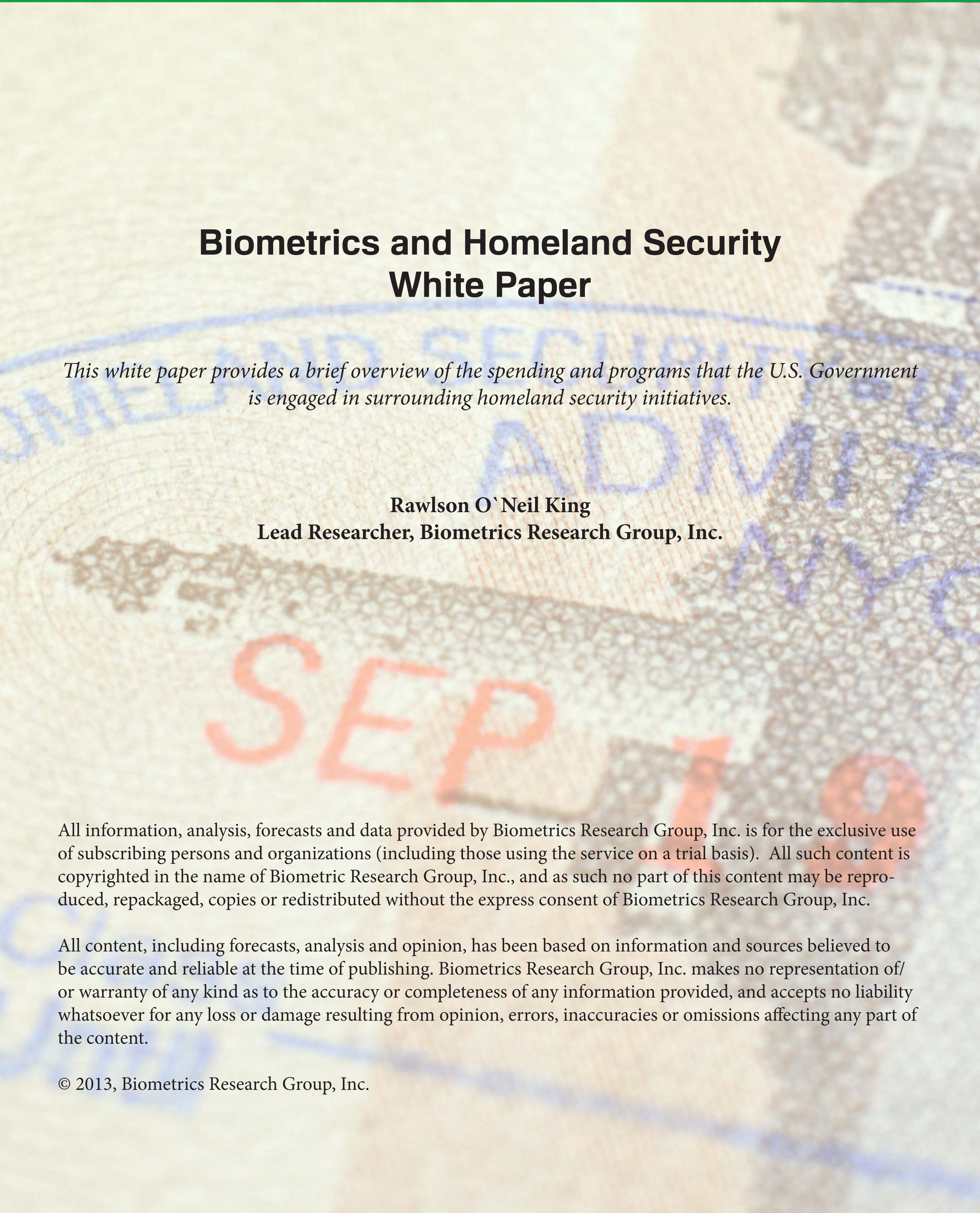
BIOMETRICS RESEARCH GROUP, INC.



Biometrics and Homeland Security White Paper

This white paper provides a brief overview of the spending and programs that the U.S. Government is engaged in surrounding homeland security initiatives.

Rawlson O`Neil King
Lead Researcher, Biometrics Research Group, Inc.

All information, analysis, forecasts and data provided by Biometrics Research Group, Inc. is for the exclusive use of subscribing persons and organizations (including those using the service on a trial basis). All such content is copyrighted in the name of Biometric Research Group, Inc., and as such no part of this content may be reproduced, repackaged, copies or redistributed without the express consent of Biometrics Research Group, Inc.

All content, including forecasts, analysis and opinion, has been based on information and sources believed to be accurate and reliable at the time of publishing. Biometrics Research Group, Inc. makes no representation of/or warranty of any kind as to the accuracy or completeness of any information provided, and accepts no liability whatsoever for any loss or damage resulting from opinion, errors, inaccuracies or omissions affecting any part of the content.

TABLE OF CONTENTS

Research Methodology

Biometrics Research Group, Inc. uses a combination of primary and secondary research methodologies to compile the necessary information for its research projections.

The conclusions drawn are based on our best judgment of exhibited trends, the expected direction the industry may follow, and consideration of a host of industry drivers, restraints, and challenges that represent the possibility for such trends to occur over a specific time frame. All supporting analyses and data are provided to the best of ability.

Primary Research

Biometrics Research Group, Inc. conducts interviews with technology providers, clients, and other organizations, as well as stakeholders in each of the technology segments, standards organizations, privacy commissions, and other influential agencies. To provide balance to these interviews, industry thought leaders who track the implementation of the biometric technologies are also interviewed to get their perspective on the issues of market acceptance and future direction of the industry.

