United States General Accounting Office

GAO

November 2002

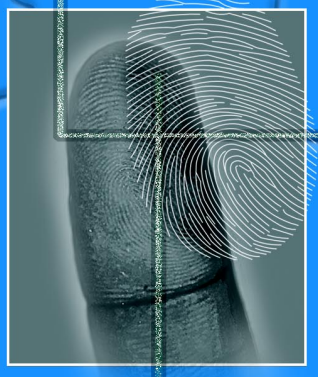
Technology Assessment

Using Biometrics for Border Security









GAO

Accountability * Integrity * Reliability

GAO-03-174

Contents

Letter		1
Technology Assessment Overview		2
	Purpose	2
	Background	3
	Results in Brief	4
	Border Control Overview	7
	Biometric Technologies	9
	Scenarios for Using Biometric Technologies for Border Security	11
	The Role of Biometrics in Border Security	16
Chapter 1	**Introduction**	18
	The Federally Mandated Biometric Chimera System	19
	An Overview of This Report	21
Chapter 2	**Today's U.S. Border Control Procedures**	23
	How U.S. Passports Are Issued	24
	How U.S. Visas Are Issued	29
	Inspection at U.S. Ports of Entry	32
Chapter 3	**Biometric Technologies for Personal Identification**	39
	Biometrics Defined	39
	How the Technologies Work	39
	Leading Biometric Technologies	45
	Emerging Biometric Technologies	49
	Common Applications of Biometric Technologies	52
	Performance Issues	54
	Technologies Viable for U.S. Border Control	69
	Biometric Technology Applied to Border Control Today	74
Chapter 4	**Scenarios for Border Control with Biometrics**	79
	Watch List Check before Issuing Travel Documents	79
	Watch List Check before Entering the United States	83
	U.S. Visas with Biometrics	85
	U.S. Passports with Biometrics	88
	Implementing Multiple Scenarios	91

Chapter 5	**Applying Biometrics to Border Control: Challenges and Implications**	93
	The Performance of Biometric Technologies	93
	How Introducing the Technology Affects People and Procedures	96
	Weighing Costs and Benefits	103
	Effects on Privacy and the Economy	115
Chapter 6	**Summary**	121
	Key Considerations in Using Biometrics for Border Control	122
	High-Level Analysis of Four Scenarios Using Biometrics	125
	The Role of Biometrics in Border Security	127
	Agency Comments and Our Evaluation	129
	External Reviewers' Comments	133
Appendix I	**Our Technology Assessment Methodology**	136
Appendix II	**Fingerprint Recognition Technology**	139
	How the Technology Works	142
	The Leading Vendors	146
	The Cost of Devices	147
	Performance Issues	147
	User Acceptance	148
	The Technology's Maturity	149
	Border Control Applications Piloted and Deployed	157
	Processing Issues	158
	Device Durability and Environmental Constraints	158
Appendix III	**Hand Geometry Technology**	159
	How the Technology Works	159
	The Leading Vendors	160
	The Cost of Devices	160
	Performance Issues	160
	User Acceptance	160
	The Technology's Maturity	161
	Border Control Applications Piloted and Deployed	163
	Device Durability and Environmental Constraints	166

Appendix IV **Facial Recognition Technology** 169

How the Technology Works 169
The Leading Vendors 172
The Cost of Devices 172
Performance Issues 173
User Acceptance 174
The Technology's Maturity 175
Border Control Applications Piloted and Deployed 189
Processing Issues 191
Device Durability and Environmental Constraints 192

Appendix V **Iris Recognition Technology** 193

How the Technology Works 194
The Leading Vendors 196
The Cost of Devices 196
Performance Issues 196
User Acceptance 197
The Technology's Maturity 197
Border Control Applications Piloted and Deployed 199
Processing Issues 202
Device Durability and Environmental Constraints 202

Appendix VI **Cost Estimates for Using Biometrics for Border Security** 203

Initial Cost Elements 203
Recurring Cost Elements 204
Assumptions 206
Estimated Costs for Conducting Watch List Checks with Biometrics 207
Estimated Costs for Issuing Visas with Biometrics 208
Estimated Costs for Issuing Passports with Biometrics 215

Appendix VII **Comments from the U.S. Department of State** 222

Appendix VIII **Comments from the U.S. Department of Justice** 224

Appendix IX **GAO Contacts and Acknowledgments** 229

GAO Contacts 229
Acknowledgments 229

Bibliography 230

Tables

Table 1: Leading Biometric Technologies 5
Table 2: Number of Inspections at U.S. Ports of Entry, Fiscal Year 2001 9
Table 3: Estimated Costs for Implementing Border Security Scenarios 15
Table 4: Number of Inspections at U.S. Ports of Entry, Fiscal Year 2001 23
Table 5: Leading Biometric Technologies and Their Template Size 46
Table 6: Emerging Biometric Technologies and Their Maturity 50
Table 7: Independent Biometric Test Results, 1991–2002 60
Table 8: Four Viable Biometric Technologies Compared 69
Table 9: The Enrollment Size of Seven Operational Biometric Systems 94
Table 10: Estimated Number of Biometric Matching Transactions in Four Border Control Scenarios 94
Table 11: Security Risks and Mitigating Techniques 103
Table 12: The Number and Type of Fraudulent Documents INS Inspectors Intercepted, Fiscal Year 2001 106
Table 13: Estimated Costs for Watch List Checks 110
Table 14: Estimated Costs for Issuing Visas with Biometrics 112
Table 15: Estimated Consular Costs for Issuing Visas with Biometrics 112
Table 16: Estimated Costs for Issuing Passports with Biometrics 113
Table 17: Cost Estimate Uncertainty Analysis for Four Scenarios 114
Table 18: Summary of Biometric Systems Privacy Guidelines 118
Table 19: Estimated Costs for Implementing Border Security Scenarios 125
Table 20: Leading Vendors of Fingerprint Recognition Biometrics 147
Table 21: Summary of Results from the Fingerprint Verification Competition 2000 153
Table 22: Summary of Results from the Fingerprint Verification Competition 2002 154

Table 23: INS's IDENT Fingerprint Benchmark Test Results, 1998 157
Table 24: Identix Airport Facial Biometric Pilot Results 176
Table 25: Facial Recognition Product Usability Test 185
Table 26: Estimated Costs for Watch List Checks before Issuing Travel Documents and before Entering the United States 208
Table 27: Estimated Costs for Issuing Visas with Biometrics Using Fingerprint Recognition 210
Table 28: Estimated Costs for Issuing Visas with Biometrics Using Iris Recognition 211
Table 29: Estimated Costs for Issuing Visas with Biometrics Using Facial Recognition 212
Table 30: Estimated Costs for Issuing Visas with Biometrics Using Fingerprint and Iris Recognition 213
Table 31: Estimated Costs for Issuing Visas with Biometrics Using Fingerprint and Facial Recognition 214
Table 32: Estimated Costs for Issuing Visas with Biometrics Using Fingerprint, Iris, and Facial Recognition 215
Table 33: Estimated Costs for Issuing Passports with Biometrics Using Fingerprint Recognition 216
Table 34: Estimated Costs for Issuing Passports with Biometrics Using Iris Recognition 217
Table 35: Estimated Costs for Issuing Passports with Biometrics Using Facial Recognition 218
Table 36: Estimated Costs for Issuing Passports with Biometrics Using Fingerprint and Iris Recognition 219
Table 37: Estimated Costs for Issuing Passports with Biometrics Using Fingerprint and Facial Recognition 220
Table 38: Estimated Costs for Issuing Passports with Biometrics Using Fingerprint, Iris, and Facial Recognition 221

Figures

Figure 1: The U.S. Passport Application Process 25
Figure 2: A U.S. Passport Cover 28
Figure 3: A U.S. Passport's Biography Page 29
Figure 4: The U.S. Visa Application Process 30
Figure 5: A U.S. Visa Foil 32
Figure 6: The U.S. Port of Entry Inspection Process 33
Figure 7: Motor Vehicles Waiting for Inspection at the Paso del Norte Port of Entry, El Paso, Texas 36
Figure 8: A Driver Being Questioned at a Port of Entry 37
Figure 9: The Biometric Verification Process 42

Figure 10: The Biometric Identification Process 44
Figure 11: The General Relationship between FMR and FNMR 56
Figure 12: Standards for Biometric Systems 66
Figure 13: The Front of a Laser Visa 76
Figure 14: The Back of a Laser Visa 77
Figure 15: Issuing U.S. Visas by a Watch List Check Process 80
Figure 16: Issuing U.S. Passports by a Watch List Check Process 81
Figure 17: System Architecture for a Biometric Watch List Check before Issuing Travel Documents 82
Figure 18: Entering the United States by a Watch List Check Process 83
Figure 19: System Architecture for a Biometric Watch List Check before Entering the Country 84
Figure 20: Issuing U.S. Visas with Biometrics 86
Figure 21: Port of Entry Visa Inspection with Biometrics 87
Figure 22: System Architecture for Issuing Visas with Biometrics 88
Figure 23: Issuing U.S. Passports with Biometrics 89
Figure 24: Port of Entry Passport Inspection with Biometrics 90
Figure 25: System Architecture for Issuing Passports with Biometrics 91
Figure 26: Using Fingerprint Biometrics for Physical Access 140
Figure 27: Using Fingerprint Biometrics for Logical Access 140
Figure 28: A Fingerprint Biometric Device for Personal Identification 141
Figure 29: Common Fingerprint Features 144
Figure 30: Established Fingerprint Types. 145
Figure 31: An IDENT Workstation 150
Figure 32: Fingers Guided by Pegs in a Biometric Hand Geometry Measurement 159
Figure 33: A Traveler Using an INSPASS Hand Geometry Device 164
Figure 34: A Traveler Using Ben Gurion Airport's Biometric Hand Geometry System 165
Figure 35: A Typical Hand Geometry Recognition Device 167
Figure 36: A Hand Geometry Recognition Device That Is Enclosed 168
Figure 37: Local Feature Analysis: A Topographical Grid of Facial Regions 170
Figure 38: Two-Dimensional, Gray-Scale Images of an Eigenface Template 171
Figure 39: CCTV Surveillance Equipment 173
Figure 40: Facial Recognition Distance Identification 178
Figure 41: Facial Recognition Distance Verification 179
Figure 42: Facial Recognition Expression Identification 180

Figure 43: Facial Recognition Expression Verification 180
Figure 44: Facial Recognition Media Identification: Digital to 35 mm 181
Figure 45: Facial Recognition Media Verification: Digital to 35 mm 182
Figure 46: Facial Recognition Pose Identification 183
Figure 47: Facial Recognition Temporal Identification 184
Figure 48: Facial Recognition Temporal Verification 184
Figure 49: The Iris and Other Parts of the Eye 193
Figure 50: Iris Recognition Physical Access Control System 194
Figure 51: Iris Recognition System with Desktop Camera 195
Figure 52: Mapping the Eye for Iris Recognition Systems 196
Figure 53: Iris Recognition Device for Border Control at London's Heathrow Airport 200
Figure 54: Border Control Lane with Iris Recognition Device at London's Heathrow Airport 200

Abbreviations

AAMVA	American Association for Motor Vehicle Administration
AFIS	automated fingerprint identification system
ANSI	American National Standards Institute
API	application programming interface
APIS	Advance Passenger Information System
ATM	automated teller machine
BAPI	biometric application programming interface
CBEFF	Common Biometric Exchange File Format
CCD	Consular Consolidated Database
CCTV	closed-circuit television
CLASS	Consular Lookout and Support System
DOD	Department of Defense
EER	equal error rate
EPPS	Expedited Passenger Processing System
ETT	enrollment timed test
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FERET	Face Recognition Technology
FMR	false match rate
FNMR	false nonmatch rate
FRVT 2000	Facial Recognition Vendor Test 2000
FRVT 2002	Facial Recognition Vendor Test 2002
FTE	failure to enroll

FTER	failure to enroll rate
FVC 2000	Fingerprint Verification Competition 2000
FVC 2002	Fingerprint Verification Competition 2002
IAFIS	Integrated Automated Fingerprint Identification System
IAFS	Immigration and Asylum Fingerprint System
IBG	International Biometric Group
IBIA	International Biometric Industry Association
IBIS	Interagency Border Inspection System
ICAO	International Civil Aviation Organization
IDENT	Automated Biometric Fingerprint Identification System
INCITS	InterNational Committee for Information Technology Standards
INS	Immigration and Naturalization Service
INSPASS	INS Passenger Accelerated Service System
IRS	Internal Revenue Service
JPEG	Joint Photographic Experts Group
LFA	local feature analysis
NAFTA	North American Free Trade Agreement
NAS	National Academy of Sciences
NIST	National Institute of Standards and Technology
NPL	National Physical Laboratory
NSA	National Security Agency
OIDTT	old image database timed test
PALS	Portable Automated Lookout System
PFM	Passport Files Miniaturization
PIN	personal identification number
PRISM	Passport Records Imaging System Management
RSI	Recognition Systems Inc.
SENTRI	Secure Electronic Network for Travelers Rapid Inspection
TECS	Treasury Enforcement Communications System
WSQ	wavelet scalar quantization

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

November 15, 2002

The Honorable Richard J. Durbin
Chairman
The Honorable Robert F. Bennett
Ranking Minority Member
Subcommittee on Legislative Branch
Committee on Appropriations
United States Senate

As directed in the Fiscal Year 2002 Legislative Branch Appropriations Conference Report (House Report 107-259) and subsequent support letters from interested Members of the Congress, we conducted a pilot program in technology assessment that examined the use of biometric technologies for border control. This report discusses the current maturity of several biometric technologies and possible implementation of these technologies in current border control processes. Policy implications and key considerations for the use of biometric technologies are also discussed.

