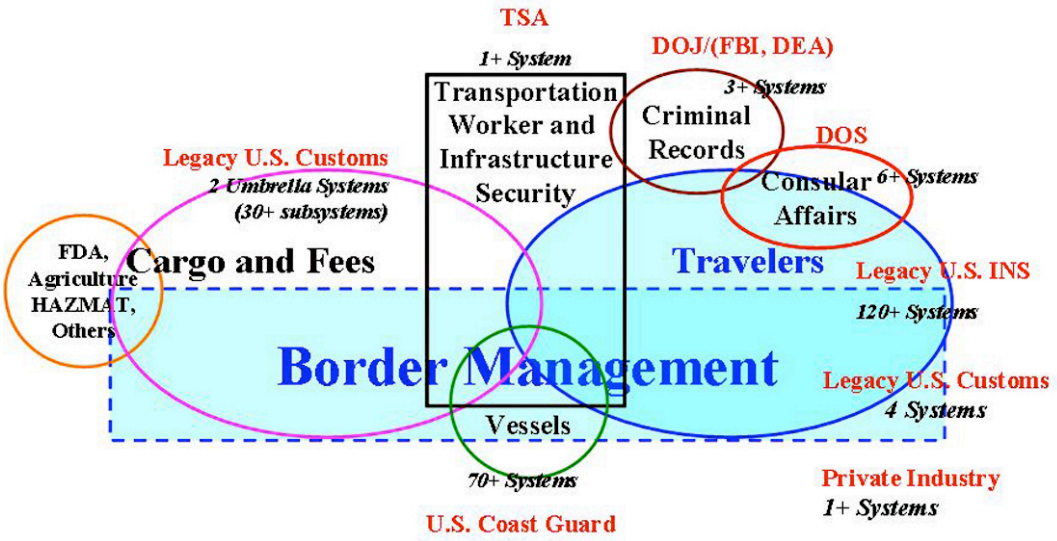


Figure 1. Border management domain.

In 2003, the report's scope has grown to cover this entire range of border management functions. The key players in border management are DHS (with the bulk of these functions), DOJ, and DOS. DHS has several overlapping components that make it necessary for IT systems to interoperate. IT systems in other departments also need to interoperate at a lesser extent.

Under DHS, key border management components are cargo systems, traveler systems, commercial vessels, and transportation workers and infrastructure security.

- Cargo systems deal with the import of cargo to and export of cargo from the U.S.; they manage the physical and financial compliance with the law, as well as mitigating the threats these activities might create. The technical team reviewed two umbrella IT systems and two subsystems.
- Travelers, foreign as well as U.S. citizens, cross the borders of the U.S. The entry and exit of certain foreign individuals merit particular interest. In addition, managing the visits of foreign travelers from the time they request permission to enter and their arrival and subsequent departure from the country is important. Of the 120+ legacy INS systems, the team reviewed 29. In addition, the team reviewed two legacy USCS systems and one private industry system related to travelers.
- The USCG monitors commercial vessels on the waterways. These vessels carry cargo or passengers and may include foreign crewmembers. USCG is the first to physically encounter a vessel before it arrives at a POE. The team reviewed three of the USCG systems.
- Transportation workers and infrastructure security are key concerns especially at POEs because they provide the lifeline for commerce and commercial exchanges that support the economy of this country. The TSA has at least one significant IT effort in the planning stages and one system that was not reviewed in great detail but has a significant role.

Other departments also play important roles in border management.

- DOS' Consular Affairs Offices are the first point of contact for many foreign travelers and issue visas that allow many to board for an inbound trip to the U.S. They can also screen out those ineligible to enter the U.S. The team has reviewed six systems in support of Consular Affairs and visa issuance operations.
- The DOJ FBI's criminal record information provides key information enabling quick identification of individuals with criminal records either by name or by fingerprints. This function also supports background investigations for transportation workers and others. Two systems play a significant role in providing access to this information, and the team reviewed them. The matrix referenced below also lists a third system that the team did not review in depth.

Overall, these entities might use more than 200 systems, so the team has concentrated on the key border management systems to narrow the scope of the report to a manageable set. The key systems for the above components amount to 50 individual systems. Refer to page 33 for a complete matrix of systems reviewed.

Many laws and policies dictate and regulate how the DHS and its border management agencies and bureaus operate and how system requirements are prioritized. It is worth noting that, although the roles of the agencies and bureaus in the new department have been revised, the applicable laws have not been changed at this time. The new agencies and bureaus are still expected to satisfy the old laws and mandates, which are not well aligned with the new department.

Border Management Systems by Department and Bureau

- *Department of State*

  The core applications are built using Power Builder and with Oracle as the database. The application is in a distributed environment. Every post around the world has similar functions and needs access to centralized information. The current implementation relies on Oracle's replication capability and Power Builder's distributed application environment. The software's distributed copies allow for synchronized update of software.

  The database has replication capabilities that allow the mirroring of changes from a local subset to a centralized location, allowing posts to work on their local subset (for efficiency and other advantages) but constantly replicating all changes to the central database, which acts as a data warehouse, collecting data replicated from every post. Posts have access through the central database to data from any other post. Access control procedures are in place.

  Recently, DOS has begun making data from the central database available through Web-based clients so users can reach the server with a Web browser. DOS can also

export its entire data set using the Oracle replication capability. This is a way to share information on a routine basis with users outside of DOS. Additionally, this ability would be ideal for DMIA mining applications.

- *Legacy USCS (DHS)*

  The core systems are large mainframe-based applications. Two large umbrella systems dominate the applications. Both of these applications are a collection of COBOL programs and scripts and associated tables in databases. Collections of these programs, scripts, and tables can be envisioned as named applications. Together, they logically implement some set of business rules. The interface is mainly character-driven screens with heavy use of function keys to provide quick shortcuts to routine operations.

- *U.S. Coast Guard (DHS)*

  Two of the applications rely on the Microsoft implementation development tools and runtime environment. The other application on the secure domain is a Unix-based application soon to be reengineered. Each application has its own database. Both open Microsoft applications can easily share information because of the common tool set.

- *DOJ/FBI (DOJ)*

  The two applications reviewed are unique and complex. Each has its own environment, interfaces, and database engine. They employ commercial platforms with customized applications.

- *Legacy INS (DHS)*

  Most applications are standalone design and use a different tool set, hardware, and software suite. They range from database with character-based screen interfaces to relational databases with Web-based interfaces.

As-Is Systems Evaluation

The specific performance areas of border management information systems of interest to the DMIA Task Force include

Purpose—Clear outline of the purpose(s) for each individual system.
Interface—How, or if, it interfaces with other systems in use.
Project/Feasibility of Continued Use—Determine the prospect of continued use for each individual system in the context of overall border management systems.
Duplication/Overlapping—Identify duplicate or overlapping functions or responsibilities among the systems.
Technological Obsolescence[1]—Determine which systems currently are or will soon be obsolete.

[1] See page 9 for a complete explanation of the term technological obsolescence.

Integration—(a) Determine which systems are integrated (either fully or partially) and (b) determine which systems could be modified or enhanced and ultimately could become integrated.
Biometrics—(a) Determine which systems currently employ biometrics and (b) determine which systems could employ biometrics.

The evaluation characteristics outlined above touch on important and consequential issues of effective border management operations. The fundamental goals of border management systems are to eliminate the possibilities of activities, persons, equipment, and/or materials breeching U.S. borders with the intent to do grave harm, to facilitate the flow of legitimate enterprise activities, while protecting the privacy of the individual(s). The team assessed each system selected for evaluation in light of this goal—knowing the stated purpose of the system and understanding the significance of its purpose relative to the overall border management goals.

Purpose

The team has identified 50 individual systems to evaluate by the performance characteristics summarized above. A purpose-based categorization helps to better organize a detailed assessment of such a large number of systems. The 50 systems fall naturally into

Eight specific categories representing the general purpose they serve in the traveler system:

- Identification—Systems that assist in determining the identity of persons.
- Inspections—Inspection systems help accurately verify the identity of persons wishing to enter the country.
- Enforcement—Systems that provide case handling for violations of U.S. law by foreign nationals.
- Benefits—Systems that track and maintain the length-of-stay authorized for nonimmigrants.
- Intelligence—For the purposes of this report, systems that analyze information, often drawing and assembling “lookout” records that would result in more detailed inspection.
- Decision Support—Systems that provide analysis from enterprise data.
- Cargo—Systems that process data for the import of cargo/goods and the liquidation of import duties.
- U.S. Coast Guard—Systems that monitor commercial vessels and USCG operations.