Biometrics Research Group, Inc. also applies its own proprietary micro- and macroeconomic modeling using a regression analysis methodology to determine the size of biometric and related-industry marketplaces. Using databases of both publicly and privately-available financial data, Biometrics Research Group works to project market size and market potential, in the context of the global economic marketplace, using proven econometric models.

Secondary Research

Biometrics Research Group, Inc. also draws upon secondary research which includes published sources such as those from government bodies, think tanks, industry associations, internet sources, and Biometrics Research Group, Inc.'s own repository of news items. This information was used to enrich and externalize the primary data. Data sources are cited where applicable.

Homeland Security: An Introduction

"Homeland security" is an umbrella term referring to the effort to prevent terrorist attacks within the United States, reduce the vulnerability of the U.S. to terrorism, and to minimize the damage from attacks that do occur.

The scope of homeland security includes: emergency preparedness and response (for both terrorism and natural disasters) including volunteer medical, police, emergency management, and fire personnel; domestic and international intelligence activities, largely conducted by the Federal Bureau of Investigation (FBI); critical infrastructure and perimeter protection; border security, including both land, maritime and country borders; transportation security, including aviation and maritime transportation; biodefense; detection of radioactive and radiological materials; and research on next-generation security technologies, such as biometrics.

Homeland Security Government Reorganization

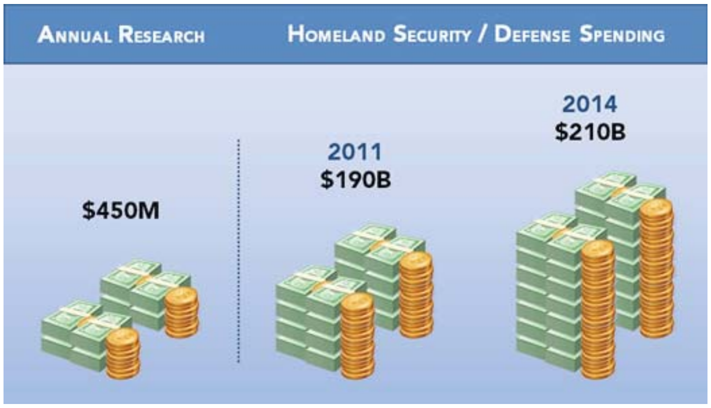
The term "homeland security" arose following a reorganization of many U.S. Government agencies in 2003 to form the United States Department of Homeland Security after the 9/11 attacks, and may be used to refer to the actions of that department, the United States Senate Committee on Homeland Security and Governmental Affairs, or the United States House of Representatives Committee on Homeland Security.

The concept of homeland security extends and recombines responsibilities of government agencies and entities. Homeland security includes 187 federal agencies and departments, including the United States National Guard, the Federal Emergency Management Agency, the United States Coast Guard, Customs and Border Protection, U.S. Immigration and Customs Enforcement, United States Citizenship and Immigration Services, the United States Secret Service, the Transportation Security Administration, the 14 agencies that constitute the U.S. intelligence community as well as Civil Air Patrol. Although many businesses now operate in the area of homeland security, it is overwhelmingly a government function.

President George W. Bush consolidated many of these activities under the United States Department of Homeland Security (DHS), a new cabinet department established as a result of the Homeland Security Act of 2002. However, much of the nation's homeland security activity remains outside of DHS; for example, the U.S Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) are not part of the Department, and other executive departments such as the Department of Defense and Department of Health and Human Services play a significant role in certain aspects of homeland security. Homeland security is ultimately coordinated at the White House by the Homeland Security Council.

U.S. Homeland Security Spending

According to the U.S. Office of Management and Budget, DHS funding only constitutes 20 percent of consolidated U.S. homeland security funding, while approximately 40 percent of the DHS budget funds civil, non-security activities, such as U.S. Coast Guard search and rescue operations and customs functions. DHS is the world's largest homeland counter terror organization, constituting 40 percent of global homeland security funding in 2010.



Biometrics Research Group Inc. has estimated, (based on calculations on previous , current and expected appropriations in a series of U.S. federal budgets, and taking into account the effects of budget sequester and the 2013 government shutdown), that annual funding for total homeland security and defense applications will rise from US$190 billion in 2011 to US$210 billion by 2014. These homeland security and defense applications mainly include border security operations along with active battlefield security measures, and interpolates research and development costs for technologies, such as biometrics.

Funding for homeland security specifically has risen from US$16 billion in fiscal year 2001 to US$71.6 billion requested in fiscal year 2012. Total homeland security spending between September 11, 2001 and May 26, 2011 has totaled US$635.9 billion. Adjusted for inflation, the U.S. has increased homeland security spending by 301 percent since fiscal year 2001. Of this, $163.8 billion has been funded within the Pentagon's annual budget. The remaining $472.1 billion has been funded through other federal agencies.

Total U.S. Government Spending on Homeland Security

Homeland security spending is incredibly difficult to quantify because funding flows through dozens of federal agencies and not just through the Department of Homeland Security (DHS). For example, of the US$71.6 billion requested for "homeland security" in fiscal year 2012, only US$37 billion was funded through DHS. A substantial portion was funded through the Department of Defense – $18.1 billion in fiscal year 2012 – and other departments, including Health and Human Services (US$4.6 billion) and the Department of Justice (US$4.1 billion).