We are sending copies of this report to the Attorney General, the Secretary of State, and interested congressional committees. We will provide copies to others on request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have questions concerning this report, you may contact me on (202) 512-2700 (kingsburyn@gao.gov) or Naba Barkakati, Senior Level Technologist, on (202) 512-4499 (barkakatin@gao.gov). Major contributors to this report are listed in appendix IX.



Nancy R. Kingsbury
Managing Director
Applied Research and Methods

Technology Assessment Overview

Purpose

One facet of the homeland security strategy focuses on border security—preventing the illegal entry of people and goods into the United States without impeding their legitimate flow. Security concerns need to be balanced with practical cost and operational considerations as well as political and economic interests. A risk-based approach can help identify and address security concerns. This is a challenging mission because

- the nation shares a 5,525 mile border with Canada and a 1,989 mile border with Mexico and has a shoreline of about 95,000 miles,
- there are almost 400 official entry points along these borders, and
- there were more than 500 million border crossings into the United States last year, two-thirds by travelers who were not citizens.

Part of the border security mission is controlling the passage of travelers through these official entry points into the United States. Biometric technologies, using one or more of a person's distinct physiological or behavioral characteristics, have been suggested as a way to help automate the identification of travelers to the United States at these ports of entry.

As directed in the Fiscal Year 2002 Legislative Branch Appropriations Conference Report (House Report 107-259) and subsequent support letters from interested Members of the Congress, this technology assessment focuses on four key questions:

1. What biometric technologies are currently deployed, currently available but not yet deployed, or in development that could be deployed in the foreseeable future for use in securing the nation's borders?
2. How effective are these technologies now or likely to be in the future in helping provide security to the nation's borders?
3. What are the economic and effectiveness trade-offs of implementing these technologies?
4. What are the implications of using biometric technologies for personal security and the preservation of individual liberties?

To answer these questions, we convened, with the assistance of the National Academy of Sciences, two meetings on biometrics and border control issues that included manufacturers of facial, fingerprint, and iris recognition and hand geometry technologies, as well as informed

representatives from academia, government, and industry groups; privacy and civil liberty advocates; and other stakeholders such as representatives of border communities and trade organizations. We also interviewed certain users of biometric technologies, including the Federal Bureau of Investigation, Immigration and Naturalization Service (INS), National Security Agency, National Institute of Standards and Technology, the Department of State, and the Canada Customs and Revenue Agency. We reviewed test documentation to understand the performance of biometric technologies and visited a number of ports of entry where these technologies may be used. We interviewed manufacturers of biometric technologies and reviewed their publications to obtain descriptive information about their equipment. We interviewed officials from biometric industry organizations, including the Biometric Consortium and the Biometric Foundation. We also interviewed the International Biometric Group (IBG). We postulated four scenarios for using biometric technologies in border security and created cost models to estimate the rough order of magnitude costs of implementing biometric technologies. We provided our assessment report to the Department of Justice and the Department of State for their review. We also had the draft report reviewed by a number of external experts.

Our report starts with a description of the current border control procedures for admitting people into the United States—issuing visas to citizens of other nations and passports to U.S. citizens and inspecting travelers at the ports of entry. Next, the report describes how biometric technologies work, including the different types of biometric technologies, their levels of maturity, and their operating and performance characteristics. We present four possible scenarios in which biometrics might be applied to current U.S. border control procedures. For each scenario, we analyze some of the costs, benefits, and risks associated with implementation. Finally, the report sums up certain policy implications and challenges to be faced if a biometric system is to be designed and deployed for border security. A number of appendixes provide details on the major biometric technologies.

Background

The United States essentially relies on a two-step approach to prevent inadmissible people from entering the country. The Bureau of Consular Affairs in the State Department is responsible for issuing international travel documents, such as passports in the United States and visas in other countries, and INS in the Department of Justice is responsible for inspecting travelers at the ports of entry.

The term biometrics covers a wide range of technologies that can be used to verify a person's identity by measuring and analyzing his or her characteristics. Identifying a person's physiological characteristics is based on data derived from measuring a part of the body directly. Technologies have been developed to measure people's fingers, hands, faces, and eye retinas and irises. Identifying a person's behavioral characteristics is based on data derived from an individual's actions, such as how he or she talks, types, or signs his or her name. Biometric systems are essentially pattern recognition systems. They use electronic or optical sensors such as cameras and scanning devices to capture images, recordings, or measurements of a person's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics.

Using biometrics as identifiers for border security purposes appears to be appealing because they can help tightly bind a traveler to his or her identity by using physiological or behavioral characteristics. Unlike other identification methods, such as identification cards or passwords, biometrics are less easily lost, stolen, or guessed.

Biometrics have been implemented to a limited degree in U.S. border control systems. For example, since 1993, the INS Passenger Accelerated Service System (INSPASS) has allowed for automated inspections of more than 35,000 frequent fliers at nine airports. The Congress has enacted laws in the past 6 years that require a more extensive use of biometrics in border control systems. These laws require that by the end of 2004, all ports of entry are to be able to perform biometric comparison and authentication of all U.S. visas and other travel and entry documents and that all systems of the State Department, INS, and federal law enforcement and intelligence agencies that contain information about aliens are to be interoperable.

Results in Brief

Biometric technologies are available today and are being used for a variety of applications such as access control and criminal identification and surveillance. We considered a number of leading and emerging biometric technologies that could potentially be used for securing the nation's borders. The seven leading biometric technologies include facial recognition, fingerprint recognition, hand geometry, iris recognition, retina recognition, signature recognition, and speaker recognition (see table 1). Of these, fingerprint recognition, facial recognition, iris recognition, and hand geometry appeared to be suitable for border security because all have been used in border control pilots and applications. However, hand geometry is not highly distinctive and cannot reliably pick out an

individual from among many. Consequently, hand geometry is not suitable if there is a need to search the biometrics database to determine if a person has previously enrolled in the database or is in a watch list. However, hand geometry is viable for verifying claimed identity when another biometric technology is used for the identification check during enrollment. We also looked at emerging biometric technologies, such as ear shape recognition and odor sensing, and found that they are in various stages of development and have not yet been used in border control applications. Our assessment is based on a snapshot of biometric technologies as they existed in early 2002.

Table 1: Leading Biometric Technologies

Technology	How it works	Suitable for border control
Facial recognition	Captures and compares facial patterns	Yes
Fingerprint recognition	Captures and compares fingertip patterns	Yes
Hand geometry	Measures and compares dimensions of hand and fingers	Yes (verification only)
Iris recognition	Captures and compares iris patterns	Yes
Retina recognition	Captures and compares retina patterns	No
Signature recognition	Captures and compares rhythm, acceleration, and pressure flow of signature	No
Speaker recognition	Captures and compares cadence, pitch, and tone of vocal tract	No

Source: GAO analysis.

To evaluate the effectiveness of biometrics in border control, it is important to recognize that the use of biometric technology would be but one component of the decision to support systems that determine who is allowed to enter the United States and who is not. Biometric technology can play a role in associating a person with travel documents such as visas and passports. When used at a border inspection, the biometric comparison can be used to help decide whether to admit a traveler into the United States.

When biometric technology is used in border control, the border control processes will have to be changed not only to use the new technology but also to compensate for its shortcomings. None of these technologies have been used in an application as large as that required for a border control system. Further, biometric technologies are not perfect—all have some measured rates of erroneously matching a person or erroneously not matching a person. The people involved, such as travelers, inspectors, and consular personnel, will have to be trained in how to use the new system and in the new border control processes.

Before any decision is made to implement biometrics in a border control system, the benefits of the system must be weighed against its costs. The purpose of any biometrics initiative is to prevent the entry of travelers who are inadmissible to the United States. For example, using a biometric watch list can provide an additional check to name-based checks and can help detect travelers trying to evade detection who have successfully established a separate name and identity. The use of passports and visas with biometrics can help positively identify travelers as they enter the United States and can limit the use of fraudulent documents, including counterfeit and modified documents, and impostors' use of legitimate documents.

To analyze the costs of using three biometric technologies—facial, fingerprint, and iris recognition—we define four scenarios in which these technologies can be used to support border control operations. Two scenarios use a biometric watch list to identify travelers who are inadmissible to the United States (1) before issuing travel documents or (2) before travelers enter the country. To help bind the claimed identity of travelers to their travel documents, biometrics could be incorporated into (1) U.S. visas or (2) U.S. passports. As defined, these four scenarios are not mutually exclusive and could be implemented independently or in combination. The costs of a biometric border control system will not be trivial. For example, our rough order of magnitude cost estimates to implement visas with biometrics are between $1.3 billion and $2.9 billion initially and between $0.7 and $1.5 billion annually thereafter.

Finally, important policy implications must be addressed in trade-offs between increasing security and the impact on areas such as privacy, economy, traveler convenience, and international relations. Civil liberties groups and privacy experts have expressed concern about the adequacy of protections under current law for biometric data and an absence of clear criteria governing data sharing. Requiring biometric-enabled visas could potentially affect the travel and tourism industry adversely. Increased inspection times because of biometric identification checks could result in longer waiting times, especially at land crossings, causing local merchants on both sides of the border to lose sales. International relations could be affected as other countries reciprocate when the United States asks visitors from those countries to provide biometric identifiers when they apply for visas.

Whether the financial and nonfinancial costs are warranted by the benefits of greater security is a policy issue that should be determined before biometric technologies are implemented in a border control system. This

report provides useful information that can help serve as the basis for these decisions. As our report describes, biometric technology is not a panacea for the border security problem. It is only one component of the decision support systems that determine who is allowed to enter the United States and who is not. A risk-based approach would be helpful in addressing the overall border security problem and the high-level goals that can be achieved with biometric technologies. The approach could rely on establishing what is being protected, who the adversaries are, what the vulnerabilities are, what the priorities are, and what mitigation strategies can be implemented. Answering these questions should help determine the proper role of biometric technologies in border security.

We provided a draft of this report to the Department of Justice and the Department of State for their review. The Department of Justice expressed some concerns, but the State Department stated that it appreciated the thorough and balanced approach we took in our assessment of the use of biometrics for border security. We include State's and Justice's comments in appendixes VII and VIII, respectively, and summarize them in chapter 6. State and Justice also provided technical comments on the draft, which we incorporated as appropriate.

We also provided a draft of this report to 16 different organizations, representing government, industry, and academia, for their review. We received comments and suggestions from 10 reviewers. The comments included the correction of technical inaccuracies and the highlighting of certain aspects of the assessment that reviewers considered important. We have incorporated these comments, where appropriate, in the report. We summarize these comments in chapter 6.

Border Control Overview

The United States relies essentially on two primary procedures to facilitate the entry of people authorized to enter the country and to ensure that inadmissible people are prevented from entering. The State Department's Bureau of Consular Affairs issues international travel documents, including passports to U.S citizens and visas to people who are not U.S. citizens and are traveling to the United States. INS inspects travelers entering the United States through official ports of entry. In addition, INS's Border Patrol is responsible for securing the borders and apprehending travelers entering through other than official ports of entry.

Passport Processing

Passports are issued to U.S. citizens to permit their travel abroad and to facilitate their entry back into the United States. U.S. citizens can apply for

passports at one of more than 4,500 passport acceptance offices. Few of these offices are State Department offices—most are offices in facilities such as U.S. post offices or state, county, township, and municipal government offices. Passport acceptance agents review application packages for completeness and complete a checklist regarding their impressions of applicants and their applications. After the applications are sent to the central application processing center, they are run through a State Department computer system that checks to see (1) whether the applicant has been identified as someone who is not eligible to receive a passport, (2) whether the individual already has an active passport, and (3) whether the individual has multiple applications in process. Passport examiners review the results of these checks and the applications and decide whether to issue passports. If an application is approved, a passport is generated and sent to the applicant.

Visa Processing

With some exceptions, visitors to the United States are required to have a visa to enter. Worldwide, travelers can apply for a visa at 210 embassies and consulates. Visa applications are entered into a State Department computer system and are checked to determine items such as whether an applicant has been identified as someone who is not eligible to receive a visa, whether the applicant's passport matches a passport that has been reported as lost or stolen, or whether the applicant has been refused a visa in the past. In some cases, an interview with the visa applicant or a security advisory opinion from State headquarters is required. In determining whether to grant the visa, the consular officer reviews the data provided in the application and the computer system and, if applicable, the interview and security advisory opinion. If the application is approved, a visa foil is generated and provided to the traveler.