Eight specific categories representing the general purpose they serve in the cargo system:

- Entity ID—Systems that support and maintain the creation of electronic identification of organizations and other entities associated with cargo importation.
- Inspection/Examination—Systems that support the inspection/examination process of cargo.
- Enforcement—Systems that deal with case management when laws have been violated while importing cargo through the border.
- Release—Systems that handle the information associated with the release of cargo once it has been inspected/examined.
- Liquidation—Systems that deal with the transactions for the liquidation or payment of import duties.
- Shipment Management—Systems that allow the preparation of all required documentation to import cargo.
- Intelligence (Targeting systems)—For the purposes of this report, systems that analyze patterns and trends to identify cargo requiring more detailed inspection.
- Decision Support—Systems that provide analysis from enterprise data.

Interface

The systems evaluated show a wide range of interrelationships. For example, a criminal history information system shares information with a number of agencies including the FBI, various criminal justice agencies, and appropriate courts. Entry/exit information from the inspection operations is subsequently transferred to an enforcement system, a decision support system, a benefits system, another intelligence system, and an identification system.

Prospect/Feasibility of Continued Use

The team used the design and software implementation of each system to evaluate feasibility of continued use. Exceptional design enables systems to accommodate changes and enhancements and incorporates industry standard technologies. Four systems are noted for their ***exceptional*** design, software implementation, and overall usability. If two specific systems receive software upgrades, they could be reasonable candidates for continued use. Updating this software to a more modern operating system would be reasonably straightforward.

Some of the system managers the team interviewed spoke of plans to upgrade and enhance system performance capabilities. It is assumed that timely improvements will be made to these systems as scheduled.

Duplication/Overlapping

Duplication and/or overlapping characteristics imply that certain systems serve the same purpose, replicate certain functionalities, or have been replaced with other capable systems. It is not surprising that a number of these systems are considered obsolete. It is reasonable to expect that the functionality of obsolete systems has migrated to other, more modern systems and, therefore, overlap with them.

Some identification systems and some lookout databases appear to have a natural clustering of overlaps. It is likely that their functionality is better served by integrating them. Two systems have a closely shared relationship, suggesting consolidation of these two systems should be investigated.

Technological Obsolescence

Comparing the "modernness" of a system's technology with current, best practice determines whether the system is obsolete. Because certain systems are deemed technologically obsolete does not mean that they should be quickly removed from service, that they are less than adequate, or that they are "pitifully weak" systems; they can still provide fully satisfactory information. However, upgrading, enhancing, or replacing technologically obsolete systems is part of the routine course of responsible system stewardship.

The team considered systems **technologically obsolete** if the hardware supporting the system is no longer routinely maintained by private industry and/or the operating system has been generally replaced by more comprehensive capabilities. The **implementation** of a system is **obsolete** if the model of the procedures and data does not accommodate changes and enhancements. For example, if the implementation of a system does not permit the straightforward addition of normal business rules, then the system is deemed obsolete.

The majority of systems the team judged obsolete have platform deficiencies. However, two systems are uniquely obsolete in both implementation and platform. Because modern capabilities have replaced a number of these systems, it may be prudent to develop a plan for removing/replacing these systems in an orderly fashion. The systems considered "partially" obsolete merit immediate upgrading.

Integration

Integration means that the systems function together in a unified manner to accomplish the objectives of border management activities. The team determined the system integration characteristics of each system based on generally good business practices, overall security requirements, and unified system performance expectations.

Of the currently **integrated** systems, three have the potential for limited integration in the future. All of the other currently integrated systems can be incrementally integrated as required for the near future. Only two of the systems currently partially integrated offer the

potential for a more comprehensive level of integration. Five of the minimally integrated systems can be integrated well beyond their current status. It may be possible to more fully integrate two of the systems that are not currently integrated.

Biometrics

Biometrics is the automated method of identifying or authenticating the identity of living persons based on physiological or behavioral characteristics. Biometrics includes facial photographs, fingerprints, hand geometry, voice recognition, and many other unique human identifiers. Many systems could include more extensive biometric information.

The biometric information most of the systems use includes photographs and fingerprints. All of these systems have significant potential for greatly expanded biometric identifiers. Although the advantages of multiple biometric information sets have not been rigorously quantified, it appears that biometric diversity will enhance the quality of person identification and/or validation systems.

Observations

Observation 1. **Transfer/exchange diversity limits information quality.**

The wide range of data transfer connections could seriously hamper the timeliness and availability of critical information to the relevant systems. The potential propagation of errors, the variations of definitions among the systems, the limitations imposed by law, the differing system priorities, and the lack of centralized oversight help create this limitation.

Observation 2. **As anticipated, essentially all of the systems examined manage/manipulate information.**

With few exceptions, the systems of interest do indeed acquire, maintain, and post large amounts of information. The fundamental technology by which information management is accomplished differs little with the various systems. Most are built upon linear data construction techniques together with “keyword” searchable file structures.

Observation 3. **Obsolete systems are notably populated by overlaps and duplications.**

The majority of systems determined to be obsolete also have overlapping or duplicative operational capabilities. This implies that system overlaps are at least partially attributable to unmitigated obsolescence. Experience has shown that system-wide inefficiencies are more likely to occur if effective modernization strategies are not routinely implemented.

Observation 4. **Most systems are obsolete because of platform problems.**

Almost without exception, technologically obsolete systems use outdated technologies (mainframe computational systems). The likely consequences of obsolescence may include significant maintenance costs, extremely limited interoperability, and little, if any, adaptability.

Observation 5. **Most systems are or readily could be integrated.**

Over 80% of the systems the team evaluated were at least "minimally" integrated, and, almost without exception, system-by-system implementation technologies do not prevent integration. This is very good news. However, domain-wide "functional integration" should be evaluated because it is much more consequential than individual "system-by-system integration."

Observation 6. **Biometric identifiers have been implemented across a broad range of appropriate applications. Most systems are designed to accept biometrics in a reasonably straightforward manner.**

The team found no glaring deficiencies relative to the use of biometric identifiers. Most of the systems have the obvious opportunity to enhance the use of biometrics to improve the quality of person identification results.

Observation 7. **The efficacy of the information ultimately posted by each individual system is inseparably coupled to the quality of the data resident in the system's data sources.**

Successfully applying the information management capabilities in this report ultimately depends on the accuracy, completeness, timeliness, and relevance of the source data upon which these capabilities are built.

Observation 8. **Four systems have exceptional design, software implementation, and overall usability.**

These systems clearly represent exceptional information technology implementation. These systems should form the core element from which to derive evolving information systems to meet the demands of the future.

Observation 9. **Modern communication technologies have not been fully exploited by any of the border management systems.**

Modern information technologies have developed remarkably diverse and useful techniques for communicating complex information to people (digitized voice transmissions, animations, graphics, tabulations, iconic representations, multidimensional virtual environments, three-dimensional engineering plots, geographically correct simulations, site-specific GPS-connected locators, etc.). The end user can select the communication environment(s) that works best for his/her situation.

Observation 10. **Robust information technologies depend on robust infrastructures for successful implementation.**

The current support infrastructure is not sufficiently robust to sustain broad information technology deployment. It does have, however, specific, localized elements that are somewhat adequate. Infrastructure elements include high-speed, high-capacity transmission systems (satellites), workstations, data storage and access systems, ergonomically compliant communication hardware, information input/output systems, and security-compliant encryption systems.

Observation 11. **Technological obsolescence is not a small problem: one-third of the systems have notable technology and/or design modernization challenges.**

Information systems that become technologically obsolete are not necessarily useless or unsatisfactory. Operational systems that are obsolete reflect as much on the attitude and style of the organizational support managers as on the system itself. Getting along with "old" technology is risky. Old systems tend to be well suited for operational conditions that no longer exist. Old systems are not likely to be prepared for surprise situations, emergencies, or rapidly changing national priorities. One-of-a-kind technologies are very costly (more than just dollars) to repair, maintain, and, ultimately, to replace.

Recommendations

Recommendation 1—**Personal privacy information must be rigorously protected.**

It is essential to the ultimate successful implementation of modern IT systems that the privacy of personal information and other associated information be scrupulously protected from unauthorized access, use, disclosure, or manipulation. Modern access control technologies together with administrative controls should be used to ensure that privacy laws, regulations, and public trust expectations are fully met.

Recommendation 2—**Consistent with privacy considerations, address the security advantages of understanding the consequences of persons' and organizations' long-term behavior.**

To realize the full benefits of modern information technologies, it is absolutely essential to (a) track and assess person activity patterns over relatively long periods (>25 years), (b) recognize and understand person-by-person behavior patterns, and (c) track person-to-person linkages, contacts, and often subtle interrelationships.

Recommendation 3—**Determine the security implications of interagency integration schemes.**

The team determined the integration condition of the systems in this report based solely on the individual systems. Domain-wide integration across many agencies and organizations has the greatest security value to border management operations.

Recommendation 4—**Rigorously assess the value of multiple biometric measures.**

It is not clear that multiple biometric benchmarks actually improve person identification, detection, and/or validation. Rigorous analyses should be conducted before making a national commitment to large-scale, domain-wide biometric deployments.