Current Year Dollars (Billions)				Constant FY2013 Dollars (Billions)				
Fiscal Year	Non-DoD Annual Totals	DoD Annual Totals	Total Homeland Security	Fiscal Year	Non-DoD Annual Totals	DoD Annual Totals	Total Homeland Security	Deflators
2001	12.0	4.0	16.0	**2001**	15.5	5.2	20.7	0.7734
2002	27.7	5.2	32.9	**2002**	35.3	6.6	41.8	0.7862
2003	34.0	8.4	42.4	**2003**	42.4	10.5	52.9	0.8023
2004	33.8	7.0	40.8	**2004**	41.1	8.5	49.6	0.8226
2005	37.2	17.2	54.4	**2005**	43.8	20.2	64.0	0.8493
2006	39.6	17.5	57.1	**2006**	45.1	19.9	65.0	0.8782
2007	43.3	16.5	59.8	**2007**	47.9	18.3	66.2	0.9042
2008	47.1	18.0	65.1	**2008**	50.9	19.5	70.4	0.9252
2009	54.3	19.5	73.8	**2009**	57.9	20.8	78.6	0.9385
2010	51.6	19.1	70.7	**2010**	54.5	20.1	74.6	0.9472
2011	50.0	17.0	67.0	**2011**	51.8	17.6	69.4	0.9659
2012 Enacted	50.6	17.4	68.0	**2012 Enacted**	51.5	17.6	69.1	0.9837
2013 Requested	51.0	18.0	68.9	**2013 Requested**	51.0	18.0	68.9	1.0000
Total	**532.2**	**184.7**	**716.9**	**Total**	**588.5**	**202.8**	**791.3**	

Homeland Security	2001-2011 Spending	2001 Spending	2011 Spending	Percentage Increase
	$635.9 billion	$16 billion	$71.6 billion	301 percent

A tremendous amount of homeland security and defense funding is allocated to mundane physical security measures and is provided to state governments through grants to protect infrastructure. However, biometric technology is a leading policy driver within the executive branch of the U.S. Government and has been lauded as a new innovation that can protect and secure national borders.

Indeed, the National Commission on Terrorist Attacks Upon the United States identified biometrics as a key set of technologies that could provide the enhanced security required to protect U.S. borders. Historically, legislation and government implementation have been catalysts for the use of advanced technology. With homeland security initiatives increasing, the escalating use of biometrics is projected to propel growth in the near to mid-term.

Earlier in the decade, biometrics had been identified as a major "killer application" within the information technology field. Not unlike the development of a previous killer application known as the Internet, the U.S. Government is funding biometric technology research projects through the military (i.e., Advanced Research Projects Agency). Of course, due to the nature of biometric measures such as fingerprinting, a large proportion of this internal government research activity is also being conducted by law enforcement agencies (i.e., Federal Bureau of Investigation).

Internationally, there are several criminal and civilian government projects aimed at improving security, but it is the U.S. Government that has purchased biometric equipment on a grand scale. The U.S. Enhanced Border Security and Visa Entry Reform Act of 2002 required all entry ports to the U.S. to install biometric identifiers by October 2004. This required participating countries in the U.S. Visa Waiver program to issue machine-readable passports to their nationals as well, creating a huge opportunity for biometric technology providers.

Use of Biometrics for Homeland Security Applications

The Department of Homeland Security coordinates its biometric activities through the Office of Biometric Identity Management (OBIM). The office coordinates what was formerly referred to as the US-VISIT program, which uses biometrics to simplify travel for legitimate visitors. US-VISIT was appropriated US$232 million and reorganized into the OBIM through the 2013 Homeland Security Appropriations Act.

Biometrics collected by OBIM and linked to specific biographic information enable a person's identity to be established, then verified, by the U.S. Government. With each encounter, from applying for a visa to seeking immigration benefits to entering the United States, OBIM:

- Checks a person's biometrics against a watch list of known or suspected terrorists, criminals and immigration violators

- Checks against the entire database of all of the fingerprints the Department of Homeland Security has collected since OBIM began to determine if a person is using an alias and attempting to use fraudulent identification

- Checks a person's biometrics against those associated with the identification document presented to ensure that the document belongs to the person presenting it and not someone else

OBIM provides the results of its biometric checks to decision makers when and where they need it. At airports across the U.S., OBIM uses the Guardian line of fingerprint scanners from Cross Match Technologies to collect biometric data from visitors. These services help prevent identity fraud and deprive criminals and immigration violators of the ability to cross our borders. Based on biometrics alone, OBIM has helped stop thousands of people who were ineligible to enter the United States.

Arguably, OBIM's use of biometrics has helped strengthen U.S. immigration and border security to a level that did not exist previously. It is estimated by the Department of Homeland Security that every day, 30,000 authorized federal, state and local government users query OBIM's data in order to accurately identify people and determine whether they pose a risk to the United States.

OBIM supplies the technology for collecting and storing biometric data, provides analysis of the data to decision makers and ensures its integrity. By using biometrics, OBIM prevents the use of fraudulent documents, protect visitors from identity theft and stops thousands of criminals and immigration violators from entering the country.

Trusted Traveler Programs

The OBIM is also responsible for trusted traveler programs. Trusted traveler programs provide expedited travel for pre-approved, low risk travelers through dedicated lanes and kiosks. These programs have proliferated over the past several years due to increased air travel and globalized business. The United States, through its Department of Homeland Security, offers multiple programs: which include NEXUS, SENTRI, Global Entry and Pre✓.

NEXUS

NEXUS is a joint program with the Canada Border Services Agency that allows pre-screened, approved travelers faster processing. NEXUS was established in 2002 as part of the Shared Border Accord, a partnership between the United States and Canada that creates open channels of dialogue and working groups committed to the mutual goals of securing the shared border, while promoting the legitimate trade and travel vital to both economies.

NEXUS is an integrated program with one application and fee submission providing expedited passage in air, land and marine modes of travel. Each approved member will receive a radio frequency identification card. However, individuals who are interested in air travel must undergo an iris capture to have their membership accepted at airports.

Iris recognition biometric technology works with the unique patterns of the iris, which are the colored ring around the pupil of the eye. There are 266 unique characteristics in the human iris which the technology reads.