Port of Entry Inspections

All people legally entering the United States must be processed through an air, land, or sea port of entry. As shown in table 2, about 82 percent of border crossings occurred at land ports of entry last year. An individual entering the country through an official port of entry first enters a process called primary inspection. Inspectors determine whether travelers qualify for admission or additional review is necessary. If additional review is necessary, the individual is referred to secondary inspection, where a final decision on whether to admit the traveler is made. During fiscal year 2001, about 1.7 percent of the more than 500 million border crossers entering the country were referred to secondary inspection, where 707,920 were denied admission.

Table 2: Number of Inspections at U.S. Ports of Entry, Fiscal Year 2001

Type of port	Number of ports	Number of inspections
Sea	86	11,952,501
Air	155	79,598,681
Land	154	414,364,965
Total	**395**	**505,916,147**

Source: GAO analysis of INS data.

The processes used for primary inspection vary, depending on the mode of travel—air, land, or sea—and the traveler's nationality. INS uses a combination of methods to inspect travelers, including a brief interview with the travelers, an inspection of their travel or identification documents, and computer checks of their names or the license plates of their vehicles. The traveler's nationality also dictates the documentation requirements. For example, U.S. citizens do not require passports unless they are returning from outside the Western Hemisphere. In general, aliens must present their passport and a U.S.-issued visa. Citizens of countries participating in the visa waiver program do not require a visa to enter the United States.

Biometric Technologies

Biometric technologies have been used in a wide array of applications, including access control to buildings and computers, criminal identification and surveillance, licensing and voter applications, and fraud reduction. Biometric technologies can be used in a verification or identification mode. Regardless of the method used, an enrollment process is required to capture a biometric sample, extract and encode the sample as a biometric template, and store the data in a database for future comparisons. In verification mode (e.g., access control to a building with an identity card), the biometric system verifies the validity of a claimed identity, answering the question "Is this person who she claims to be?" In identification mode (e.g., criminal surveillance), the biometric system compares the individual's biometric with all stored biometric records to answer the question "Who is this person?"

We considered seven leading biometric technologies: facial recognition, fingerprint recognition, hand geometry, iris recognition, retina recognition, signature recognition, and speaker recognition. Four—facial recognition, fingerprint recognition, hand geometry, and iris recognition—appear to be suitable for border control applications. All four have been used in border control pilots and applications. The three other technologies have key

problems that inhibit their use for border control. Retina recognition is considered to be too intrusive because many users experience discomfort in using the devices, which operate close to their eyes. Signature recognition has a high error rate because it has been found that people do not always sign their name the same way each time. Speaker recognition has been piloted in a border control environment but has been found to be unreliable. Also, speaker recognition systems do not perform well in noisy environments such as would be encountered at ports of entry.

The emerging technologies we considered—facial thermography, gait recognition, ear shape recognition, DNA matching, odor sensing, blood pulse measurement, skin pattern recognition, vein scan, and nailbed identification—are in various stages of development and have not yet been used in border control applications.

Fingerprint recognition has been widely used and accepted, primarily in law enforcement, for four decades. Facial recognition can be used to compare either a live facial scan to a stored biometric template or a static image to a digitized photograph. Facial images are already prevalent in travel documents, and people are accustomed to having their picture taken. Hand geometry has been widely used in access control applications and is relatively easy to use. Iris recognition identifies people by numerous characteristics of the colored ring surrounding the pupil of the eye, some of which tend to remain stable throughout life.

In order to differentiate between biometric technology products, they are often characterized by factors such as accuracy, testing, standards, and user acceptance. The accuracy of a biometric technology is usually measured by three key error statistics: the rate at which a system erroneously matches a person, the rate at which a system erroneously does not match a person, and the rate at which people are unable to enroll in a system. To evaluate biometric technologies, the results of independent tests should be consulted. In addition, tests have been conducted in which researchers have successfully fooled biometric systems with artificial characteristics such as a latex finger or a facial picture. Adherence to standards enhances the ability of a biometric device to store and exchange data. Another factor to consider in selecting a biometric technology is the ease of use. Some people find biometric technologies difficult, if not impossible, to use. Still others resist biometrics in general as intrusive, inherently offensive, or just uncomfortable to use.

No biometric technology is best for every situation, but it is possible to determine the most accurate, easiest to use or deploy, or cheapest,

depending on the objectives to be achieved. For example, hand geometry requires the least data storage, fingerprint and iris recognition have the lowest error rates, and facial recognition is the easiest to use. However, each technology also has its limitations. For example, about 2 to 5 percent of people cannot be easily fingerprinted because their fingerprints have become dry or worn from age, extensive manual labor, or exposure to corrosive chemicals. Facial recognition systems have not performed particularly well in independent testing. Iris recognition is a relatively new technology and has not been used in any large operational applications as fingerprint and facial recognition systems have. Hand geometry is not highly distinctive and thus is not suitable for identification applications. These limitations and others would have to be considered if these technologies were to be deployed within a border control system. (More details on the biometric technologies can be found in chapter 3 and appendixes II to V.)

Scenarios for Using Biometric Technologies for Border Security

We developed and analyzed four different scenarios in which fingerprint, facial, or iris recognition biometric technologies or some combination of them could be used to improve current border control procedures. Two scenarios use a biometric watch list to identify travelers who are inadmissible to the United States (1) before issuing travel documents or (2) before travelers enter the country. To help bind travelers to their travel document, two other scenarios could be used to incorporate biometrics into (1) U.S. visas or (2) U.S. passports. These four scenarios can be implemented independently or in combination.

The first scenario involves the use of facial recognition to help identify people ineligible to receive a passport or a visa. The biometric identification check would be conducted at the same time as other computer checks are conducted on each travel document application. The second scenario uses an automated facial recognition system at the ports of entry that can observe a person's face and check the observed facial features against a watch list of people who should be denied access to the country. Both scenarios require the creation of a biometric-based watch list that stores photographs of individuals selected according to criteria determined by border security and other law enforcement agencies. While both scenarios require a centralized facial recognition server to perform matches, performing checks at the ports of entry would also require the purchase of facial recognition systems for the almost 4,000 inspection stations at the ports of entry.

The two other scenarios introduce biometrics to visas and passports. In both of these scenarios, travel document applicants would be required to

have their biometric sample collected—at 1 of 210 embassies and consulates for visa applicants or at 1 of 4,500 passport acceptance offices for passport applicants. As part of the enrollment and document issuance process, an additional identification check of applicants would be made against the database of issued documents to ensure that a person does not receive multiple documents under different identities. Biometric scanners would also have to be installed at the ports of entry to verify the identity of travelers with biometrically enabled travel documents.

The Effect on Border Control Processes

The successful implementation of any technology depends not only on the performance of the technology but also on the operational processes that employ the technology and the people who execute them. The implementation of biometrics in border security is no exception. Further, the use of technology alone is not a panacea for the border security problem. Instead, biometric technology is just a piece of the overall decision support system that helps determine whether to allow a person into the United States. The first decision is whether to issue travelers a U.S. travel document. The second decision, made at the ports of entry, is whether to admit travelers into the country. Biometrics can play a role in both decisions. Sorting the admissible travelers from inadmissible ones is now done by using information systems for checking names against watch lists and by using manual human recognition capabilities to see if the photograph on a travel document matches the person who seeks entry to the United States. When enabled with biometrics, automated systems can verify the identity of the traveler and assist inspectors in their decision making.

The four biometric scenarios will affect key border security processes. A key factor is the performance of the biometric technology. For example, if the biometric technology that is used to perform watch list checks before travel documents are issued has a high rate of false matches, workload could increase at the embassies and consulates for visas and at the passport centers for passports. If the same biometric solution were used at the ports of entry, it could lead to increased delays in the inspection process and an increase in the number of secondary inspections.

Exception processing will have to be carefully considered. Exceptions include people who fail to enroll in a system or are not correctly matched by a verification system. Exception processing that is not as good as biometric-based primary processing could be exploited as a security hole. Failure of equipment must also be considered and planned for. Further, for issuing visas or passports with biometrics, an appropriate transition

strategy must be devised to simultaneously handle biometric travel documents and the current travel documents that could remain valid without biometrics for the next 10 years.

Maintaining Information Security

Implementing biometrically enabled travel documents requires a strong binding and verification process to tie individuals to their identities using their biometrics. A process that does not have strong binding mechanisms can provide little improvement over existing procedures. A failure in the enrollment or the verification process could undermine the use of biometric technologies. For example, procedures must be developed to handle individuals who could not be enrolled in the system. Even if individuals are properly enrolled, they might not be properly matched during inspection. Adequate procedures have to be in place to properly differentiate between system problems and persons who are impostors or otherwise inadmissible to the United States. Information security also is important in ensuring strong binding. If rogue individuals can modify the biometric database or the token on which individual biometric records are stored, a person's bond to his or her biometric data can be compromised.

Weighing Costs and Benefits

Before any significant project investment is made, the benefit and cost information of the project should be analyzed and assessed in detail. The project concept should be based on high-level system goals, which for a border control system would include items such as binding a biometric feature to a person's identity on a travel document, identifying undesirable persons on a watch list, checking for duplicate enrollments in the system, verifying identities at the borders, ensuring the security of the biometric data, and ensuring the adequacy of privacy protections.

The desired benefit of all the scenarios we describe—the use of biometric watch lists or biometrically enabled travel documents—is the prevention of the entry of travelers who are inadmissible to the United States. More specifically, the use of a biometric watch list can provide an additional check to name-based checks and can help detect travelers who are trying to evade detection and have successfully established separate names and identities. The use of passports and visas with biometrics can help positively identify travelers as they enter the United States and can limit the use of fraudulent documents, including counterfeit and modified documents and impostors' use of legitimate documents.

These benefits have several limitations. First, the benefit achieved in each scenario is directly related to the performance of the biometric

technology. The performance of facial, fingerprint, and iris recognition is unknown for systems as large as a biometric visa system that would require the storage and comparison against 100 million to 240 million records. The largest facial, fingerprint, and iris recognition systems contain 60 million, 40 million, and 30,000 records, respectively.

For the watch list scenarios, the population of the watch list is critical to the system's effectiveness. Issuing passports and visas with biometrics will only assist in identifying those currently required to obtain passports or visas to enter this country. For example, U.S. citizens do not have to have a passport to return from Canada or Mexico. Canadians, Mexicans with border crossing cards, and aliens participating in the visa waiver program do not have to have a visa to enter the United States. The issuance of passports and visas with biometrics is also dependent on establishing the correct identity during enrollment. This process will typically be dependent on the presentation of identification documents. If the documents do not specify the applicant's true identity, then the travel document will still be linked to a false identity.

Further, biometric technology is not a solution to all border security problems. Biometric technology can address only problems associated with identifying travelers at official locations such as embassies, passport acceptance offices, and ports of entry. While the technology can help reduce the number of illegal immigrants who cross with fraudulent documents, it cannot help with illegal immigrants who cross "between the borders" and not at a port of entry. INS has previously estimated that up to 60 percent of the 275,000 new illegal immigrants a year do not present themselves at a port of entry to enter the United States. In addition, biometrics cannot help with aliens who enter through ports of entry and are properly admitted by an inspector but may overstay their visit.

The security benefits gained from the use of biometrics must be weighed against the cost of implementing the scenario. For each of the four scenarios, we created cost models to estimate the cost of developing, implementing, and maintaining various biometric processes. We included the costs of both the technology and the effects on people and processes. Table 3 summarizes the initial and annual recurring costs of implementing each scenario. The initial costs include elements such as development, installation, training, biometric hardware and software, and consular facility renovation. The recurring costs include elements such as biometric hardware and software maintenance, system support and operational personnel, consular personnel, facility maintenance, and annual supplies. While the costs of people and space required to enroll travelers in

biometric systems at embassies and consulates are included, the costs of people and space required to verify the biometrics at ports of entry are not included. Consular staff and space are major cost drivers. For example, for issuing visas with biometrics, these costs make up between 21 percent and 31 percent of the system's total initial cost and between 23 percent and 29 percent of its total recurring cost.

Table 3: Estimated Costs for Implementing Border Security Scenarios

Scenario	Initial cost	Annual recurring cost
Watch list check before issuing travel documents	$53	$73
Watch list check before entering the United States	330	237
Issuing visas with biometrics	1,399–2,845	698–1,482
Issuing passports with biometrics	4,446–8,766	1,555–2,363

Note: Dollars are in millions.

Source: GAO analysis.

The watch list scenarios assume the use of facial recognition technology, because faces from photographs are often the only biometric available for individuals who may be inadmissible to the United States. Travel documents with biometrics can use facial, fingerprint, or iris recognition or some combination of the three.

Protecting Privacy and Civil Liberties

The Privacy Act of 1974 limits federal agencies' collection, use, and disclosure of personal information, including personal information such as finger or voice print and photographs. Accordingly, the Privacy Act generally covers federal agency use of personal biometric information. However, as a practical matter, the act is likely to have a more limited application for border security. First, the act applies only to U.S. citizens and lawfully admitted permanent resident aliens. Second, the act includes exemptions for law enforcement and national security purposes. Representatives of civil liberties groups and privacy experts have expressed concerns regarding (1) the adequacy of protections for security, data sharing, identity theft, and other identified uses and (2) secondary uses and "function creep." The Internal Revenue Service, the RAND Corporation, and IBG have developed privacy frameworks that establish guidelines on issues with the scope and capabilities of biometric systems, the protection of data, the protection of users, and the disclosure, auditing, accountability, and oversight of biometric systems.