Recommendation 5—**Proactively avoid systematic technical obsolescence.**

Planning that includes the routine assessment, justification, and the ultimate **timely** upgrade (or removal) of key information systems should be an integral part of all operational activities, funding strategies, and organizational responsibilities associated with homeland security assignments.

Recommendation 6—**Ensure the quality of the data that supports database systems.**

The value of information is inseparably coupled to the legitimacy of the data from which the information is extracted. The quality of the data sources supporting the information technologies must be managed in partnership with border management system improvements.

Recommendation 7—**Streamline access to information.**

Access to relevant information in a timely fashion is an essential element of border protection operations. Systems providing the necessary information should avoid complex interconnections and the current excessively diverse data sources. Deploying modern communication technologies will enhance information clarity to all front line decision makers such as USBP agents and CBP officers.

Recommendation 8—**Ensure "new" systems are designed to easily accommodate change.**

The development of a national strategy for applying modern information technologies to border management issues is an essential part of achieving national security objectives. It is anticipated that "new" data systems, applications, and other tools will be deployed as an integrated approach to border management activities in the future. Every effort should be made to assure that "new" systems are designed with change in mind. For example, the business rules and/or processes that determine how to accomplish entry should not be hard-coded into new or upgraded information technology tools.

Section 2: A Future Border Management Domain

The Border Management Domain Today

Travelers

The process for travelers occurs in a step fashion. (In this report, traveler refers to individuals who enter or leave the U.S. at a POE; travelers can be U.S. citizens or foreign nationals.)

- Most foreign travelers get a visa to travel to the U.S. (Citizens of countries in the Visa Waiver Program do not need a visa for most visits less than 90 days.)
- The traveler embarks on an inbound trip on a commercial carrier to the U.S. (Air commercial carriers, by law, must provide Advance Passenger Information [API] when they depart from an overseas port.)
- The traveler arrives at a POE. A CBP officer examines travelers and their documentation. The CBP officer then records the type of admission and length of stay authorized for this visit for foreign travelers. (U.S. citizens are examined to establish citizenship and allowed to proceed, unless customs or agriculture issues arise).
- A foreign traveler might require benefits or other visit management functions while in the U.S., such as reporting a change of address or change of status.
- The foreign traveler departs in a timely fashion. (Those who do not depart, however, create various other challenges.)

The step process is probably very similar for most travelers in the overall concept except cases that require special handling, for example:

- Individuals from certain countries must be registered and their biometrics captured. These individuals must also report their departure—a more strictly controlled process than for the rest of the foreign travelers.

- Another special case occurs when someone attempts to enter the country illegally, many at POEs, but most between POEs. The process for these individuals is not the same as that of legal visitors and may involve returning them to their country of origin.

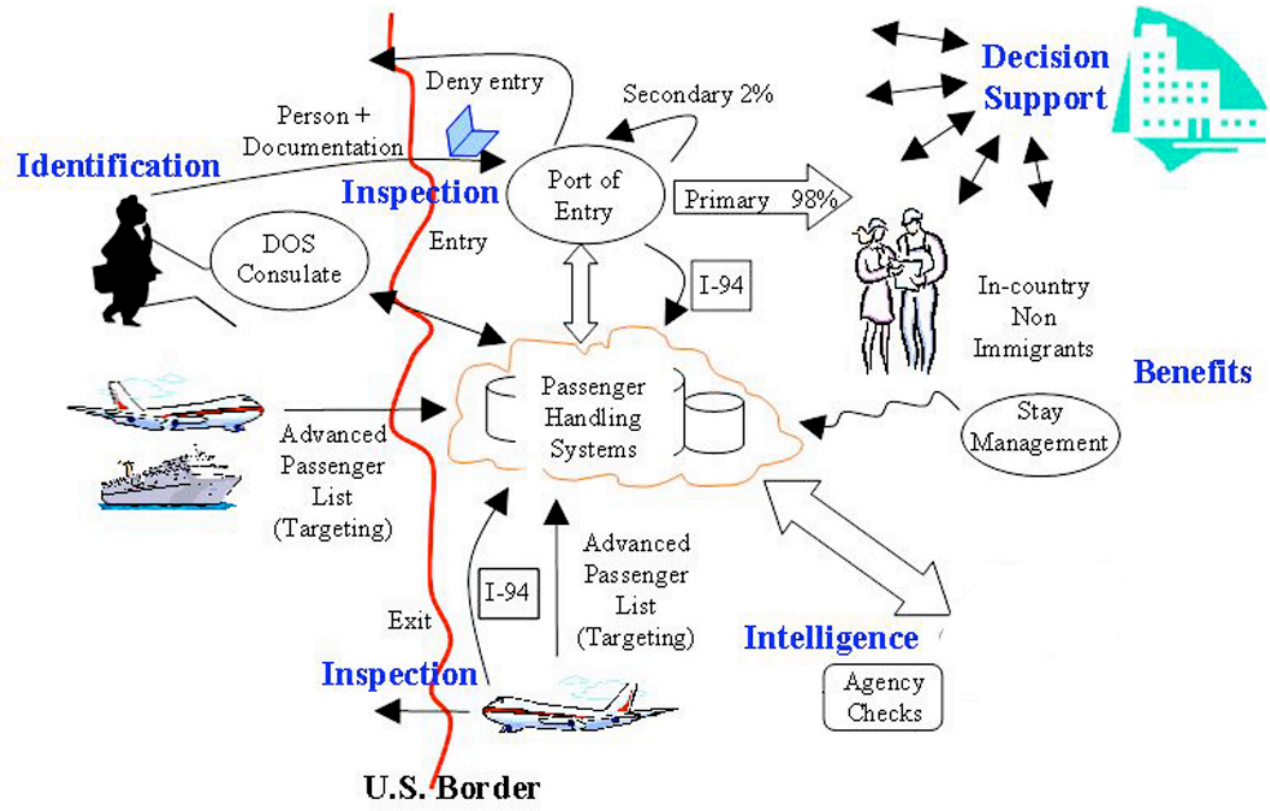


Figure 2. The traveler functional area.

Each of these steps might require a specific set of functions.

- The *identification* function creates a unique electronic identity for the individual and usually generates some kind of documentation. The visa issuance step performs an identification function. A similar function also happens when a U.S. citizen enrolls in a dedicated commuter lane program or when the U.S. Border Patrol captures an illegal alien between the POEs or at a foreign port and enters information about the illegal alien in their tracking system for future reference.

- *Enforcement* functions take place not only between POEs, they can also happen at a POE when an individual presents fraudulent documentation. Such individuals have most likely broken the law and may be removed from the country.

- The *inspection* function is similar—trying to verify the identity of an individual and presenting documents—no matter where it occurs. POEs must have a way to register the inspection event for foreign travelers to enable later visit compliance adjudication.

- The *benefits* function encompasses services such as petitioning for a student visa, adjustment of status, extension of stay, and naturalization of a foreign national.

- The *intelligence* function, for the purposes of this report, analyzes information behind the scenes, often creating “lookout” records that would result in more detailed inspection.

- The *decision support* function provides access to information from all sources while protecting privacy and controlling other access to everything collected in the process. Decision support can also sanitize the data for general reporting requirements or planning purposes.

The team derived a high-level conceptual system, as depicted in Figure 3, from the analysis of the current traveler domain.

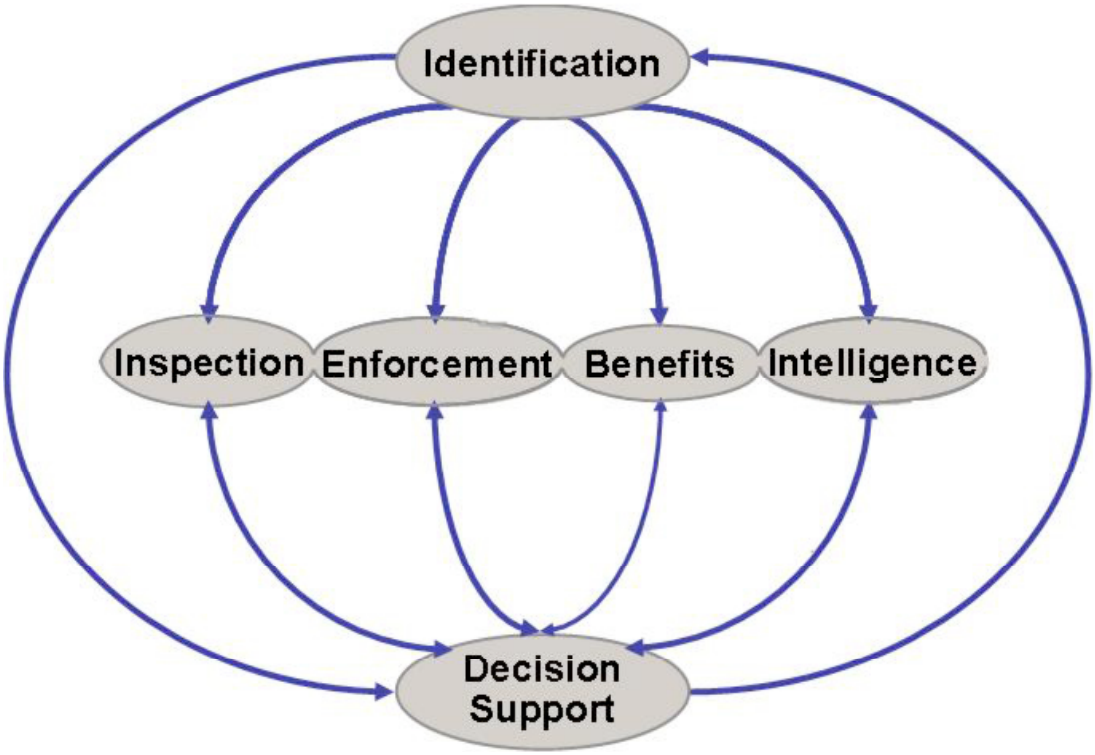


Figure 3. Conceptual IT system.