The iris recognition process involves taking a photograph of the irises. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment in the muscle. Although the coloration and structure of the iris is genetically linked, the details of the patterns are not. The iris develops during prenatal growth through a process of tight forming and folding of the tissue membrane. Prior to birth, degeneration occurs, resulting in the pupil opening and the creation of unique iris patterns. Although genetically identical, an individual's irises are unique and structurally distinct, which allows them to be used for recognition purposes. Iris patterns are processed and encoded into a record that is stored and used for comparison any time a live iris is presented for verification. When using the self-serve kiosk,

NEXUS Program	Administered by Customs and Border Protection, the NEXUS Program provides expedited processing for pre-approved, low-risk travelers by United States and Canadian officials at dedicated processing lanes at designated northern border ports of entry, at NEXUS kiosks at Canadian airports where preclearance is available, and at marine reporting locations.
SENTRI	Administered by Customs and Border Protection, Secure Electronic Network for Travelers Rapid Inspection (SENTRI) is the U.S. Customs and Border Protection's trusted traveler program for approved frequent border crossers at southern land borders. SENTRI allows pre-approved, low-risk travelers access to dedicated commuter lanes, which expedites crossing between the U.S. and Mexico.
Global Entry	Administered by Customs and Border Protection, participants in the Global Entry program can use kiosks at international airports, present machine-readable passports or U.S. permanent resident cards, place their fingertips on the scanner and make a customs declaration. The kiosk issues the traveler a transaction receipt and directs the traveler to baggage claim and eventually, the exit. Travelers must be pre-approved and all applicants undergo a rigorous background check and interview before enrollment.
Pre✓	Pre✓ is an expedited screening initiative, operated by the Transportation Safety Administration. Implementing a key component of the agency's intelligence-driven, risk-based approach to security, Pre✓ enhances aviation security by placing more focus on pre-screening individuals who volunteer to participate to expedite travel experience. Certain frequent flyers from Alaska Airlines, American Airlines, Delta Air Lines, United Airlines, US Airways and certain members of CBP's Trusted Traveler programs, including Global Entry, SENTRI, and NEXUS who are U.S. citizens are eligible to participate. In addition, passengers 12 and younger are allowed through TSA Pre✓ lanes along with eligible passengers.

the system will compare irises with the record stored in the database.

To get the clearest iris photo during enrolment, an applicant must remove eyewear, including prescription glasses and contacts, as well as sunglasses and colored or patterned contact lenses. At the kiosk, NEXUS users do not need to remove prescription glasses or contact lenses, but they do need to remove sunglasses and patterned contacts. There are no known health or safety issues associated with using an iris recognition device. Iris recognition technology involves a monochrome camera that uses visible and safe low-range infrared light.

During the application process, if a person indicates they have a disability that affects their vision which may make it difficult to take a clear photo of the iris, the information is added to their profile. When that person arrives at the airport, instead of using a kiosk, as a NEXUS member they can use a "special services" counter where they would answer standard customs and immigration questions. In these situations, a "non-iris capture" sticker is placed on their membership card at time of enrollment, which allows them to enjoy expedited passage using the special services counter.

NEXUS is available at the following Canadian airports: Halifax Robert L. Stanfield International Airport (YHZ); Montréal-Pierre Elliott Trudeau International Airport (YUL); Ottawa Macdonald-Cartier International Airport (YOW); Toronto Pearson International Airport (YYZ); Winnipeg James Armstrong Richardson International Airport (YWG);Calgary International Airport (YYC); Edmonton International Airport (YEG); and Vancouver International Airport (YVR).

A NEXUS membership card fulfills the travel document requirements of the Western Hemisphere Travel Initiative (WHTI) that has required a passport or other secure travel document by all U.S. and Canadian citizens seeking entry or re-entry into the U.S. by air since 2007 and by land and sea since 2009.

Individuals may qualify to participate in NEXUS if they are a citizen or permanent resident of the United States or Canada residing in either country, or if they are a citizen of a country other than Canada or the United States who plan to temporarily reside lawfully in Canada or the United States for the term of their NEXUS membership and who pass various criminal history and law enforcement checks by both countries.

NEXUS is an example of cross-border coordination at work. A key goal of the partnership is to establish and expand trusted travel lanes at airports, waterways, and land crossings. It's a way to strike the right balance between enhanced security and faster, more efficient travel between the U.S. and Canada.

SENTRI

Secure Electronic Network for Travelers Rapid Inspection (SENTRI) is a program similar to NEXUS that provides expedited entry into the both the United States and Mexico. SENTRI provides expedited processing for pre-approved, low-risk travelers. Applicants must voluntarily undergo a thorough biographical background check against criminal, law enforcement, customs, immigration, and terrorist indices; a 10-fingerprint law enforcement check; and a personal interview with a U.S. Customs and Border Protection (CBP) Officer.

SENTRI was first implemented at the Otay Mesa, California port of entry on November 1, 1995. SENTRI-dedicated commuter lanes also exist in El Paso, TX; San Ysidro, CA; Calexico, CA; Nogales, AZ; Hidalgo, TX; Brownsville, TX; Anzalduas, TX; Laredo, TX; San Luis, AZ and Douglas, AZ.

Under both NEXUS and SENTRI programs, members can enjoy the benefits of Global Entry at no additional cost through using the automated kiosks for entry at participating airports.

Global Entry

Global Entry is a CBP program that allows expedited clearance for pre-approved, low-risk U.S. citizens and permanent residents upon arrival in the United States. At specific U.S. airports, program participants proceed to Global Entry kiosks, present machine-readable passport or U.S. permanent resident cards, place their fingertips on the scanner for fingerprint verification, and make a customs declaration. The kiosk issues the traveler a transaction receipt and directs the traveler to baggage claim and the exit.