The Effect on Convenience, the Economy, and International Relations

Any lengthening in the process of obtaining travel documents or entering the United States could affect travelers significantly. At some consular posts, visas are issued the day applications are received. Even without biometrics, the busiest ports of entry regularly have delays of 2 to 3 hours. Increases in inspection times could compound these delays. Delays inconvenience travelers and could result in fewer visits to the United States or lost business to the nation. Further studies will be necessary to measure what the potential effect could be on the American economy and, in particular, on the border communities. These communities depend on trade with Canada and Mexico, which totaled $653 billion in 2000.

Finally, the use of biometrics in the United States could affect the number of international visitors and how other countries treat visitors from the United States. Visitors from some countries may not want to come to the United States if it is less convenient to do so. In addition, because much of visa issuance policy is based on reciprocity—the process for allowing a nation's citizens to enter the United States is similar to the process followed by that nation for visitors from the United States—other nations may start requiring biometric samples from U.S. citizens if the United States requires biometric samples from their citizens. (More details on costs and benefits, as well as the potential implications, of using biometrics are provided in chapter 5.)

The Role of Biometrics in Border Security

People are identified by three basic means: by something they know, something they have, or something they are. Current U.S. border security processes identify travelers by using travel documents such as passports and visas and asking travelers questions—things the travelers have and know. The travel document also establishes a traveler's eligibility to enter the country.

The use of biometrics—things the travelers are—can more securely bind a person's identity to a travel document. Two processes are keys to achieving this binding. First, a strict and thorough enrollment step is necessary to bind a person to an identity. The identity claimed by the traveler is based on documents such as a birth certificate, passport, or other government-issued documents. If processes are not in place to ensure the validity of the traveler's claimed identity, the person could be linked with a false identity. Second, an effective matching process is required to link the person to the travel document. If a person can bypass the biometric check or can deceive the biometric system, the person may be erroneously granted admission to the United States. The performance of the biometric technology is also important to the execution of these

processes. Effective enrollment and matching processes could allow for the use of biometric-enabled travel documents that will establish not only the traveler's eligibility to enter the country but also that the traveler is indeed the individual depicted on the document.

However, biometric technology is just one component of the decision support systems that help determine who is allowed to enter the United States and who is not. For example, the technologies may be able to reduce document fraud but may not be able to detect illegal entry to the United States through other than official ports of entry. A risk-based approach would be helpful in addressing the overall border security problem and the high-level goals that can be achieved with biometric technologies. The approach could rely on answering five basic questions: What are we protecting? Who are the adversaries? What are the vulnerabilities? What are the priorities? What mitigation strategies can be used? A decision to implement our four scenarios or any others should be based on an approach that answers these questions. The scenarios could be partially implemented or combined in different ways. New scenarios could be defined in which travelers voluntarily enroll in a biometric identification system similar to INSPASS for expedited border crossing. Trade-offs should be made to determine the best implementation of biometrics for border security. For example, a partial implementation may be less costly without sacrificing any of the security benefits.

Regardless of how biometric technology is used in border security, using a risk-based approach should help in developing the high-level goals of a system and its concept of operation. The answers should also help point out the limitations of such a system and what it will not be able to provide. They can also play a role in the analysis and weighting of the benefits in a cost-benefit analysis, as well as the trade-off analysis between greater security and issues such as privacy and the economy. With these answers, the proper role of biometric technology in border security can be determined.

Chapter 1: Introduction

A primary element of the homeland security strategy is the improvement of U.S. border security—preventing the illegal entry of people and goods into the United States while facilitating their legitimate flow. Security concerns need to be balanced with practical cost and operational considerations as well as political and economic interests. The United States shares a 5,525 mile border with Canada and a 1,989 mile border with Mexico. Its maritime border includes 95,000 miles of shoreline. There were more than half a billion border crossings into the United States last year; about two-thirds were not by U.S. citizens. The number of distinct travelers into the country each year is unknown because some people enter the country many times in one year, some daily.

Facilitating the flow of people while preventing illegal border crossings is a matter of identifying travelers. People are identified by three basic means: by something they know, something they have, or something they are. People and systems regularly use these means to identify people in everyday life. For example, members of a community routinely recognize one another by how they look or how their voices sound—by something they are. Automated teller machines (ATM) recognize customers from their presentation of a bank card—something they have—and their entering a personal identification number (PIN)—something they know. Using keys to enter a locked building is another example of using something you have. More secure systems may combine two or more of these approaches.

Generally, identifying travelers at the borders is performed by inspecting their travel documents, such as passports and visas, and asking them questions—things the travelers have and know. The U.S. Department of State issues passports to U.S. citizens and visas to others who are not U.S. citizens. The Immigration and Naturalization Service (INS) inspects these travel documents at officially designated air, land, and sea ports of entry.

Technologies called biometrics can automate the identification of individual travelers by one or more of their distinct physical or behavioral characteristics. Biometrics have been suggested as a way of improving the nation's ability to positively determine whether people are admissible to the United States. The term biometrics covers a wide range of technologies that can be used to verify identity by measuring and

analyzing human characteristics—relying on attributes of the individual instead of things the individual may have or know.[1]

Identifiable physiological characteristics include fingerprints, irises and retinas, hand geometry, and facial geometry. How a person signs his or her name is an example of an identifiable behavioral characteristic while speech combines both physiological and behavioral characteristics. To be effective identifiers, biometrics should be universally present, unique to the individual, and stable over time. Biometrics theoretically represent a more effective approach to security because each person's biometric characteristics are distinct and, when compared with identification cards and passwords, are less easily lost, stolen, or guessed.

The Federally Mandated Biometric Chimera System

Biometrics have already been implemented to a limited degree in U.S. border control systems. For example, the INS Passenger Accelerated Service System (INSPASS) has identified travelers and expedited their inspections at nine North American airports for almost 10 years. The Congress has mandated a more extensive use of biometrics in automated border control systems. A series of laws enacted between 1996 and spring 2002 requires the federal government to develop Chimera, an automated information system, to gather and share information among agencies about aliens seeking to enter or stay in the United States.[2] The major requirements for the Chimera system are (1) biometric identifiers; (2) machine-readable visas, passports, and other travel and entry documents; and (3) interoperability among all State Department, INS, and federal law enforcement and intelligence agency systems that contain information about aliens. Chimera will be used to screen applicants for visas and admission to the United States, identify inadmissible and deportable aliens, track lost and stolen passports, monitor foreign students studying

[1]The term biometrics is commonly used to mean biometric technologies and the characteristics themselves.

[2]See 8 U.S.C. §1365a and §1722. These laws' requirements reflect provisions of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (Public Law No. 104-208, div. C, §110, Sept. 30, 1996), the INS Data Management Improvement Act of 2000 (Public Law No. 106-215, June 15, 2000), the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Public Law No. 107-56, §403(c) and §414, Oct. 26, 2001), and the Enhanced Border Security and Visa Entry Reform Act of 2002 (Public Law No. 107-173, May 14, 2002).

in the United States, and help administer law enforcement and national security.[3]

The State Department, the Justice Department, and the National Institute of Standards and Technology (NIST) were to report jointly to the Congress by November 10, 2002, to assess the action needed to implement machine-readable, tamper-resistant travel and entry documents and the biometric comparison and authentication of such documents. By October 26, 2004, State and Justice are to issue to aliens only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers. At the same time, Justice is to install at all ports of entry equipment and software that allow the biometric comparison and authentication of all U.S. visas and other travel and entry documents issued to aliens and machine-readable passports.

To provide the technological basis for Chimera by January 26, 2003, as well as its supporting systems and databases, NIST is to develop a technology standard, including biometric identifier standards for verifying individual identities.

To address concerns about how information in the system will be used, particularly with regard to privacy protection and security, the law mandates that several steps be taken by October 26, 2002. First, the plan for sharing law enforcement and intelligence information with the State Department and INS must establish conditions for State's and INS's use of the information that include their

- limiting its redissemination;
- ensuring that it is used solely for authorized purposes, with criminal penalties for its misuse;
- ensuring its accuracy, security, and confidentiality;

[3]The information in Chimera is to be accessible to federal law enforcement and intelligence officers who, under federal regulation, are responsible for investigating or identifying aliens (Enhanced Border Security and Visa Entry Reform Act, §202(a)(5) (8 U.S.C. §1722)), to federal law enforcement officials to identify and detain individuals who pose a threat to national security (USA PATRIOT Act, §414(b) (8 U.S.C. §1365a note)), and, at the discretion of the attorney general, to federal, state, and local law enforcement officials for law enforcement purposes (INS Data Management Improvement Act, §2 (8 U.S.C. §1365a(f)(2)), amending the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, §110).

- protecting privacy rights;
- providing data integrity by removing obsolete and incorrect information; and
- protecting intelligence sources and methods.[4]

Second, the Department of State and the Department of Justice are to report jointly on the "development, implementation, efficacy, and privacy implications" of a "cross-agency, cross-platform electronic system" for sharing law enforcement and intelligence information regarding aliens seeking to enter the United States.[5]

Third, the president is to establish a commission on interoperable data sharing to oversee Chimera.[6] The commission's duties include monitoring the protections outlined above and considering recommendations regarding security innovations, the adequacy of privacy protections, the adequacy of mechanisms for correcting errors, and other protections against the unauthorized use of data in the system.

An Overview of This Report

This technology assessment focuses on four key questions:

1. What biometric technologies are currently deployed, currently available but not yet deployed, or in development that could be deployed in the foreseeable future, for use in securing the nation's borders?
2. How effective are these technologies now or likely to be in the future in helping provide security to our borders?
3. What are the economic and effectiveness trade-offs of implementing these technologies?

[4]Enhanced Border Security and Visa Entry Reform Act, §201(c)(3) and §201(c)(4) (8 U.S.C. §1356a note). The USA PATRIOT Act §403(a) (amending 8 U.S.C. §1105) has virtually identical requirements with regard to the State Department's receiving National Crime Information Center data.

[5]USA PATRIOT Act, §403(c)(2) and §403(c)(4).

[6]Enhanced Border Security and Visa Entry Reform Act, §203 (8 U.S.C. §1723).

4. What are the implications of using biometric technologies for personal security and the preservation of individual liberties?

To answer these questions, we first describe current border control procedures for admitting people to the United States—issuing visas to citizens of other nations and passports to U.S. citizens and inspecting travelers at the ports of entry. Second, we describe how biometric technologies work, including the different types of biometric technologies, their levels of maturity, and their operating and performance characteristics. We also describe current applications of various biometric technologies.

We present four possible scenarios in which biometrics might be applied to current U.S. border control procedures. For each scenario, we analyze some of the costs, benefits, and risks associated with implementation. Finally, we sum up the implications and challenges to be faced if a biometric system is to be designed and deployed for border security.

Chapter 2: Today's U.S. Border Control Procedures

Last year, there were more than half a billion border crossings into the United States at almost 400 designated ports of entry. Many of these border crossings were by travelers who crossed the border many times in 1 year, some daily. Table 4 shows that the vast majority of inspections—those at border crossings—are at land ports. At land ports of entry in fiscal year 2001, more than 414 million border crossers entered the United States as one of more than 56 million pedestrians or in one of more than 140 million vehicles.

Table 4: Number of Inspections at U.S. Ports of Entry, Fiscal Year 2001

Type of port	Number of ports	Number of inspections
Sea	86	11,952,501
Air	155	79,598,681
Land	154	414,364,965
Total	**395**	**505,916,147**

Source: GAO analysis of INS data.

The laws and regulations governing entry into the United States and the conditions of stay vary by citizenship and method of travel.[1] In general, entry must be accompanied by the appropriate travel documents. U.S. citizens generally must have a U.S. passport to leave or enter the United States. Immigrants generally must have either a U.S. permanent resident card or an immigrant visa and a passport from their own country. Nonimmigrants generally must have a passport from their country and a nonimmigrant visa. The numerous exceptions to these rules include the following:

- Passports are not required of U.S. citizens returning from Canada or Mexico.[2]
- Passports are not required of Canadian citizens unless they are returning from outside the Western Hemisphere. Visas are generally not required for Canadian citizens.

[1]The Immigration and Nationality Act of 1952, as amended (8 U.S.C. §1101 et seq.), and titles 8 and 22 of the Code of Federal Regulations are the primary sources of U.S. immigration law.

[2]According to the Department of Justice, passports are not required of U.S. citizens returning from any point within the Western Hemisphere except Cuba.

- Passports and visas are not required of Mexican citizens who possess a border crossing card issued by the U.S. government allowing them to enter for business or pleasure.