Cargo

A comprehensive system controls and tracks all commercial goods imported into the U.S. by the cargo process. The automated system receives all data from the time merchandise and goods are prepared for import to the final liquidation of duty fees. It receives the data primarily through electronic data interchange. It tracks the merchandise and processes paperwork requirements for both CBP and the importing community.

The entry process has two basic phases that track and control cargo: physical entry and financial liquidation. Each phase requires a different inspection and uses different system components.

Physical entry process

- *Arriving by sea*—The majority of cargo entering the U.S. arrives by sea, and nearly 50% of the value of all U.S. imports arrives by sea containers. In fiscal year 2002 (FY02), legacy USCS/CBP recorded that 21,285,262 containers entered the U.S. on sea vessels.[1] Starting in FY02, carriers had to submit a cargo declaration 24 hours before loading cargo aboard the vessel at a foreign port. When cargo arrives at a U.S. POE, CBP officers perform nonintrusive x-ray or gamma-ray secondary inspections on cargo based on selection criteria. CBP has a very sophisticated methodology targeting high-risk cargo, coupled with intelligence, enabling them to focus their enforcement resources in this area and to examine 100% of that high-risk cargo. There are also initiatives in place, such as the Container Security Initiative (CSI), that assist in identifying the high-risk cargo and facilitate the processing of low-risk cargo.

- *Arriving by land/rail*—The land POEs process the next highest volume of cargo. In FY02, legacy USCS/CBP recorded 1,430,107 containers entering by truck and 11,129,390 containers entering by rail.[2] A cargo system component tracks and releases highly repetitive shipments at land border locations. A CBP officer scans a bar code and verifies that the bar code matches the invoice data. After verifying the data, the CBP officer releases the cargo, noting only the quantity of items imported, unless he or she determines something is amiss. Having the information electronically greatly facilitates the movement of vehicle traffic and eliminates time-consuming data entry by the CBP officer. CBP uses nonintrusive x-ray or gamma-ray inspection to perform secondary inspections on cargo based on selection criteria.

- *Arriving by air*—Airports handle the smallest volume of cargo. Only 2% by weight of all cargo moves by air worldwide.[3] However, airfreight transport now accounts for well over a third of the value of the world trade in merchandise. The lower decks of passenger aircraft currently carry about 58% of global airfreight. CBP counts air cargo by entries, not by container. Entries can be as large as a car or as small as a widget. The main system can begin to track cargo status when the flight departs from the last foreign airport with a separate component.

Vessels (USCG)

Two important border management roles the U.S. Coast Guard plays are monitoring cargo vessels in the waterways in and around the POEs and providing security. The Coast Guard's IT systems focus on prearrival information. Cargo vessel personnel must notify the USCG of their intent to enter a port 96 hours before arrival and before the vessel enters a 24-mile perimeter. Before a cargo vessel 3000 tons or larger enters the perimeter, it must transmit the information required for cargo, crew and passengers, and the vessel. The USCG will not let a vessel enter the perimeter without the complete set of required information. After receiving the information, the USCG makes a determination

[1] U.S. Customs News, Press Release, June 2002, Office of Public Affairs: http://www.customs.gov/hot-new/pressrel/2002/0604-00.htm.
[2] Ibid.
[3] Ibid.

whether to board a vessel for inspection. Another longer-reaching effort to “secure the supply chain” for cargo is underway. This activity establishes a security monitoring of certain U.S.-bound cargo from the time it is loaded to the time it reaches a POE in the U.S.

Transportation Workers and Infrastructure (TSA)

The primary mission of the TSA is to protect U.S. transportation systems to ensure security and freedom of movement of travelers and commerce. Its responsibilities extend to all modes of travel and include the requisite infrastructure necessary to support a variety of critical transportation activities. The TSA has made significant progress in providing efficient and effective screening for airline passengers, goods, and cargo.

TSA currently is involved in a variety of advanced technology initiatives, one of which is the Transportation Worker Identification Card (TWIC). When fully developed and deployed, TWIC should be a nationwide transportation worker identity solution that verifies the identity of transportation workers, validates their background information, assists transportation facilities with managing their security risks, and accounts for personnel access to transportation facilities and activities of authorized personnel.

Cargo IT System Components

When importers are preparing shipments, a broker component first collects data in the main system. Qualified participants file required import data electronically with CBP. Although participation is voluntary, brokers, importers, carriers, port authorities, and independent service centers currently file over 96% of all entries with this component. CBP officers must enter the remaining 4% of cargo data entries manually.

Before the cargo arrives, a manifest component handles notification of its pending arrival. It also allows for faster identification and release of low-risk shipments and allows participants to transmit manifest data for sea, air, and rail electronically before carrier arrival. CBP can determine in advance whether the merchandise merits examination or should receive immediate release.

When the carrier arrives at the border, the primary inspection consists of presenting forms and documents to CBP officers—Entry Form CF 3461/Alt, invoice, packing list, bill of lading, etc. To expedite the release of cargo during primary inspection, a bar code system tracks and releases highly repetitive shipments at land border locations. The CBP officer only needs to note the quantity of items imported, unless he or she detects that something is amiss. Depending on the type of cargo, other government agencies may need to make additional inspections.

Financial release process

When the inspection is complete and the cargo date of entry is recorded, the Entry Summary form, CF-7501, is created to determine the duty fees. Importers must submit the summary entry form no later than ten days from release. Fees are based on value at date of release. Customs fees, duties, and taxes must be collected. A clearinghouse

component provides a means for filers to handle the payment electronically. Payment authorization can be transmitted to debit the payer's account and credit the agency location code established in the Treasury for CBP for the amount due. Currently 96% of all cargo entries use the CBP clearinghouse component.

"Entry summary selectivity" reviews the entry summary data. This process uses a line item from the entry summary. The system matches national and local selectivity criteria to assess risk by importer and value to determine if duty fees are correct. The selectivity process allows for a more detailed inspection to determine the accuracy of the financial transactions associated with the imported cargo. When the review process is complete and all payments are collected, the cargo is considered liquidated, and cargo processing is finalized.