Travelers must be pre-approved for the Global Entry program. All applicants undergo a rigorous background check and interview before enrollment.

While Global Entry's goal is to speed travelers through the process, members may be selected for further examination when entering the United States. Any violation of the program's terms and conditions will result in appropriate enforcement action and revocation of the traveler's membership privileges.

Global Entry kiosks are available at the following participating airports: Baltimore/Washington International Thurgood Marshall Airport (BWI); Boston-Logan International Airport (BOS); Calgary International Airport (YYC); Charlotte-Douglas International Airport (CLT); Chicago O'Hare International Airport (ORD); Dallas/Ft. Worth International Airport (DFW); Denver International Airport (DEN); Detroit Metropolitan Airport (DTW); Dublin Airport (DUB); Edmonton International Airport (YEG); Ft. Lauderdale/Hollywood International Airport (FLL); George Bush Intercontinental Airport, Houston (IAH); Guam International Airport (GUM); Halifax Stanfield International Airport (YHZ); Hartsfield-Jackson Atlanta International Airport (ATL); Honolulu International Airport (HNL); John F. Kennedy International Airport, New York (JFK); John Wayne Airport (SNA); Los Angeles International Airport (LAX); McCarran International Airport, Las Vegas (LAS); Miami International Airport (MIA); Minneapolis/St. Paul International Airport (MSP); Montreal Pierre Elliott Trudeau International Airport (YUL); Newark Liberty International Airport (EWR); Orlando International Airport (MCO); Orlando-Sanford International Airport (SFB); Ottawa Macdonald-Cartier International Airport (YOW); Philadelphia International Airport (PHL); Phoenix Sky Harbor International Airport (PHX); Portland International Airport (PDX); Raleigh-Durham International Airport (RDU); Saipan International Airport (SPN); Salt Lake City International Airport (SLC); San Antonio International Airport (SAT); San Diego International Airport (SAN); San Francisco International Airport (SFO); San Juan-Luis Muñoz Marin International Airport (SJU); Seattle-Tacoma International Airport-SeaTac (SEA); Shannon Airport (SNN); Tampa International Airport (TPA); Toronto Pearson International Airport (YYZ); Vancouver International Airport (YVR); Washington-Dulles International Airport (IAD); and Winnipeg James Armstrong Richardson International Airport (YWG).

However, NEXUS and SENTRI members will need to check their account status to see if they qualify under Global Entry, as they may need to submit their 10-fingerprint data or any other necessary documentation in order to receive Global Entry benefits.

Over 650,000 people have registered for NEXUS cards, and the majority are satisfied with the service benefits. By being able to pass through automated passport control, many travelers can spend less than a minute to enter or re-enter the United States. Besides expedited arrival into the U.S. for immigration and customs, those in trusted traveler programs often get expedited security screening at many airports.

Global Entry costs US$100 per person, while NEXUS costs US$50 and SENTRI costs US$122.25 per person.

TSA Pre✓

The Department of Homeland Security also runs Pre✓, administered by the Transportation Security Administration (TSA). The TSA Pre✓ pre-screening initiative allows eligible passengers to volunteer information about themselves to expedite their screening experience. Eligible passengers enter a separate security lane where they undergo expedited screening, and may pass through screening technology without removing shoes, light outerwear, belts, or laptops or 3-1-1 compliant liquids/ gels from their carry-on. To be eligible, participants must be U.S. citizens traveling through one of the 25 participating U.S. airports and must be members of CBP Trusted Traveler programs or select frequent flyers of participating airlines. More than 2.8 million passengers have received expedited screening through TSA Pre✓ security lanes since the initiative began in October 2011.

Since inception to July 2013, 12 million travelers have used the program, which has so far been deployed at 40 American airports. Roughly 2 million people travel by plane in the United States each day. To initiate the Pre✓ program, TSA entered into partnerships with companies that offer travel incentives. Earlier this year, Loews Hotels offered YouFirst Platinum loyalty rewards members complimentary enrollment in the Global Entry program. CBP has also worked with American Express and United Airlines who currently provide reimbursements for their top-tier customers, and continues to partner with other private sector entities to expand the network of Global Entry members.

For autumn 2013, TSA has proposed to open the program to all U.S. citizens and permanent residents. A single applicant will pay an anticipated US$85 enrollment fee online, or at an enrollment center. Under the program, there will be a five-year term of eligibility, after which members will need to reapply. TSA expects the vetting process to take approximately two to three weeks. A U.S. passport will not be required to enroll. The first two enrollment locations, Washington Dulles International Airport (IAD) and Indianapolis International Airport (IND), will open in fall 2013 with plans to expand to additional enrollment sites nationwide.

Applicants will receive a confirmation letter via U.S. mail. Approved applicants will be issued a 'Known Traveler Number' to be used when booking travel. Passengers will enter their Known Traveler Number (KTN) in the 'known traveler field' when booking travel reservations. Passengers may also enter KTNs to frequent flyer airline profiles, where it will be stored for future reservations.

Current TSA Pre✓ participants, including those eligible via a CBP Trusted Traveler Program such as Global Entry, will continue to receive TSA Pre✓ eligibility. Participants who opted-in through their airline frequent flyer program may want to consider applying for TSA Pre✓, as they are more likely to be selected for TSA Pre✓ expedited screening more often if they are vetted via the TSA Pre✓ application process.

Biometrics Research Group, Inc. projects that trusted traveler programs will eventually become the de facto best practice for airport security clearance. In 2011, CBP noted that it had slightly less than 200,000 people registered in its Trusted Traveler Programs. In 2012, CBP acknowledged that it had approximately 290,000 people registered in its Trusted Traveler Programs. Based on the fact that CBP will attempt to market its programs to enroll at least 10 percent of frequent travelers who arrive at U.S. airports, Biometrics Research Group estimates that trusted traveler program usage will increase to 500,000 people by 2015.