- Visas are not required of citizens of countries participating in the visa waiver program who enter for business or pleasure.[3]

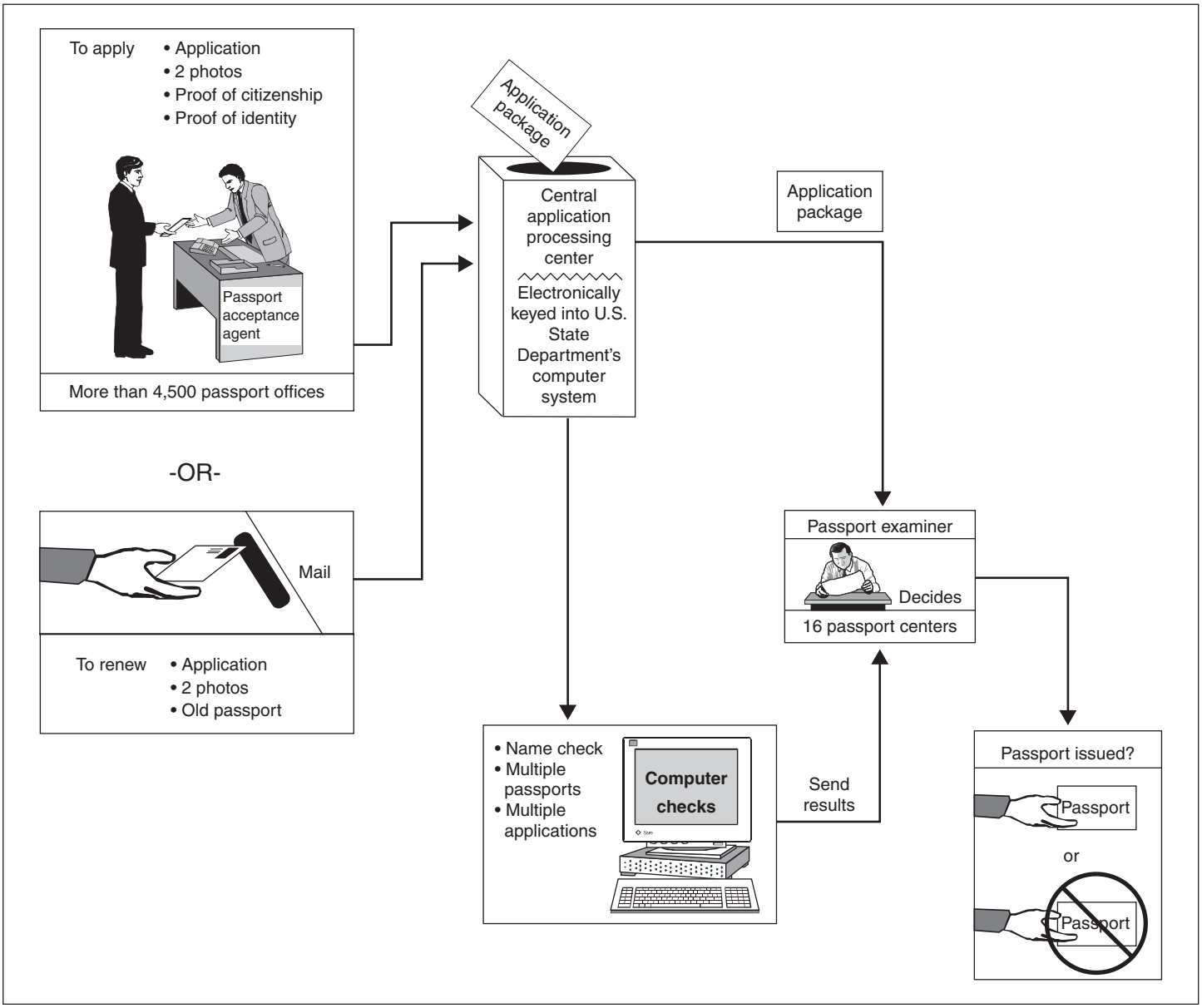
The United States relies on two primary procedures to facilitate the entry of people authorized to enter the country and to ensure that inadmissible people are prevented from entering. The State Department's Bureau of Consular Affairs issues international travel documents, including passports to U.S citizens and visas to people who are not U.S. citizens. INS inspects travelers entering the United States through official ports of entry. In addition, INS's Border Patrol is responsible for securing the borders and apprehending travelers entering through other than official ports of entry.

How U.S. Passports Are Issued

U.S. citizens can apply for a passport at more than 4,500 passport acceptance offices (see figure 1). Few of these are State Department offices; most are offices in facilities such as U.S. post offices or state, county, township, and municipal government offices. All first-time applicants for a passport must appear before a passport acceptance agent at one of these offices.

[3]The visa waiver program permits nationals from designated countries to apply for admission to the United States for 90 days or less as nonimmigrant visitors for business or pleasure without first obtaining a U.S. nonimmigrant visa. The following countries participate: Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, the United Kingdom, and Uruguay (8 U.S.C. §1187, 8 C.F.R. §217.2).

Figure 1: The U.S. Passport Application Process



Source: GAO adaptation of State Department data.

Passport applicants must submit a passport application, proof of U.S. citizenship, proof of identity, two passport photographs, and the application fee. Passport acceptance agents, trained by the State Department to look for potential fraud, review application packages and may ask for additional documentation at their discretion. The agents fill out an observation checklist that includes any concerns they have about the validity of an applicant's identity or citizenship documents. Passport acceptance agents also are to ensure that the photographs match the applicant. The acceptance agents send the application packages to a central application processing center.

Applicants submitting renewal applications may mail them directly to the central application processing center. The old passport, which can serve as proof of identity and citizenship, is sent with the renewal application. About 25 percent of the passport applications the State Department receives arrive through the mail.

At the central application processing center, the application information is electronically keyed into State's computer system, and the application package is forwarded to 1 of 16 State Department passport centers. State's computer systems conduct the following checks:

- A name check, using the Consular Lookout and Support System (CLASS). CLASS, which is used also before U.S. visas are issued, contains lookout records of people who may be ineligible to receive a passport and is populated from a variety of sources, including intelligence, immigration, and child support enforcement data. CLASS also includes information on passports and visas reported lost and stolen. Passport applicants are checked against about 3.2 million records in CLASS.

- A check to determine if the applicant already has an active U.S. passport. An estimated 55 million U.S. passports are currently valid.

- A check to determine if the applicant has multiple passport applications in progress.

At the passport centers, passport examiners review each application, including the results of the computer checks, and determine whether to issue passports. A passport may be refused to an applicant for a variety of reasons: The applicant may be subject to an outstanding federal warrant

for a felony, subject to a court order committing the applicant to a mental institution, or in arrears for child support payments in excess of $5,000.[4]

A passport examiner looks at an entire application as a whole. A "hit" on one of the computer checks does not necessarily result in a rejected application. For example, some government officials who apply may have both a personal passport and an official passport. The passport examiner may resolve name check hits with other data such as place of residence or Social Security number to differentiate between people who may have the same name but are not the same person. If the examiner suspects a problem with the application package, the case can be given to a fraud program manager, who can perform a more detailed investigation, such as verifying the authenticity of the identification or citizenship documents.

If the passport examiner is satisfied that the applicant's documents are authentic and that there is no reason to deny a passport, then the examiner approves the application and the applicant is issued a U.S. passport. Normally, the process takes about 6 weeks. Annually, the State Department issues about 7 million passports that are valid for either 5 or 10 years, depending on the type of passport and the age of the applicant. U.S. passports are depicted in figures 2 and 3.

[4]Passports may be denied for reasons set forth in 22 C.F.R. §51.70.

Figure 2: A U.S. Passport Cover



Source: State Department.

Figure 3: A U.S. Passport's Biography Page



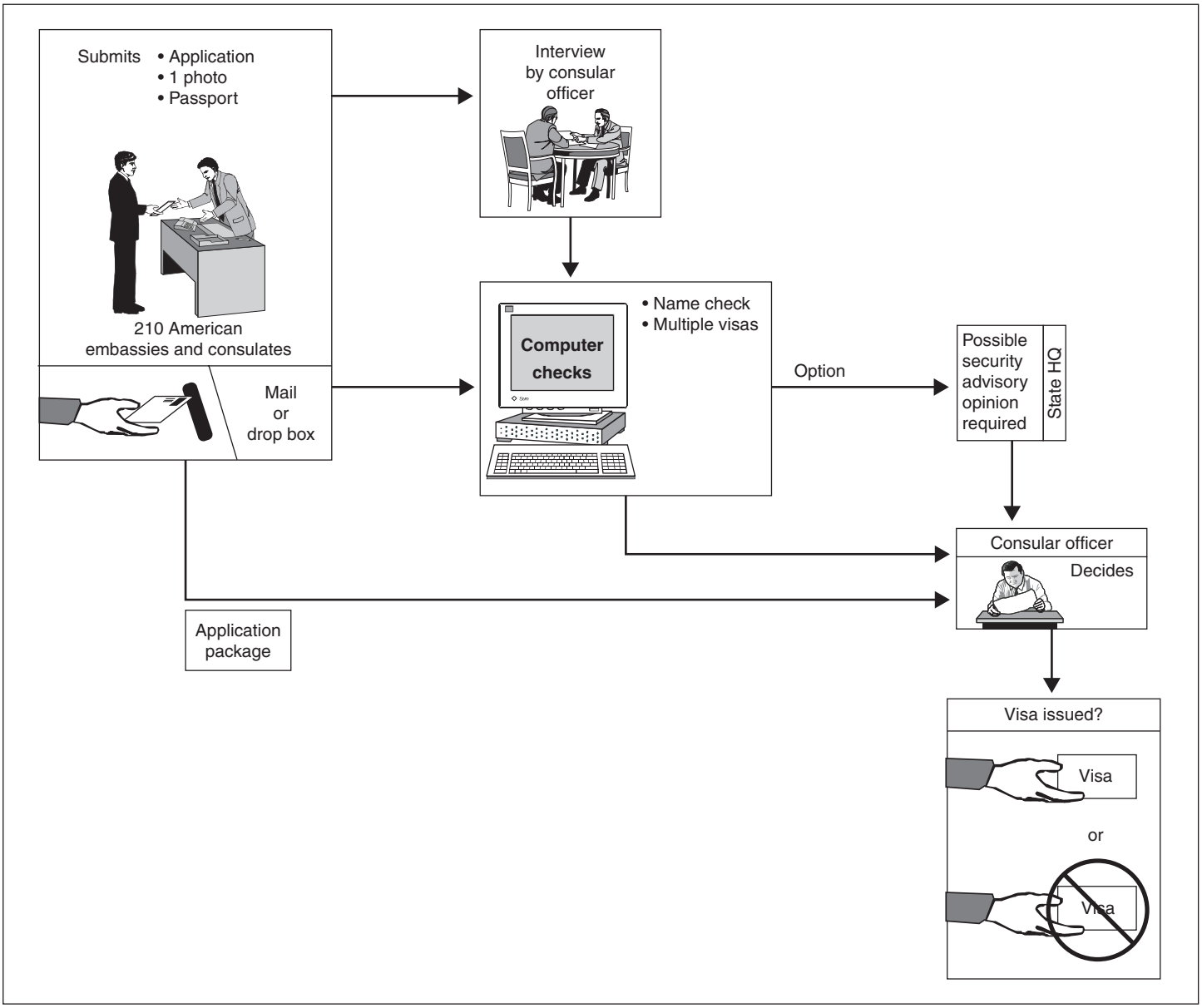
Source: State Department.

How U.S. Visas Are Issued

With some exceptions, foreign visitors must present a visa to enter the United States. Applicants can apply in person for an immigrant or nonimmigrant visa at 210 American embassies or consulates (see figure 4). The vast majority of issued U.S. visas are nonimmigrant visas. An applicant for a nonimmigrant visa must submit an application, passport, and photograph.[5] Some applications may be submitted by mail or in a drop box outside the embassy or consulate. About 37 percent are submitted this way.

[5]The process for issuing immigrant visas, although similar to that for nonimmigrant visas, includes other procedures and checks such as the submission of an immigration petition to INS. About 628,000 immigrant visas are issued each year.

Figure 4: The U.S. Visa Application Process



Source: GAO adaptation of State Department data.

After the data are keyed into the State Department's visa computer system, a consular officer reviews the application package. The officer may interview the applicant, depending on the consular post and the type of visa being applied for. Computer checks are conducted:

- A name check, using CLASS, looks for any matches with individuals who may be ineligible to receive a visa. Visa applications are checked against about 6.5 million records in CLASS.[6] CLASS also includes records of lost and stolen passports reported by other countries.

- A check, using the Consular Consolidated Database (CCD), determines whether the applicant has previously applied for a visa or currently has a valid U.S. visa. CCD stores information about visa applications, issuances, and refusals and obtains information about visa cases every 5 to 10 minutes from each consular post. CCD has about 58 million visa records.

The consular officer makes a decision on whether to issue a visa, based on information gathered from the visa application, passport, supporting documentation, interview (if applicable), and computer checks. In some cases, such as a name-check hit in CLASS, a security advisory opinion from State Department headquarters may also be required. Visas may be denied for a variety of reasons, including health-related reasons, certain criminal offenses, and immigration violations.[7] Using fraudulent documents to obtain a U.S. visa is also grounds for denial.

For nonimmigrant visas, the consular officer must be satisfied that an applicant is not intending to become an immigrant. If the consular officer is satisfied that the applicant's documents are authentic and that there is no reason to deny a visa, then the officer approves the application and a visa is issued (see figure 5). The process can take from a day to several weeks to complete. Last year, of the 10.5 million applications received, about 7.5 million nonimmigrant visas were issued. Depending on the type of visa and the nationality of the applicant, visas can be issued for up to 10 years.