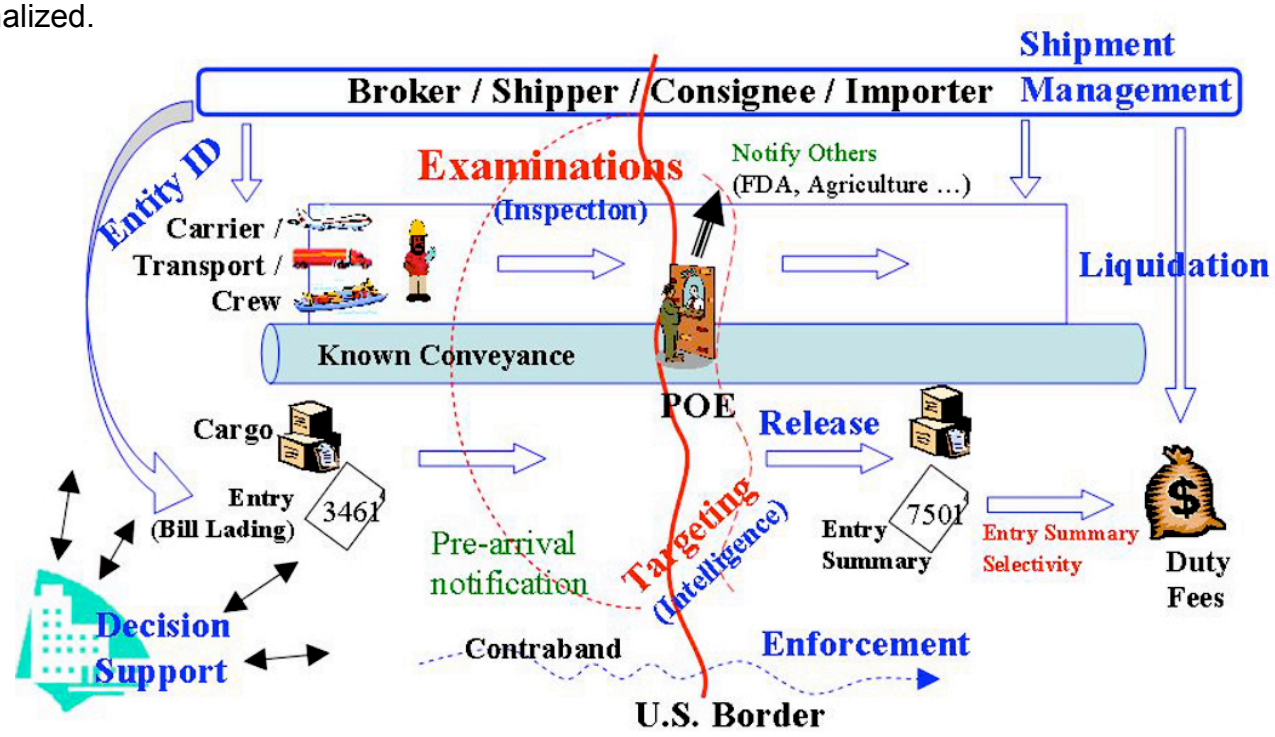


Figure 4. The cargo functional area.

For the cargo systems, a conceptual system (see Figure 5) is in an early draft stage. It contains many categories similar to the traveler system, and it recognizes the fact that the two systems overlap in several areas. This work is very preliminary at this time.

- Entity ID – Systems that support and maintain the creation of electronic identification of organizations and other entities associated with cargo importation.
- Inspection/Examination – Systems that support the inspection/examination process of cargo.
- Enforcement – Systems that deal with case management when laws have been violated while importing cargo through the border.

- Release – Systems that handle the information associated with the release of cargo once they have been inspected/examined.
- Liquidation – Systems that deal with the transactions for the liquidation or payment of import duties.
- Shipment Management – Systems that allow the preparation of all required documentation to import cargo.
- Intelligence (Targeting systems) – For the purpose of this report, systems analyzing patterns and trends to identify cargo requiring more detailed inspection.
- Decision Support – Systems that provide analysis from enterprise data.

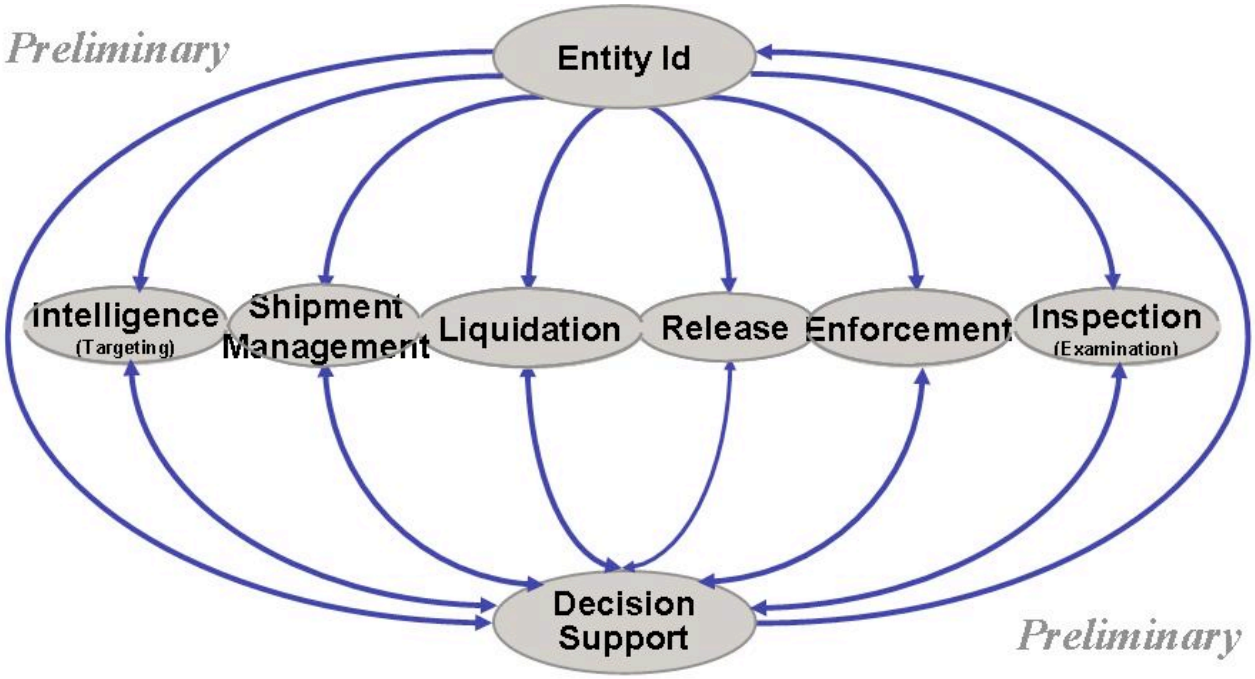


Figure 5. Preliminary cargo conceptual design.

The team will continue to explore these cargo systems with the appropriate entities to further a conceptual interface for these systems and, where appropriate, overlaps with the conceptual traveler design.

IT system components common to both *Traveler* and *Cargo.*

Functional Area	**Component Tasks**
Identification	Collects and updates data to identify the entity crossing the border and associated organizations. The types of entities consist of the traveler and the different roles associated with the traveler, cargo identification, the carrier or vessel on which the cargo is carried, and the Entry filer. (Entry filer is the entity who is responsible for paying the duties for the cargo.)

Inspection/ Examination	Collects and updates data to identify an event, entry and/or exit, at a specific point in time; records the history associated with the crossing event and associated entities.
Enforcement	Collects and updates data for violations of the law. Its primary function is case management for violations of the law.
Intelligence	For the purpose of this report, the common factor for travelers or cargo is that this function "examines data for patterns of interest" to draw actionable traveler lookouts or cargo targeting information.
Decision Support	Integrates the data across the whole enterprise of IT systems and their specific functions; provides data integration and access control to properly protect the data across the enterprise.

Unique to *Traveler:* cargo is that this function

Visit Management/ Benefits	Collects and updates data for length of stay and change of status for the traveler.

Unique to *Cargo:*

Shipment Management	Tracks a shipment and the different entities that make up a unique shipment at a point in time; looks at the cargo, crew, vessel, and entry filer.
Release	Supports the proper computation of duty fees for cargo that has crossed the border and the physical release of the cargo.
Liquidation	Handles the financial processing of the cargo. Duty fees must be paid before a shipment may be released.

Developing Border Management IT Systems for the Future

Work on the conceptual system in this year's report began with modeling the system at a high level to describe the problem domain as a whole. The report now examines the distinct parts of the problem at a lower level of abstraction and breaks the problem into smaller, manageable components, each a collection of general functions. Based on a logical grouping or unique area of operation, the collection of functions represents what tasks each component should perform. The team will describe each component and how the components interconnect with one another. The way to achieve application interoperability is by having a working set of components and a collaboration between those components.

These components of functional areas perform specific tasks within the border management problem domain. The functional area is responsible for managing specific data elements. High-level components depend upon lower-level components, which depend upon components at yet a lower level. The lowest level contains detailed implementations, which themselves depend upon the abstractions. Using this analysis as a blueprint to construct software would require many more levels of detail. However, because the implementation is dependant on the abstraction, this keeps the software implementation flexible.

The conceptual "To Be" system the team recommends is an attempt to provide application integration across the existing IT systems and data management functions within the scope of border management. The IT systems' application integration will consist of a working set of distinct functional areas. The primary border management functional areas have unique system components. Each component encapsulates border management functions that operate on the specific entity, traveler or cargo. Each component can use data from the other components to support its functional area.

Finding the best way to apply abstraction to a problem will aid in the design. Abstraction is the elimination of the irrelevant and the amplification of the essential. The team's conceptual design leverages the current IT systems and interoperates the functional areas. To point out the essential, the team will examine each component and the information it tracks to make the best use of the current border management systems.

As previously mentioned, analysis in the cargo areas is still preliminary and may be revised in the future.

Conceptual System Modeling

The massive flow of people and goods across our borders helps drive our economy but can also serve as a conduit for terrorists, weapons of mass destruction, illegal migrants, contraband, and other unlawful commodities. The new threats and opportunities of the 21st century demand a new approach to border management. President Bush envisions a border that is ground on two key principles:

- First, America's air, land, and sea borders must provide a strong defense for the American people against all external threats, most importantly international terrorists but also drugs, foreign disease, and other dangerous items.