Trusted traveler programs not only expedite passengers, but also facilitate information transfer between governments for identity verification at borders. As a consequence, the United States is not alone in using biometrics to enhance security and facilitate legitimate travel. The United Kingdom, Australia, the European Union, Japan, Canada, Mexico and others are implementing biometric identification programs to expedite travel and improve border security.

International and Departmental Biometrics Data Sharing

The U.S. Government works with the above countries to share best practices and move toward a consistent approach that provides for secure global travel. As countries continue to develop compatible biometric systems, the U.S. will be able to more accurately identify dangerous people, while making travel safer, more convenient, predictable and secure, but difficult, unpredictable and intimidating for those who want to attack American interests.

With the goal of improving biometric data interoperability capabilities between countries, Accenture was awarded a nine-month contract from the Department of Homeland Security to expand international data-sharing capabilities and secure Web services for the OBIM.

The contract is worth $30 million and according to the company, work under the contract will support sharing between the United States, United Kingdom, New Zealand, Canada and Australia.

Accenture is also set to expand the use of secure Web services for all stakeholders, facilitating access of this data. The company says that since the development of reusable 'services', the time it takes for new users to access the system has decreased from nine months to three weeks.

OBIM also provides biometric information to internal government clients, including the U.S. Department of State, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, U.S. Citizen and Immigration Services, the U.S. Coast Guard and the Transportation Security Administration. Upgrades under the contract also will enable biometric information to be shared in real time with the U.S. Department of Justice and U.S. Department of Defense.

The U.S. Department of Homeland Security tested a crowd-scanning facial recognition system last year, called the Biometric Optical Surveillance System (BOSS), following two years of government-funded development.

The documents obtained under a Freedom of Information Act request determined that a $5.2 million contract for the system was awarded to Electronic Warfare Associates, an American military contractor, which was the only company to place a bid.

As the documents outline, the system consists of two towers with infrared sensors that capture two pictures of people from different angles to create a 3D visualization of a person's face to perform comparison or identification through facial recognition. To test the system, the Department of Homeland Security hired the Pacific Northwest National Laboratory, though it was ultimately determined that the system was not yet ready. Those developing BOSS are striving for 80-90 percent accuracy at a distance of 100 meters.

U.S. Immigration and Customs Enforcement receives information from OBIM to identify those who may have overstayed terms of their admission. OBIM matches entry and exit records and provides this information to ICE. This enhanced information sharing process provides an increased capability to identify and apprehend overstays—a critical tool with which to manage the immigration and border system. Before OBIM, international travelers who overstayed their authorized period of admission were only identified as a consequence of some other encounter with law enforcement.

The U.S. Coast Guard uses OBIM biometrics based services at sea to apprehend and prosecute illegal migrants and migrant smugglers. The Coast Guard uses mobile biometric collection devices—handheld scanners and cameras—to collect and compare biometric information against information in the OBIM database about criminals and immigration violators.

One of the manufacturers supplying mobile collection devices to DHS is Cross Match Technologies. The firm's SEEK Avenger mobile handheld unit is aimed at immigration, customs, border control, law enforcement and security communities. The SEEK Avenger weighs just over 3 lbs and according to the company, is the only multi-biometric handheld capable of capturing stand-off dual iris (SAP 40) and fingerprint (FAP 45) images in direct sunlight.

A built-in contact card reader and optional MRZ and ePassort reader provides users the flexibility to configure their optimal credentialing solution. A 5MP camera provides 1D/2D barcode reading, captures evidentiary photos and video, and takes facial images utilizing auto-facial recognition. The optional communications cap incorporates into the device, providing LTE/3G or other network certified cellular modems for additional connectivity beyond Bluetooth and Wi-Fi.

This capability is part of a pilot program to collect biometric information from migrants interdicted while attempting to illegally enter U.S. territory through the eastern Caribbean Sea, around Puerto Rico and the U.S. Virgin Islands, the San Juan sector. The success of the program led the Coast Guard to expand mobile biometric collection to the Florida Straits in 2008.

U.S. Citizenship and Immigration Services uses OBIM's services to establish and verify the identities of people applying for immigration benefits, including asylum or refugee status.

CBP officers are responsible for screening all international travelers to the United States. As part of the screening process, CBP officers collect digital fingerprints and a digital photograph from international travelers. Using OBIM's services, officers quickly and accurately verify whether the person applying for entry is the same person to whom the visa was issued. And for all travelers, with or without a visa, officers use OBIM's services to verify that travelers are who they say they are and that they do not pose a threat to the United States.

The practice of using fingerprints as a method of identifying individuals has been in use since the late nineteenth century when Sir Francis Galton defined some of the points or characteristics from which fingerprints can be identified. These "Galton Points" are the foundation for the science of fingerprint identification, which has expanded and transitioned over the past century.

Fingerprint identification began its transition to automation in the late 1960s along with the emergence of computing technologies. With the advent of computers, a subset of the Galton Points, referred to as minutiae, has been utilized to develop automated fingerprint technology.

A fingerprint usually appears as a series of dark lines that represent the high, peaking portion of the friction ridge skin, while the valley between these ridges appears as white space and are the low, shallow portion of the friction ridge skin. Fingerprint identification is based primarily on the minutiae, or the location and direction of the ridge endings and bifurcations (splits) along a ridge path.

A variety of sensor types — optical, capacitive, ultrasound, and thermal — are used for collecting the digital image of a fingerprint surface. Optical sensors take an image of the fingerprint, and are the most common sensor today.