[6]The State Department is adding 8 million criminal history alien records from the Federal Bureau of Investigation (FBI). These records include foreign-born individuals and individuals with unknown place of birth.

[7]Visas may be denied for reasons listed in the Immigration and Nationality Act, §212 (8 U.S.C. §1182).

Figure 5: A U.S. Visa Foil

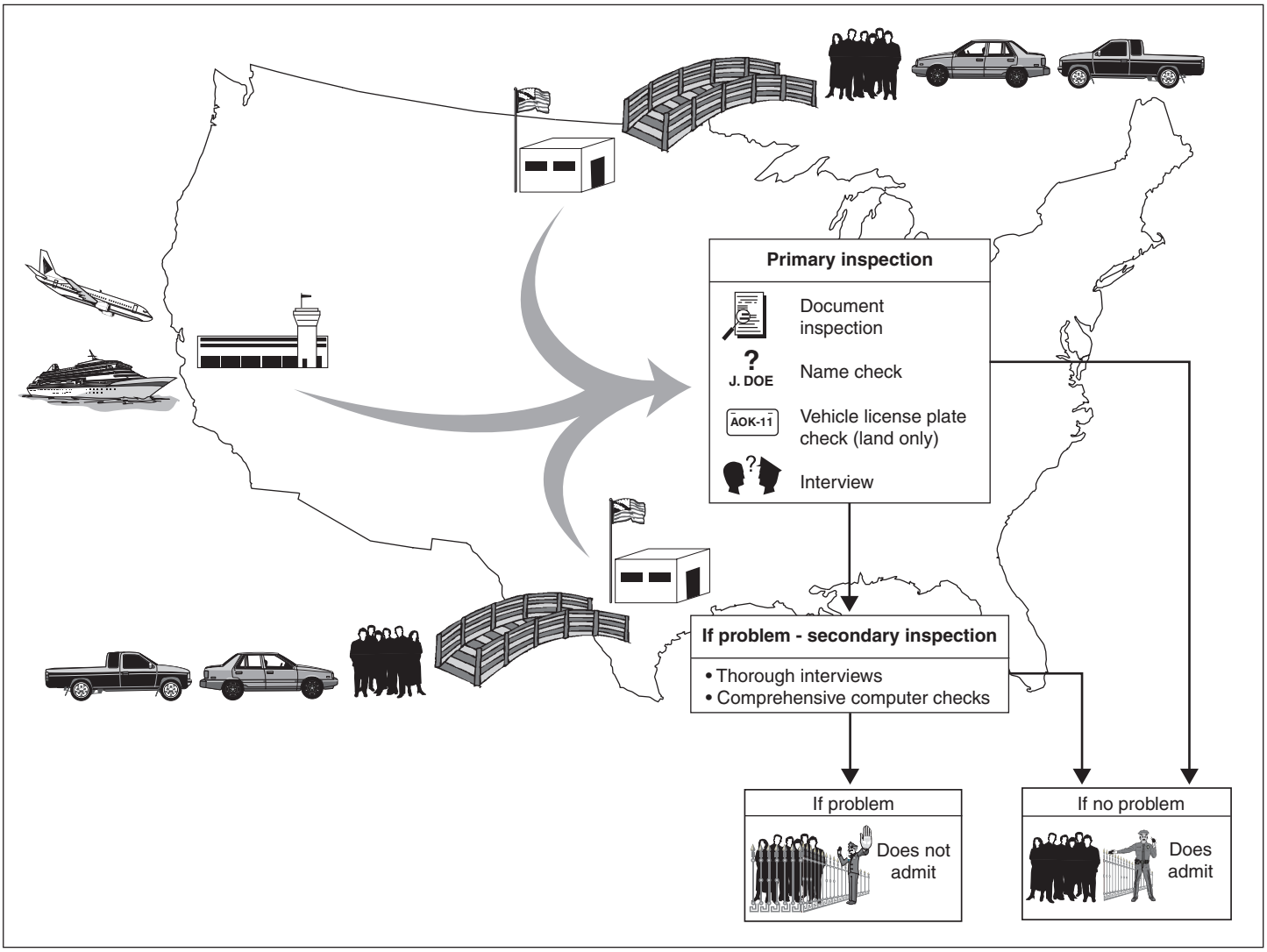


Source: State Department.

Inspection at U.S. Ports of Entry

Lawful entry into the United States generally must be completed through an official air, land, or sea port of entry. Nearly 82 percent of the more than 500 million inspections occur at land ports. Travelers' nationalities and how they enter dictate the primary inspection procedures (see figure 6). A primary inspector is to question each traveler regarding his or her identity and purpose for entering the United States. In addition, the nspector can inspect a traveler's travel documents and perform computer checks on the traveler's name or motor vehicle license plate. While the State Department is responsible for initially granting or denying permission to come to the United States, inspectors ultimately decide whether to allow the traveler into the country at the ports of entry. The issuance of a U.S. visa does not guarantee permission to enter.

Figure 6: The U.S. Port of Entry Inspection Process



Source: GAO adaptation of INS data.

At primary inspection, the INS inspector either permits travelers to enter or refers them to secondary inspection, where a more detailed review of the travel documents or further questioning can be conducted by another INS inspector. People may be refused entry for the same reasons they can be denied a visa. For U.S. citizens, once an inspector is convinced that a traveler is a citizen, the inspection is considered complete for immigration

purposes. However, checks can still be conducted to determine whether the person is wanted by law enforcement authorities.

Overall, in fiscal year 2001, about 1.7 percent of travelers entering the United States were referred to secondary inspection. Of those referred, about 8 percent were denied admission to the United States. The numbers in fiscal year 2001 were

- primary inspections: 505,916,147,
- secondary inspections: 8,838,624, and
- travelers denied admission: 707,920.

At air ports of entry, commercial carriers are required to submit passenger and crew manifests to INS through the Advance Passenger Information System (APIS) for flights into the United States. For each passenger, the first and last name, date of birth, nationality, and passport number are transmitted. With information from APIS, INS passenger analysis units can analyze intelligence on passengers before flights arrive and identify passengers who will require referral to secondary inspection.

Primary inspectors are to examine travel documents from all travelers at air ports of entry. A name check is also to be conducted on all travelers, using the Interagency Border Inspection System (IBIS). Machine-readable passports are read with IBIS; the primary inspector manually types in the names of travelers who do not have machine-readable passports. IBIS is a multiagency database of lookout information that alerts inspectors of conditions that may make travelers inadmissible to the United States. It also provides information about warrants for U.S. citizens who may be wanted by U.S. law enforcement agencies. IBIS contains data from law enforcement and other agencies with inspection responsibilities at the ports of entry, including the Animal Plant Health Inspection Service, the Drug Enforcement Administration, and the Federal Bureau of Investigation (FBI).

At sea ports of entry, some commercial carriers submit passenger manifests to INS through APIS before docking.[8] As at airports, INS's

[8]In January 2003, INS plans to publish regulations in response to the Enhanced Border Security and Visa Entry Reform Act to mandate electronic manifest transmission from carriers at air and sea ports of entry for all arriving and departing passengers.

passenger analysis units identify passengers who require further examination when they enter the United States. At sea ports of entry equipped with IBIS, the operation is very similar to that at an airport. However, at most sea ports of entry, inspections are conducted aboard a vessel. When the vessel docks, it is sealed so that no goods or persons can be offloaded until it has been inspected.

INS inspectors board ships with the Portable Automated Lookout System (PALS) housed on a laptop computer. PALS contains lookout information but does not have as many records as IBIS and is not updated as often. INS inspectors use PALS to perform name checks and examine documents of all aliens aboard a vessel. For U.S. citizens, only documents are checked. The inspection process on some of the larger cruise ships can take up to 6 hours to complete.

At land ports of entry, the procedures differ for pedestrians and those in vehicles. In addition, at land ports, INS shares primary inspection responsibilities with the Customs Service of the Treasury Department. INS and Customs inspectors are cross-designated to perform each other's primary inspection duties so that either inspector may conduct the primary inspection, following both INS and Customs procedures. INS has established procedures to examine travelers expeditiously at many land ports of entry because of the large volume of traffic at land crossings. Figure 7 shows vehicles waiting at a U.S. land port of entry.

Figure 7: Motor Vehicles Waiting for Inspection at the Paso del Norte Port of Entry, El Paso, Texas



Source: GAO.

For pedestrians at land ports of entry, generally all travelers' documents are to be checked. If IBIS is available, a traveler's name is either machine-read from the machine-readable passport or manually keyed in by an inspector. U.S. citizens are not required to have a passport when entering at a land port. Usually, they need only make an oral declaration of U.S. citizenship. Similarly, at land ports of entry, Canadians are not required to have a passport. Mexicans who possess a border crossing card are not required to present either a Mexican passport or a U.S. visa.[9] Approximately 5 million border crossing cards have been issued to Mexican nationals.

For vehicles at land ports of entry, license plates of all vehicles are to be checked through IBIS. Some ports are equipped with automated license plate readers. At others, an inspector manually keys license plate

[9]A Mexican border crossing card permits the holder to enter for business or pleasure and stay in the United States for 72 hours or less, going no farther than 25 miles from the border.

information into IBIS as vehicles approach the inspection booth. As with a name check, IBIS contains lookout information that alerts inspectors of conditions that may make the occupants of a vehicle inadmissible. Documents and names of the vehicle's occupants are checked randomly or when an inspector suspects that something is wrong. Figure 8 shows a driver being questioned at a land port of entry.

Figure 8: A Driver Being Questioned at a Port of Entry



Source: U.S. Customs Service.

At land borders, aliens who require additional documentation, such as an Arrival/Departure Record, are to be referred to secondary inspection and queried through IBIS. This includes aliens in possession of a nonimmigrant visa and those traveling under the visa waiver program.

Some land ports of entry have implemented a program called Secure Electronic Network for Travelers Rapid Inspection (SENTRI) to expedite the inspection of vehicles and their occupants. With SENTRI, border crossers register their vehicles and up to eight occupants, who are checked against the IBIS database. Vehicles are identified when approaching a SENTRI-equipped port of entry, using a transponder installed on the vehicles. Pictures taken of each potential vehicle occupant at registration are presented to the primary inspector on a computer

screen in the inspection booth when a vehicle drives up. The inspector visually compares the pictures against the people in the vehicle. SENTRI has reduced the average inspection time for each vehicle to about 10 seconds from the earlier 30 to 40 seconds.

Similar to SENTRI, other vehicle ports of entry have implemented a program called NEXUS that is run jointly by the United States and Canada. Instead of issuing a transponder to a vehicle, a proximity card is issued to each registered traveler that is detected as a vehicle approaches the inspection booth of a NEXUS-equipped port of entry. Photographs of travelers detected by their proximity cards are presented to the primary inspector, who can then verify the identity of each vehicle's occupants.

Regardless of the method of entry, secondary inspection gives inspectors more time with travelers to determine their admissibility than primary inspection. In deciding whether to admit a traveler, the inspector reviews the traveler's documents for accuracy and validity and checks INS's and other agencies' databases for any information that could affect the traveler's entry, including criminal history information from the FBI and nonimmigrant visa issuance data from the State Department. A fingerprint identification system is also available in secondary inspection to determine whether INS has apprehended the person for immigration offenses or whether other law enforcement agencies are looking for the person.

Chapter 3: Biometric Technologies for Personal Identification

In this chapter, we define biometrics and explain how they work, describe leading and emerging biometrics, and briefly introduce a few of the most common applications of biometric technologies. In considering how to apply biometrics to border control, we summarize data related to accuracy, the lack of applications-dependent evaluations, systems' susceptibility to deception, the status of standards, and users' acceptance. After briefly comparing performance data on the technologies now considered most viable for U.S. border control—facial, fingerprint, and iris recognition and hand geometry—we end the chapter with a short list of biometric systems in border control situations today, here and in other countries.

Biometrics Defined

When used for personal identification, biometric technologies measure and analyze human physiological and behavioral characteristics. Identifying a person's physiological characteristics is based on direct measurement of a part of the body—fingertips, hand geometry, facial geometry, and eye retinas and irises. The corresponding biometric technologies are fingerprint recognition, hand geometry, and facial, retina, and iris recognition. Identifying behavioral characteristics is based on data derived from actions, such as speech and signature, the corresponding biometrics being speaker recognition and signature recognition.

Biometrics are theoretically very effective personal identifiers because the characteristics they measure are thought to be distinct to each person. Unlike conventional identification methods that use something you have, such as an identification card to gain access to a building, or something you know, such as a password to log on to a computer system, these characteristics are integral to something you are. Because they are tightly bound to an individual, they are more reliable, cannot be forgotten, and are less easily lost, stolen, or guessed.

How the Technologies Work

Biometric technologies vary in complexity, capabilities, and performance, but all share several elements. Biometric identification systems are essentially pattern recognition systems. They use acquisition devices such as cameras and scanning devices to capture images, recordings, or measurements of an individual's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics. Because the process is automated, biometric decision making is generally very fast, in most cases taking only a few seconds in real time.