- Second, America's borders must be highly efficient, posing little or no obstacle to legitimate trade and travel.[1]

Economically, it is vital that legitimate traffic (both people and goods) continue to move efficiently across our borders through POEs and known, low-risk traffic be facilitated. At the same time, it is critical to our country that undocumented people and illicit goods not be allowed to cross the borders and enter the country. And, overarching both economic and security expectations, it is absolutely essential that privacy of personal information be scrupulously protected. Meeting the competing needs of commerce, security, and privacy will require a vigilant balancing of priorities.

To arrive at a future concept of how IT systems will help maintain balanced system priorities, we have developed a model of the current border management functions and roles. A discussion of the modeling approach follows.

[1] President George W. Bush, available online at http://www.whitehouse.gov/homeland/homeland_security_book.html#10, August 26, 2003.

Background

Any attempt to construct a complex system should use modeling as a tool to clarify the major goals and intended uses of the system. A model is a preliminary pattern serving as the plan from which an item not yet constructed will be produced. Models are representations and simplifications of reality, and users must apply practical judgment.

Modeling the major concepts and their relationships assists in analyzing the problem domain. Multiple models describe static structures, dynamic behavior, technology usage, and product packaging constraints. With high-level models, a simplified mental model of the problem of border management emerges.

Conceptual Model

In the structural model in Figure 6, boxes with text represent ideas or concepts. The relationships that exist between the ideas or concepts are represented as lines that connect the related boxes and a text label that indicates the nature of the relationship.

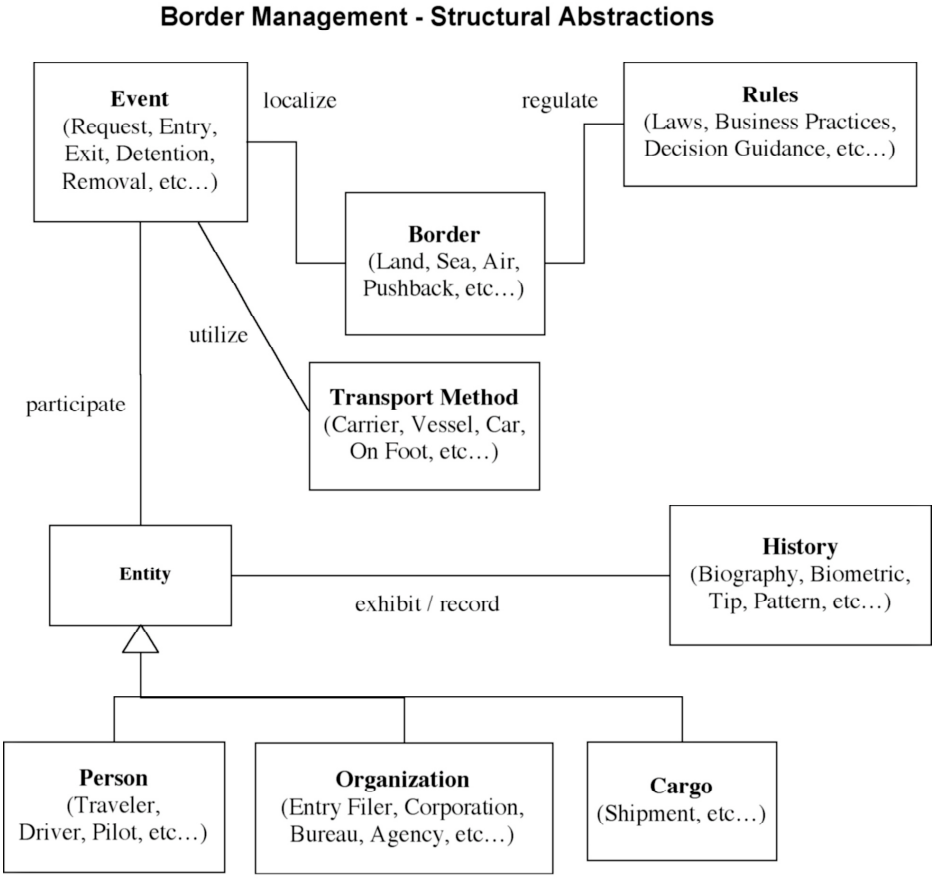


Figure 6. Border management model.

Many more levels of detail would be required before this type of model could be used as a blueprint to construct software. The model merely gives an indication of the size and shape of the challenge of border management.

The team first developed very high level models for facilitating legitimate travel and trade and minimizing risks to the nation resulting from border management activities. Then a lower-level model described assessing reasonable risk during inspection. These models allowed the team to develop the risk assessment matrix shown below.

Inspection Process

Existential Component Risk Criteria

	Scope P = Person C = Cargo	**Low**	**Medium**	**High or Unknown**
Person (Role is traveler or transport operator)	P, C			
Transport (Role is Carrier or vessel)	P, C			
Entry Filer	C			
Cargo (Role is shipment)	C			
Location (Origin, Destination, other…)	P, C			

Temporal Component Risk Criteria

	Scope P = Person C = Cargo	**Low**	**Medium**	**High or Unknown**
Any Event (includes but not limited to border crossings)	P, C			
Visit = Person + Transport + Location	P, C			
Shipment = Trip + Entry Filer + Cargo	C			

Final Risk Determination = Existential Risk Rating + Temporal Risk Rating

Low Risk	Medium Risk	High or Unknown Risk

The three inspection types are

- Prearrival Inspection,
- Point-of-Entry/-Exit Primary Inspection, and
- Secondary Inspection.

Biometrics can help determine Low, Medium, and High or Unknown ratings for the current event and/or entity being inspected and thus the final risk.

Final Risk Determination is **Low**: ⇨ expedite the event. Examples include traveler self-service with fingerprint and cargo carriers with barcode or Radio Frequency identification. See ***Bottleneck Notes*** below.

Final Risk Determination is **Medium**: ⇨ carefully examine the event and all contextual data and make a decision. Human verification of electronic data is necessary (check photo id, capture fingerprints). Human verification of paper documents is also possible.

Final Risk Determination is **High**: ⇨ check the event and all available data electronically and require human verification. This determination is more likely to result in a "disallow event" decision.

Final Risk Determination is **Unknown**: ⇨ the event may not have enough supporting data. An attempt should be made to capture as much electronic data as possible for future use. The event should be moved into one of the other categories if possible. If it is not possible to move the event into another category, it should be treated, by default, as **High**.

Bottlenecks

Figure 7 below shows three places where bottlenecks can occur to negatively affect the Inspection. Which of the three represents the slowest part of the process and what can be done to decrease inspection time?

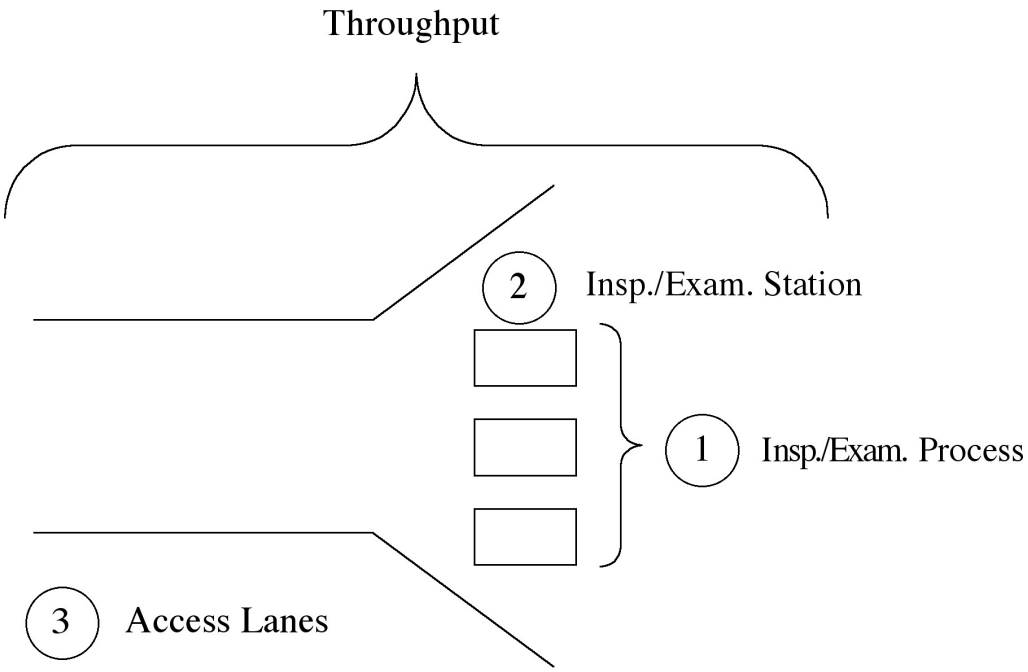


Figure 7. Throughput at border stations.