The two main categories of fingerprint matching techniques are minutiae-based matching and pattern matching. Pattern matching simply compares two images to see how similar they are. Pattern matching is usually used in fingerprint systems to detect duplicates. The most widely used recognition technique, minutiae-based matching, relies on the minutiae points, specifically the location and direction of each point. DHS collects fingerprints from non-U.S. citizens who are either crossing the border as tourists or those applying for immigration. In fact, approximately 300,000 fingerprints are collected per day and stored in the DHS biometric databases, which are interconnected with those of the state and local law enforcement.

OBIM awarded a contract to Ideal Innovations (I-3) in May 2013 to provide fingerprint analysis in support of OBIM's Biometric Support Center. The contract, with a potential value of US$58.9 million, was awarded under I-3's GSA Mission Oriented Buisness Integrated Services (MOBIS) Federal Supply Schedule. The Biometric Support Center provides fingerprint identification services when the automated matching capabilities of DHS's central repository cannot determine if two sets match. In addition, the Center provides latent print identification and biometric watch-list enrollment services to DHS and other U.S. Government agencies.

The U.S. Department of Defense and the Intelligence Community use biometric information about known or suspected terrorists on watch lists. OBIM is working across the federal government to promote intelligence efforts in identifying high-risk persons.

OBIM biometric services also facilitate the identification of terrorists by matching against latent fingerprints collected from terrorist safe houses and ongoing criminal investigations conducted around the world. The move to a 10 fingerprint collection standard expands this capability by providing additional fingerprints against which to match latent fingerprints.

The Department of Justice and State and Local Law Enforcement use OBIM's services to ensure that they have accurate immigration information about individuals they arrest.

OBIM is furthering integration, accessibility and interoperability with other law enforcement and intelligence systems. The Department of Homeland Security and the FBI are establishing interoperability between the OBIM program's Automated Biometric Identification System (IDENT) and the FBI's Integrated Automated Fingerprint Identification System (IAFIS) fingerprint databases.

A crucial step in making IDENT and IAFIS interoperable is the transition from a two- to a 10-fingerprint collection standard for the OBIM and BioVisa programs.

OBIM and the FBI are testing the first stage of IDENT/IAFIS interoperability through pilot programs with state and local law enforcement. During these pilot programs, state and local law enforcement have access to immigration status information about immigration violators they arrest on other charges. At the same time, immigration officials receive automated notification when immigration violators are arrested, so they can take necessary action. With access to immigration violation information, law enforcement officers have more information with which to make decisions about subjects they arrest.

OBIM's Biometric Support Centers helps many federal, state and local agencies with their investigations. These centers are located in San Diego, CA and Arlington, VA.

The U.S. State Department uses OBIM's services to establish and verify the identities of visa applicants at embassies and consulates around the world through its BioVisa program. Consular officers use this information in determining visa eligibility.

The U.S. Department of Homeland Security also initiated regulatory policies that require certain levels of security for government agencies and enterprises. Heightened border security, aviation security, and network security are just three of the many areas DHS is targeting. Biometric technologies are also increasingly being deployed to protect government installations such as military installations, laboratories and hospitals.

DHS also provides logistical control of hazardous materials. In July 2013, MorphoTrust, a division of SAFRAN, announced it had enrolled a total of 1.5 million commercial drivers at 135 enrollment centers for the TSA's Hazardous Materials Endorsement Threat Assessment Program.

As the exclusive enrollment services provider to the TSA in support of its Hazardous Materials Endorsement Threat Assessment Program (HTAP), MorphoTrust screens, trains and vets trusted agents and collects the biographic and biometric data from the 200,000 truck drivers who require hazardous materials endorsements on their commercial driver licenses each year.

In 2004, TSA launched the HTAP program as required under the U.S. PATRIOT Act. With this law, Congress directed TSA to perform fingerprint-based background checks for truck drivers who haul hazardous materials. The TSA created HTAP as an "agent service" offering that allows states to either participate or create their own solutions to meet this mandate. So far, 40 states have elected to use the service since its inception.

Conclusion

While the U.S. Government will still seek to utilize high-end, high technology solutions to protect homeland security, Biometrics Research Group, Inc. notes that future growth in biometrics through government spending will not be exponential due to budgetary restraints.

Previously, our firm conservatively estimated that the U.S. government was spending at least US$450 million per annum on pure biometric research. With the advent of new technologies such as rapid DNA and greater investment in facial recognition technologies, along with investments in "Big Data" systems, Biometrics Research Group now estimates that U.S. Government spending is at least US$700 million per annum on basic biometric research, despite severe spending cuts caused by budget sequestration. Consequently, spending growth will continue to grow, though it should be recognized that the government will still be the primary driver for purchases of biometric technologies and innovation, due to security and legislative requirements.

It is our contention that future spending for biometric technology by government will be extremely strategic. As the Biometrics Research Group stated previously in this research white paper, the National Commission on Terrorist Attacks Upon the United States identified biometrics as a key set of technologies that could provide the enhanced security required to protect U.S. borders. Historically, legislation and government implementation have been catalysts for the use of advanced technology.

As a result, associated budget spending for biometrics, designed to heighten homeland security, will increase, but we believe that this increase will be slight due to economic constraints and budget sequestration.

If any potential for faster government spending on homeland security can be encouraged, Biometrics Research Group projects that it will come through immigration reform. A proposed bipartisan Senate framework, if adopted, would potentially introduce biometrics to Social Security identification cards and would also require the Department of Homeland Security to complete a system to collect biographic data. Republican Senators have also attempted to establish a biometric exit system, which would collect the fingerprints of foreigners departing the United States. While initially rejected, such a system, if ever implemented, would cost several billion dollars.

About the Biometrics Research Group, Inc.

Biometrics Research Group, Inc. provides proprietary research, consumer and business data, custom consulting, and industry intelligence to help companies make informed business decisions.