Depending on the application, biometric systems can be used in one of two modes: verification or identification. Verification—also called authentication—is used to verify a person's identity—that is, to authenticate that individuals are who they say they are. Identification is used to establish a person's identity—that is, to determine who a person is. Although biometric technologies measure different characteristics in substantially different ways, all biometric systems involve similar processes that can be divided into two distinct stages: enrollment and verification or identification.

Enrollment

In enrollment, a biometric system is trained to identify a specific person. The person first provides an identifier, such as an identity card. The biometric is linked to the identity specified on the identification document. He or she then presents the biometric (e.g., fingertips, hand, or iris) to an acquisition device. The distinctive features are located; one or more samples are extracted, encoded, and stored as a reference template for future comparisons. Depending on the technology, the biometric sample may be collected as an image, a recording, or a record of related dynamic measurements. How biometric systems extract features and encode and store information in the template are based on the system vendor's proprietary algorithms.

Template size also varies, depending on the vendor and the technology. Although templates can range from 9 to 20,000 bytes, most are smaller than 1,000 bytes. Such small sizes allow for rapid comparison. Templates can be stored remotely in a central database or within a biometric reader device itself; their small size also allows for storage on smart cards or tokens.

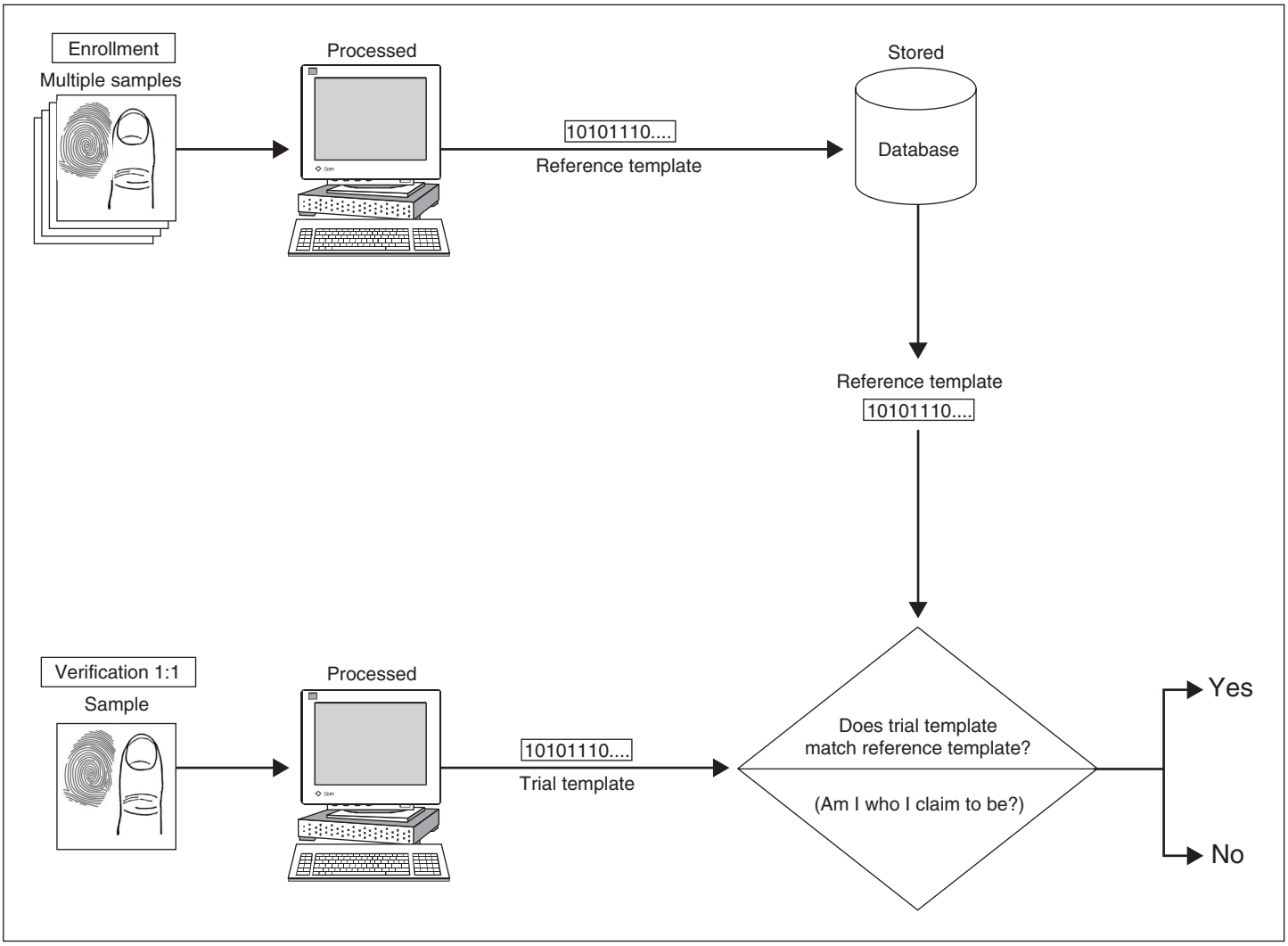
Minute changes in positioning, distance, pressure, environment, and other factors influence the generation of a template, making each template likely to be unique, each time an individual's biometric data are captured and a new template is generated. Consequently, depending on the biometric system, a person may need to present biometric data several times in order to enroll. Either the reference template may then represent an amalgam of the captured data or several enrollment templates may be stored. The quality of the template or templates is critical in the overall success of the biometric application. Because biometric features can change over time, people may have to reenroll to update their reference template. Some technologies can update the reference template during matching operations.

The enrollment process also depends on the quality of the identifier the enrollee presents. The reference template is linked to the identity specified on the identification document. If the identification document does not specify the individual's true identity, the reference template will be linked to a false identity.

Verification

In verification systems, the step after enrollment is to verify that a person is who he or she claims to be (i.e., the person who enrolled). After the individual provides whatever identifier he or she enrolled with, the biometric is presented, which the biometric system captures, generating a trial template that is based on the vendor's algorithm. The system then compares the trial biometric template with this person's reference template, which was stored in the system during enrollment, to determine whether the individual's trial and stored templates match (see figure 9).

Figure 9: The Biometric Verification Process



Source: GAO.

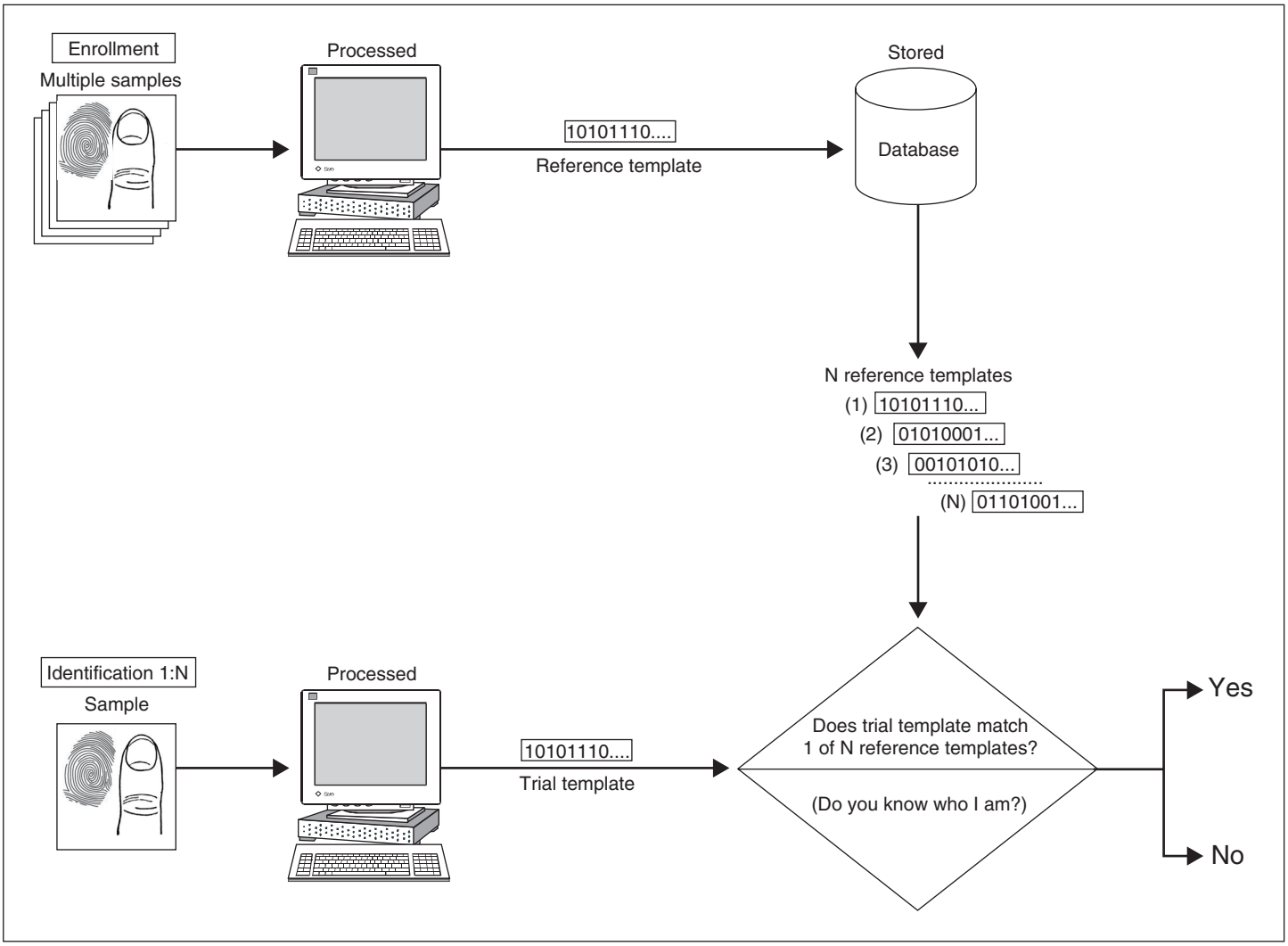
Verification is often referred to as 1:1 (one-to-one) matching. Verification systems can contain databases ranging from dozens to millions of enrolled templates but are always predicated on matching an individual's presented biometric against his or her reference template. Nearly all verification systems can render a match–no-match decision in less than a second. A system that requires employees to authenticate their claimed identities

before granting them access to secure buildings or to computers is a verification application.

Identification

In identification systems, the step after enrollment is to identify who the person is. Unlike verification systems, no identifier need be provided. To find a match, instead of locating and comparing the person's reference template against his or her presented biometric, the trial template is compared against the stored reference templates of all individuals enrolled in the system (see figure 10). Identification systems are referred to as 1:N (one-to-N, or one-to-many) matching because an individual's biometric is compared against multiple biometric templates in the system's database.

Figure 10: The Biometric Identification Process



Source: GAO.

There are two types of identification systems: positive and negative. Positive identification systems are designed to ensure that an individual's biometric is enrolled in the database. The anticipated result of a search is a match. A typical positive identification system controls access to a secure building or secure computers by checking anyone who seeks access against a database of enrolled employees. The goal is to determine whether a person seeking access can be identified as having been enrolled in the system.

Negative identification systems are designed to ensure that a person's biometric information is not present in a database. The anticipated result of a search is a nonmatch. Comparing a person's biometric information against a database of all who are registered in a public benefits program, for example, can ensure that this person is not "double dipping" by using fraudulent documentation to register under multiple identities.

Another type of negative identification system is a surveillance system that uses a watch list. Such systems are designed to identify people on the watch list and alert authorities for appropriate action. For all other people, the system is to check that they are not on the watch list and allow them normal passage. The people whose biometrics are in the database in these systems may not have provided them voluntarily. For instance, for a surveillance system, the biometrics may be faces captured from mug shots provided by a law enforcement agency.

No match is ever perfect in either a verification or an identification system, because every time a biometric is captured, the template is likely to be unique. Therefore, biometric systems can be configured to make a match or no-match decision, based on a predefined number, referred to as a threshold, that establishes the acceptable degree of similarity between the trial template and the enrolled reference template. After the comparison, a score representing the degree of similarity is generated, and this score is compared to the threshold to make a match or no-match decision. For algorithms for which the similarity between two templates is calculated, a score exceeding the threshold is considered a match. For algorithms for which the difference between two templates is calculated, a score below the threshold is considered a match. Depending on the setting of the threshold in identification systems, sometimes several reference templates can be considered matches to the trial template, with the better scores corresponding to better matches.

Leading Biometric Technologies

A growing number of biometric technologies have been proposed over the past several years, but only in the past 5 years have the leading ones become more widely deployed. Some technologies are better suited to specific applications than others, and some are more acceptable to users. Table 5 lists the seven leading biometric technologies we describe in this section.

Table 5: Leading Biometric Technologies and Their Template Size

Technology	How it works	Template size in bytes
Facial recognition	Captures and compares facial patterns	84 or 1,300[a]
Fingerprint recognition	Captures and compares fingertip patterns	250–1,000
Hand geometry	Measures and compares dimensions of hand and fingers	9
Iris recognition	Captures and compares iris patterns	512
Retina recognition	Captures and compares retina patterns	96
Signature recognition	Captures and compares rhythm, acceleration, and pressure flow of signature	1,000–3,000
Speaker recognition	Captures and compares cadence, pitch, and tone of vocal tract	10,000–20,000

[a] Depending on the algorithm.