Maintaining or increasing the quality of the data while complying with all applicable rules (laws, practices, decision guidance) is vital. The goal is to increase throughput without compromising safety and security.

If the access lanes are or cause a bottleneck, and represent the slowest part of the process, then the CBP officer will be idle. Increasing the number of access lanes would be an appropriate response for this situation. (Area number 3 in the diagram)

Otherwise, the inspection process is the bottleneck. If the time required per inspection is efficient, then increasing the number of inspection stations would be an appropriate response (Area number 2 in the diagram). If the time required per inspection is not efficient, then the process itself requires streamlining (Area number 1 in the diagram).

Biometric Identifiers

Using biometrics, an automated method of recognizing a person based on a physiological or behavioral characteristic, depends on being able to measure a characteristic that is particular to the individual and that can give similar results for that individual at future testings. The individual must enroll in the program by providing a sample of the characteristic the system uses for identity checks. The system extracts unique data from the sample and creates a template. When the individual needs access to secure information or a secure area, he or she presents the biometric to a sensor. A computer matches the new sample to the template on file. If the new sample matches within a certain range, access is granted; if the sample does not match the template, access is denied.

Current Use of Biometric Identification

Fingerprint Recognition—The friction ridge patterns of a person's fingerprints form before birth and remain consistent throughout life, barring accidental or intentional damage. Although scientific investigations are ongoing to prove the uniqueness of each person's prints, law enforcement has used fingerprints for identification purposes for over 40 years. The user can provide a flat fingerprint by pressing his or her finger flat against the scanner or a rolled fingerprint by rolling the finger from one edge of the fingernail across to the other. A scanner captures the image of the fingerprint. The image is enhanced to reduce noise from cuts and scars or worn fingerprints and increase the definition of the ridges. Proprietary algorithms extract the features that go into the fingerprint template and create the basis for identification.

Iris Recognition—A person's iris, the colored ring that surrounds the pupil of the eye, develops during gestation and becomes stable early in life; only certain medical procedures can change the nature of the iris. The iris is a complex physical structure rich in features useful for analysis. Each iris is unique; the irises of identical twins and even the right and left eyes of the same person are different. In current technologies for iris recognition, a digital photo is taken, and a computer then uses a special algorithm to analyze the zones of the iris selected for matching.

Hand Geometry—The physical characteristics and bone structure of the hand are distinctive and become stable during a person's early teens. The features of interest are the height and width of the hand's back and fingers; the width, height, and length of the fingers; the shape of the knuckles; and how far apart the joints are. Hand geometry systems measure more than 90 characteristics to develop a template less than 10 bytes large. The user places his or her hand palm down on a metal platen, using its pegs to guide the fingers into the appropriate position. A camera acquires a two- or three-dimensional image of the hand; the system uses the image's information about the physical geometry of the user's hand to create a template, which can be compared with the database to verify the user. This process does not involve fingerprints or palm prints.

Voice Recognition—Voice recognition is a combination physical and behavioral biometric; physical features like the size and shape of the mouth, lips, and nasal passages contribute to the sound of each person's voice, and behavioral factors like age and emotional state also influence how the voice sounds at a given time. The system converts the information into a digital form and analyzes the characteristic pitch, tone, and cadence of the speech.

Signature Recognition—Dynamic signature verification (DSV), using the biometrics of a person's signature to verify identity, has become increasingly popular recently. No two people will have signatures that are identical in all the features captured by DSV. DSV differs from a simple signature or "static" scan because it uses the way the signature is made to verify identity. Although a person's signature may demonstrate slight variations over time, the act of signing is natural, almost reflexive, and very difficult to imitate. The user writes his or her signature on a digitizing tablet or with a special stylus that captures the physical features of the process. The system compares these features—shape, speed, timing, pen pressure, stroke length, and when the pen is lifted off the writing surface—to those of the template on file. The DSV template stores a large amount of information against which the user's signature is checked.

Retina Scanning—The capillary pattern of the retina is unique to each eye, in animals as well as humans. Even identical twins have different patterns. These patterns do not change; unless altered by degenerative diseases like glaucoma and diabetes, the retina remains stable throughout a person's lifetime. The scan captures the capillary pattern of the user's retina. Digitizing the scan produces a 96-byte template that contains up to 400 points of reference.

DNA Recognition—DNA matching does use a physiological characteristic for personal identification. However, DNA differs from most other biometrics in several ways. It compares tangible, physical samples rather than templates generated from impressions, images, or recordings. Also, because not all stages of DNA comparison are automated, the comparison cannot be made in real time. Each person, except for identical twins, has a unique DNA pattern, and DNA does not change during a person's lifetime. Because it requires a physical sample, it cannot be faked or imitated. At this time, select law enforcement forensic investigations are the only regular users of DNA identification.

Facial Scan—Facial recognition identifies a person by looking at the outlines of the eye sockets, the cheekbones, and the sides of the mouth and capturing the image with a camera. Scans must be kept up to date because of the aging process. Two methods, local feature analysis and eigenface, take different approaches to creating facial templates.

Biometric Integration in the Near Future

By January 2004, the US Visitor and Immigration Status Indication Technology System (US-VISIT) will begin using biometric data, including photos and fingerprints, to create an electronic entry/exit system for foreign nationals entering the U.S. to work or study. US-VISIT will absorb the functions of some current systems.

CBP officers will scan the travel documents of foreigners entering the country. Once the officers scan a visitor's photograph and fingerprint, they'll check the visitor against a list of individuals who should be denied entry for a number of reasons, including terrorist connections, criminal violations, and past visa violations. The US-VISIT program expects to have systems/procedures in place to enhance the capture of departure information.

Integration Architecture

The state of identity verification in border management today varies from poor to good. Few of the systems are integrated, and those that are do not operate in real time. Border management systems currently use a variety of software languages, operating systems, networks, and databases, mostly based on older technologies that require high maintenance.

Setting up a new database of biometric signatures could bypass the limitations of the current systems. An algorithm can reduce a biometric identifier to unique, key components known as feature vectors. Identifying the key components within a digital fingerprint, photo, or other digital biometric record provides a unique, encrypted biometric signature. The terms referring to these distinctive points in the signature are minutiae or templates. The small size of the signatures means the database design is also small.

To confirm an identity, the system sends the user's personal identification to the database and retrieves the biometric signature. The user then provides a sample of the biometric identifier. If the signatures match, the user is validated and gains access.

Figure 8 illustrates various attributes for the various types of biometrics described.

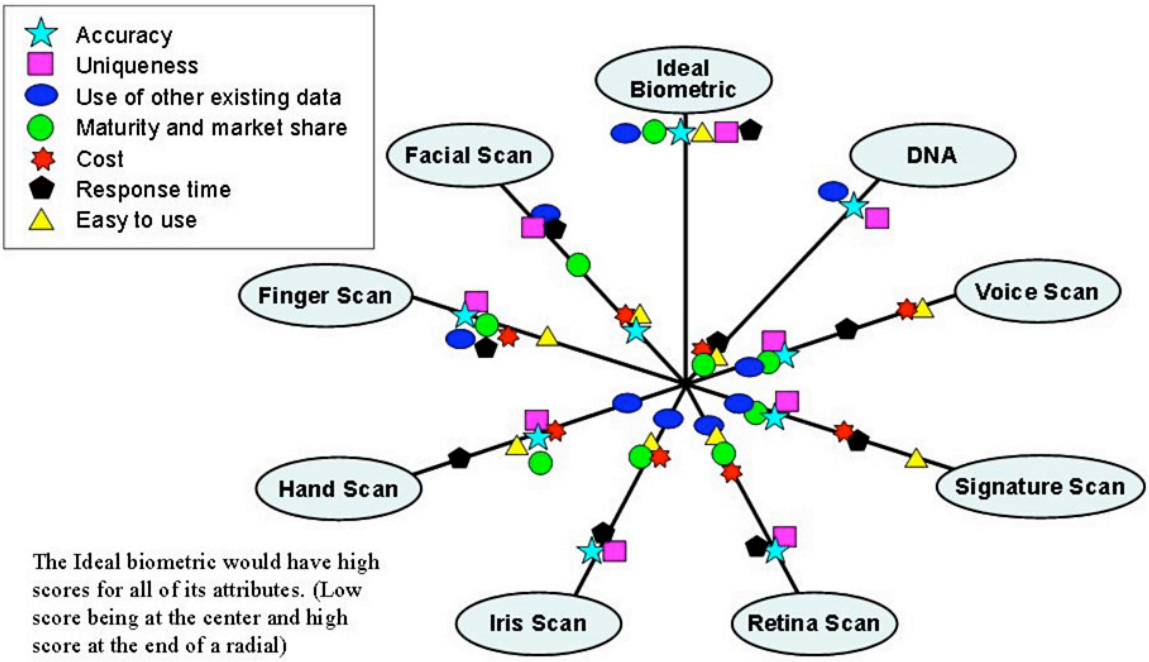


Figure 8. Features of biometric technologies ranked.