We provide news, research and analysis to companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, consultation, workshops, executive conferences and our free daily BiometricUpdate.com news service.

Biometrics Research Group has positioned itself as the world's preferred supplier of pure-play market research and consultancy services focused on the biometric marketplace, which particular focus on the law enforcement and national security sectors. Our portfolio of white papers and full research reports is based upon high-quality quantitative analysis, allowing our clients to gain deeper understanding of the marketplace.

We customize our research design, data collection, and statistical reporting using proprietary micro- and macroeconomic modeling and regression analysis.

Through integration of our research results with qualitative analysis from our BiometricUpdate.com news service, we provide actionable business analysis.

Cognitec

The face recognition company

Cognitec develops market-leading face recognition technologies for enterprise and government customers around the world.

Face recognition technologies are constantly evolving in response to new applications and quickly changing biometric markets.

Cognitec's leading-edge products efficiently implement the different processes involved in today's identity management systems using facial data:

- identity verification
- duplicate check
- background check
- management of identity information
- real-time identification in video streams
- acquisition of biometric facial photographs

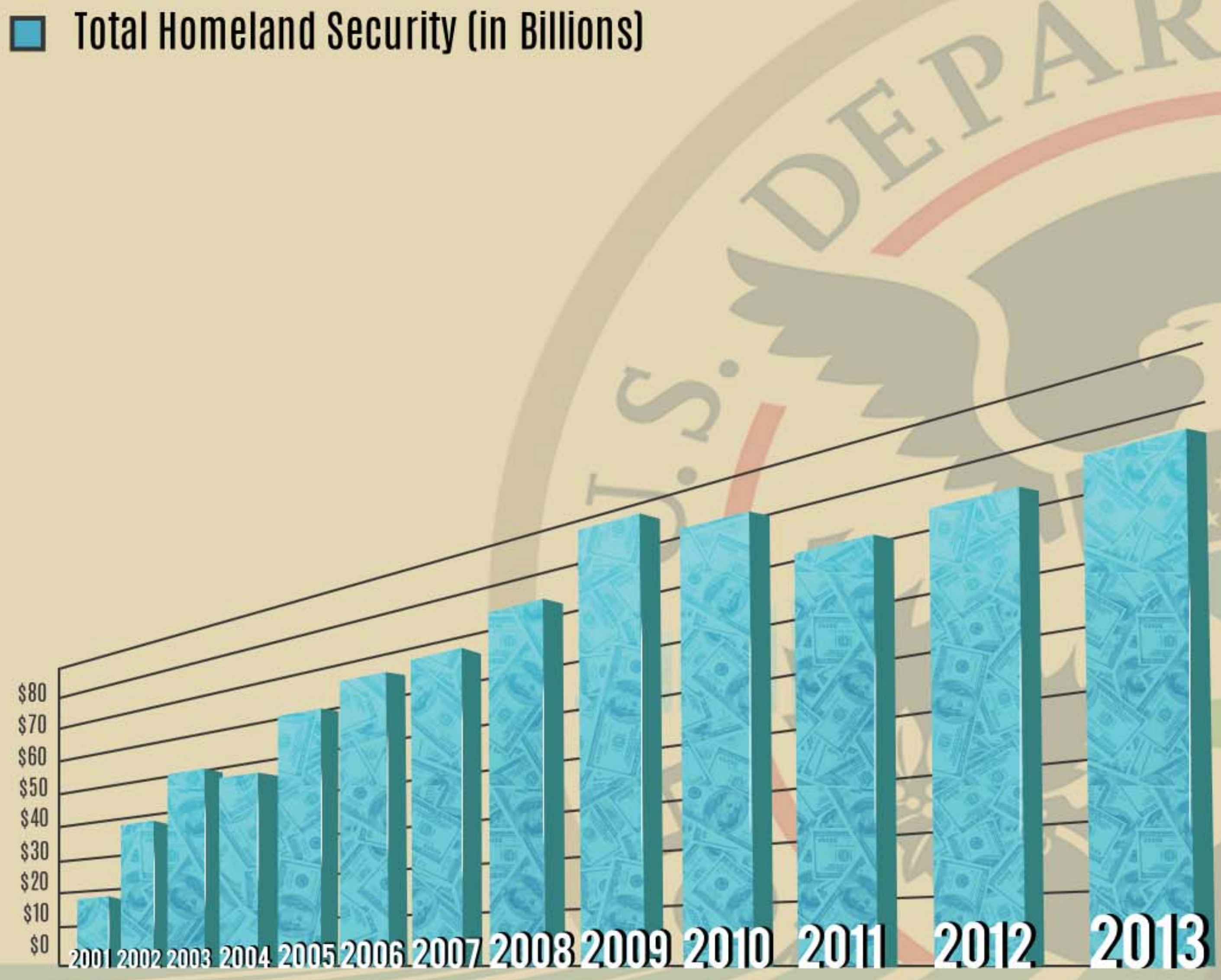
At the same time, Cognitec's products enable new commercial and consumer applications using facial data:

- analyzing people flow by count, age, gender and other measures
- recognizing VIP customers
- enabling digital signs to tailor advertisements
- logging in to computers, phones and banking machines
- indexing and sorting photographs in digital photo albums
- automotive applications for convenience and safety
- allowing humanoid/service robots to recognize faces and interact with people

Biometric performance has always been the major focus of Cognitec's research and development.

Continued tests of government authorities and industry have validated Cognitec's leadership position within the face recognition market since 2002, resulting in a track record of successful reference projects worldwide.

TOTAL U.S. HOMELAND SECURITY SPENDING


Total Homeland Security (in Billions)
$80
$70
$60
$50
$40
$30
$20
$10
$0