New and Emerging Technologies

Interoperability

In June 2003, the Center for Homeland Security at the Los Alamos National Laboratory hosted an Interoperability and Decision Support Workshop. The workshop focused on technological applications that could enhance the effectiveness of the U.S. border management systems. Workshop participants were particularly interested in technologies that could improve system interoperability and decision support needs. Most of the technologies—the results of advanced development activities at the nation's premiere weapons research laboratories—could have direct application to the urgent security needs of the borders of the U.S.

- *Knowledge Integration—Surveillance Decision Environment*

  The goal of a Surveillance Decision Environment (SDE) is to discern and communicate true information signals to appropriate parties from a large variety of sources. Initially, SDE technology may effectively contribute to many of the DHS Inspection, Enforcement, and Identification systems by integrating relevant "knowledge flows" across federal, state, and local governments' environments. As decision support systems mature and broaden, it is likely that SDE could contribute to evolving real-time information integration needs by enhancing critical "situational awareness" functionality.

- *Virtual Interactive Simulation & Inspection Tool*

  The inspection tool technology generates accurate, precision-based three-dimensional (3-D) virtual environments with physics-based objects in a dynamic, interactive environment. Implementation of an interactive simulation system could provide border management experts with a way of experiencing and interacting with 3-D computer-generated “worlds” to determine the most effective security, safety, and operations for complex border management environments. There are also commercially available technologies with some of these attributes that have been used.

- *Integrated Planning and Decision Support*

  Architectures for information unification, integrated planning, and operations support applications in an enterprise environment have been developed. These frameworks provide a secure, distributed execution environment in which confederations of organizations (government, industry, etc.) can bring together information to provide decision-makers with the domain knowledge required to support technology, policy, and program decisions.

- *Computational Linguistics*

  Computational Linguistics (CL) is the science of developing computational algorithms that help minimize confusion and misinterpretation of natural languages. When properly applied to databases and associated text, CL will interpret the information that will allow connections to be established and associations to be traced accurately, particularly in situations involving a great deal of complexity. CL can provide a spectrum of contributions for border management systems, ranging from normalizing terms and validating data through analyzing patterns and extracting information from text.

- *Biometrics*

  Biometrics is the automated method of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic(s). The use of more than one biometric measure increases the flexibility of the system relative to the wide range of unknown factors associated with human beings. Additionally, the application of multiple biometric devices will allow users to select the metric that best identifies them. Advanced biometrics has direct application to the demanding needs of the evolving border management objectives.

- *Data Integration*

  Integrating heterogeneous systems involves dealing with a large variety of data sources to create a “virtual” data repository. The virtual repository provides an integrated view of multiple data sources. This technology enables the smooth integration of information from various systems to work in a federated, heterogeneous environment. The technology employs interface standards for looking up terms and finding equivalences between many different systems. The integration technology provides a mechanism so many different organizations can implement their own rules to the process of accessing their information.

- *Integrating Heterogeneous Systems Based on Open Standard Service Components*

  Integrating heterogeneous systems involves dealing with a large variety of data sources to create a “virtual” data repository. The virtual repository provides an integrated view of multiple data sources. This technology enables the smooth integration of information from various systems to work in a federated, heterogeneous environment. The technology employs interface standards for looking up terms and finding equivalences between many different systems. The integration technology provides a mechanism so many different organizations can implement their own rules to the process of accessing their information.

- *User-Centered Design (UCD)*

  A software product may do everything it is supposed to do, but if users can't figure out how to use it or find the entire experience unbearable, the product has failed. User-centered design places the people who will ultimately use the software at the center of the design process throughout the project lifecycle. It takes into consideration factors such as perception, memory, learning, and problem solving as people interact with the software. It seeks to answer questions about the users’ expectations, tasks, and goals and then uses that information to direct the design of the software. Eliciting feedback through various methods such as design walk-throughs, card sorting exercises, paper prototyping, and usability tests results in a useful, easy–to-use software product. Research shows that improving the usability of software systems can be highly cost-effective. By considering peoples' needs and evaluating design solutions early in the design process, the project team can improve the design when changes are least expensive to make. One of the many components of UCD is Visual Ergonomics, which deals with issues related to human factors and how to display, present, and visualize information.[1]

[1] For information about visual ergonomics, see Chapter 4 of the Task Force report.

Conclusions

The Los Alamos technical support team spent many hours interviewing information technology experts throughout the border management domain. The team was encouraged by the dedication and technical expertise exhibited by the system operators. Almost without exception, the team found highly motivated persons anxiously pursuing the goals of competent border management operations.

In addition to the ideas and recommendations throughout this IT Summary and in Chapter 4 of the full Task Force report, the team has the following macro level conclusions:

(a) Adequate technology-capable personnel are available within the government to meet the technical requirements associated with enhanced security requirements of the Department of Homeland Security provided these personnel are appropriately leveraged.

(b) Border operations goals are dauntingly diverse and, therefore, present unusually challenging opportunities that cannot be addressed solely through technological means.

(c) Current information technology systems in place are not well suited for the evolving demands currently being placed upon them by the Department of Homeland Security.

(d) The Department of Homeland Security has the opportunity to oversee the confederation of an advanced suite of information technology systems that will meet, and likely exceed, security-related expectations for the coming future.

Matrix of Border Management IT Systems

Domain Category	System Id	System Name	Owner
Identification			
	CCD	Consular Consolidated Database	DOS
	IDENT	Automated Biometric Identification System	DHS
	BCC/LaserVisa	Border Crossing Card	DHS
	IAFIS	Integrated Automated Fingerprint Identification System	DOJ
	ISRS	Image Storage and Retrieval System	DHS
	IV	Immigrant Visa	DOS
	IVIS	Immigrant Visa Information System	DOS
	NIV	Non-Immigrant Visa	DOS
	NSEERS	National Security Entry/Exit Registration System	DHS
	PFM/PRISM	Passport Files Miniaturization / Permanent Image Repository	DOS
	APASS/FASTPASS	Automated Personnel Assisted Security Screening	Private Industry
	INSPASS	INS Passenger Accelerated Service System	DHS
	NEXUS	Dedicated commuter lane inspection system	DHS
	SENTRI	Secure Electronic Network for Travelers Rapid Inspection	DHS
Inspections			
	APIS	Advance Passenger Information System	DHS
	ADIS	Arrival Departure Information System	DHS
	NIIS	Non-Immigrant Information System	DHS
	OARS	Outlying Area Reporting Station	DHS
	RIPS	Record of Intercepted Passengers	DHS

Domain Category	System	Acronym Name or Description	Owner
Enforcement			
	ENFORCE	Enforcement Case Tracking System EREM, EABM, EICMIM	DHS
	NAILS	National Automated Immigration Lookout System	DHS
	ISIS	Integrated Surveillance Intelligence System	DHS/BP
	PALS	Portable Automated Lookout System	DHS
	DACS	Deportable Alien Control System	DHS
Benefits			
	CLAIMS	Computer-Linked Application Information Management System (Main Frame)	DHS
	CLAIMS3	Computer-Linked Application Information Management System (Foreign Visitors)	DHS
	CLAIMS4	Computer-Linked Application Information Management System (Naturalization)	DHS
	SEVIS	Student and Exchange Visitor Information System	DHS
	ISEAS	Interim Student, Exchange and visitor Authorization System	DHS
	RAPS/WRAPS	Refugee, Asylum and Parole System	DHS
Intelligence			
	CLASS	Consular Lookout and Support System	DOS
	LEADS	Law Enforcement Analysis Data System	DHS
	IBIS	Interagency Border Inspection System	DHS
	NADDIS	Narcotic and Dangerous Drugs Information System	DOJ
	NCIC	National Crime Information Center	DOJ
	CAPPS II	Computer Assisted Passenger Prescreening System II	DHS/TSA

Domain Category	System	Acronym Name or Description	Owner
Decision Support			
	ACRIME	Automated front-end to DHS Databases	DHS
	BORDER WIZARD	Facility simulation model	GSA
	CIS	Central Index System	DHS
	EID	Enforcement Integrated Database	DHS
	POMS	POE Office Management System	DHS
	WAM	Workforce Analysis Model	DHS
Cargo / Vessel			
	ABI/ACS	Automated Broker Interface	DHS/CS
	ACE (Umbrella)	Automated Commercial Environment	DHS/CS
	ACS (Umbrella)	Automated Commercial System	DHS/CS
	AMS/ACS	Automated Manifest System	DHS/CS
	BRASS/ACS	Border Release Advanced Selectivity System	DHS/CS
	JMIE	Joint Maritime Information Element	DHS/CG
	MISLE	Marine Information for Safety and Law Enforcement	DHS/CG
	SANS	Ship Arrival and Notification System	DHS/CG