Source: GAO analysis of manufacturer data.

Facial Recognition

Facial recognition technology identifies people by analyzing features of the face not easily altered—the upper outlines of the eye sockets, the areas around the cheekbones, and the sides of the mouth. The technology is typically used to compare a live facial scan to a stored template, but it can also be used in comparing static images such as digitized passport photographs. Facial recognition can be used in both verification and identification systems. In addition, because facial images can be captured from video cameras, facial recognition is the only biometric that can be used for surveillance purposes.

The two primary algorithms used in facial recognition systems are based on the eigenface method and local feature analysis (LFA). The eigenface method looks at the face as a whole and represents a person's face as a set of templates that require 1,300 bytes. LFA breaks down the face into feature-specific fields, such as the eyes, nose, mouth, and cheeks, creating an 84 byte template.

Fingerprint Recognition

Fingerprint recognition is one of the best known and most widely used biometric technologies. Automated systems have been commercially available since the early 1970s, and there are currently more than 75 fingerprint recognition technology companies. Until recently, it was used primarily in law enforcement applications.

Fingerprint recognition technology extracts features from impressions made by the distinct ridges on the fingertips. The fingerprints can be either flat or rolled. A flat print captures only an impression of the central area

between the fingertip and the first knuckle; a rolled print captures ridges on both sides of the finger.

An image of the fingerprint is captured by a scanner, enhanced, and converted into a template. Scanner technologies can be optical, silicon, or ultrasound technologies. Ultrasound, while potentially the most accurate, has not been demonstrated in widespread use. Optical scanners are the most commonly used. During enhancement, "noise" caused by such things as dirt, cuts, scars, and creases or dry, wet, or worn fingerprints is reduced, and the definition of the ridges is enhanced. Template size ranges from 250 bytes up to 1,000 bytes, depending on which vendor's proprietary algorithm the system uses. Approximately 80 percent of vendors base their algorithms on the extraction of minutiae points relating to breaks in the ridges of the fingertips. Other algorithms are based on extracting ridge patterns.

Hand Geometry

Hand geometry systems have been in use for almost 30 years for access control to facilities ranging from nuclear power plants to day care centers. Hand geometry technology measures the width, height, and length of the fingers, distances between joints, and shapes of the knuckles.

Hand geometry systems use an optical camera and light-emitting diodes with mirrors and reflectors to capture two orthogonal two-dimensional images of the back and sides of the hand. Ninety-six measurements are then extracted and a 9 byte template is derived, making it the smallest in the biometric industry.

Although the basic shape of an individual's hand remains relatively stable over his or her lifetime, natural and environmental factors can cause slight changes.

Iris Recognition

Iris recognition technology is based on the distinctly colored ring surrounding the pupil of the eye. Made from elastic connective tissue, the iris is a very rich source of biometric data, having approximately 266 distinctive characteristics. These include the trabecular meshwork, a tissue that gives the appearance of dividing the iris radially, with striations, rings, furrows, a corona, and freckles. Iris recognition technology uses about 173 of these distinctive characteristics. Formed during the eighth month of gestation, these characteristics reportedly remain stable throughout a person's lifetime, except in cases of injury.

Iris recognition systems use a small, high-quality camera to capture a black-and-white, high-resolution image of the iris. They then define the boundaries of the iris, establish a coordinate system over the iris, and define the zones for analysis within the coordinate system. The visible characteristics within the zones are then converted into a 512 byte template that is used to identify or verify the identity of an individual.

Retina Recognition

Retina recognition technology captures and analyzes the patterns of blood vessels on the thin nerve on the back of the eyeball that processes light entering through the pupil. Retinal patterns are highly distinctive traits. Every eye has its own totally unique pattern of blood vessels; even the eyes of identical twins are distinct. Although each pattern normally remains stable over a person's lifetime, it can be affected by disease such as glaucoma, diabetes, high blood pressure, and autoimmune deficiency syndrome.

The fact that the retina is small, internal, and difficult to measure makes capturing its image more difficult than most biometric technologies. An individual must position the eye very close to the lens of the retina-scan device, gaze directly into the lens, and remain perfectly still while focusing on a revolving light while a small camera scans the retina through the pupil. Any movement can interfere with the process and can require restarting. Enrollment can easily take more than a minute. The generated template is only 96 bytes, one of the smallest of the biometric technologies.

One of the most accurate and most reliable of the biometric technologies, it is used for access control in government and military environments that require very high security, such as nuclear weapons and research sites. However, the great degree of effort and cooperation required of users has made it one of the least deployed of all the biometric technologies. Newer, faster, better retina recognition technologies are being developed.

Signature Recognition

Signature recognition authenticates identity by measuring handwritten signatures. The signature is treated as a series of movements that contain unique biometric data, such as personal rhythm, acceleration, and pressure flow. Unlike electronic signature capture, which treats the signature as a graphic image, signature recognition technology measures how the signature is signed.

In a signature recognition system, a person signs his or her signature on a digitized graphics tablet or personal digital assistant. The system analyzes signature dynamics such as speed, relative speed, stroke order, stroke count, and pressure. The technology can also track each person's natural signature fluctuations over time.

The signature dynamics information is encrypted and compressed into a template that can range from slightly larger than 1,000 bytes to approximately 3,000 bytes. These templates are large by biometric standards and reflect the variety of data available in a typical signature.

Speaker Recognition

Differences in how different people's voices sound result from a combination of physiological differences in the shape of vocal tracts and learned speaking habits. Speaker recognition technology uses these differences to discriminate between speakers.

During enrollment, speaker recognition systems capture samples of a person's speech by having him or her speak some predetermined information into a microphone or telephone a number of times. This information, known as a passphrase, can be a piece of information such as a name, birth month, birth city, or favorite color or a sequence of numbers. Text independent systems are also available that recognize a speaker without using a predefined phrase.

This phrase is converted from analog to digital format, and the distinctive vocal characteristics, such as pitch, cadence, and tone, are extracted, and a speaker model is established. A template is then generated and stored for future comparisons. Voice templates are much larger than templates generated from other biometric technologies, typically 10,000 to 20,000 bytes.

Speaker recognition can be used to verify a person's claimed identity or to identify a particular person. It is often where voice is the only available biometric identifier, such as telephone and call centers.

Emerging Biometric Technologies

Newer biometric technologies using diverse physiological and behavioral characteristics are in various stages of development. Some are commercially available, some may emerge over the next 2 to 4 years, and others are many years from implementation. Table 6 lists the 9 we describe in this section and their current maturity. Each technique's

performance can vary widely, depending on how it is used and its environment in which it is used.

Table 6: Emerging Biometric Technologies and Their Maturity

Technology	How it works	Maturity
Vein scan	Captures images of blood vessel patterns.	Commercially available.
Facial thermography	Infrared camera detects heat patterns created by the branching of blood vessels and emitted from the skin.	Initial commercialization attempts failed because of high cost.
DNA matching	Compares actual samples of DNA rather than templates generated from samples.	Many years from implementation.
Odor sensing	Captures the volatile chemicals that the skin's pores emit.	Years away from commercial release.
Blood pulse measurement	Infrared sensors measure blood pulse on a finger.	Experimental.
Skin pattern recognition	Extracts distinct optical patterns by spectroscopic measurement of light scattered by the skin.	Emerging.
Nailbed identification	An interferometer detects phase changes in back-scattered light shone on the fingernail; reconstructs distinct dimensions of the nailbed and generates a one-dimensional map.	Emerging.
Gait recognition	Captures a sequence of images to derive and analyze motion characteristics.	Emerging; requires further development.
Ear shape recognition	Is based on distinctive ear shape and the structure of the cartilaginous, projecting portion of the outer ear.	Still a research topic.

Source: GAO analysis.

Vein scan biometric technology can automatically identify a person from the patterns of the blood vessels in the back of the hand. The technology uses near-infrared light to detect vein vessel patterns. Vein patterns are distinctive between twins and even between a person's left and right hand. Developed before birth, they are highly stable and robust, changing throughout one's life only in overall size. The technology is not intrusive, and works even if the hand is not clean. It is commercially available.

Facial thermography detects heat patterns created by the branching of blood vessels and emitted from the skin. These patterns, called thermograms, are highly distinctive. Even identical twins have different thermograms. Developed in the mid-1990s, thermography works much like facial recognition, except that an infrared camera is used to capture the images. The advantages of facial thermography over other biometric technologies are that it is not intrusive—no physical contact is required—every living person presents a usable image, and the image can be collected on the fly. Also, unlike visible light systems, infrared systems work accurately even in dim light or total darkness. Although identification systems using facial thermograms were undertaken in 1997, the effort was suspended because of the cost of manufacturing the system.

DNA matching is a type of biometric in the sense that it uses a physiological characteristic for personal identification. It is considered to be the "ultimate" biometric technology in that it can produce proof-positive identification of a person, except in the case of identical twins. However, DNA differs from standard biometrics in several ways. It compares actual samples rather than templates generated from samples. Also, because not all stages of DNA comparison are automated, the comparison cannot be made in real time. DNA's use for identification is currently limited to forensic applications. The technology is many years away from any other kind of implementation and will be very intrusive.

Researchers are investigating a biometric technology that can distinguish and measure body odor. This technology would use an odor-sensing instrument (an electronic "nose") to capture the volatile chemicals that skin pores all over the body emit to make up a person's smell. Although distinguishing one person from another by odor may eventually be feasible, the fact that personal habits such as the use of deodorants and perfumes, diet, and medication influence human body odor renders the development of this technology quite complex.

Blood pulse biometrics measure the blood pulse on a finger with infrared sensors. This technology is still experimental and has a high false match rate, making it impractical for personal identification.

The exact composition of all the skin elements is distinctive to each person. For example, skin layers differ in thickness, the interfaces between the layers have different undulations, pigmentation differs, collagen fibers and other proteins differ in density, and the capillary beds have distinct densities and locations beneath the skin. Skin pattern recognition technology measures the characteristic spectrum of an individual's skin. A light sensor illuminates a small patch of skin with a beam of visible and near-infrared light. The light is measured with a spectroscope after being scattered by the skin. The measurements are analyzed, and a distinct optical pattern can be extracted.

Nailbed identification technology is based on the distinct longitudinal, tongue-in-groove spatial arrangement of the epidermal structure directly beneath the fingernail. This structure is mimicked in the ridges on the outer surface of the nail. When an interferometer is used to detect phase changes in back-scattered light shone on the fingernail, the distinct dimensions of the nailbed can be reconstructed and a one-dimensional map can be generated.

Gait recognition, recognizing individuals by their distinctive walk, captures a sequence of images to derive and analyze motion characteristics. A person's gait can be hard to disguise because a person's musculature essentially limits the variation of motion, and measuring it requires no contact with the person. However, gait can be obscured or disguised if the individual, for example, is wearing loose fitting clothes. Preliminary results have confirmed its potential, but further development is necessary before its performance, limitations, and advantages can be fully assessed.

Ear shape recognition is still a research topic. It is based on the distinctive shape of each person's ears and the structure of the largely cartilaginous, projecting portion of the outer ear. Although ear biometrics appears to be promising, no commercial systems are available.

Common Applications of Biometric Technologies

Reduced cost, smaller size, greater accuracy, and greater ease of use are making biometrics increasingly feasible for international travel documentation, citizenship identification, automated banking, and benefits dispersal. Biometrics have either been adopted or are being contemplated for adoption in dozens of applications, ranging from modest—providing time and attendance reports for small companies—to expansive—ensuring the integrity of a registration database of 10 million voters.

Access Control

Biometric systems have long been used to complement or replace badges and keys in controlling access to entire facilities or specific areas within a facility. The entrances to more than half the nuclear power plants in the United States employ biometric hand geometry systems. They protected athletes housed in Olympic Village at the 1996 games in Atlanta.

Recent reductions in the price of biometric hardware have spurred logical access control applications. Fingerprint, iris, and speaker recognition are replacing passwords to authenticate individuals accessing computers and networks. The Office of Legislative Counsel of the U.S. House of Representatives, for example, is installing an iris recognition system to protect confidential files and working documents. Other federal agencies, including the Department of Defense (DOD), Department of Energy, and Department of Justice, as well as the intelligence community, are adopting similar technologies.

Fraud Reduction

Leading banks and other financial service companies are experimenting with facial, iris, and speaker recognition systems to authenticate ATM users and to combat credit and debit card fraud. Hand geometry and iris and facial recognition have been deployed at ATMs in North America, Europe, and Asia. The JPMorgan Chase Bank allows some customers to access accounts by speaker recognition. To address concerns about security and fraud, organizations that offer Internet shopping are also considering biometric technologies to authorize various types of transactions.

Biometrics can also be used in monitoring applications. Adding biometrics to time and attendance processes, for example, helps prevent hourly employees from punching time cards for their absent friends, a practice that is estimated to cost employers hundreds of millions of dollars annually. Biometrics are also being applied to prevent prison inmates from swapping identities with visitors as they leave prisons.

In addition, biometric technologies are being used in large-scale identification systems to determine whether applicants are already enrolled under a different identity. One specific application has been to prevent individuals from cheating public sector benefits programs by collecting benefits under multiple identities. A number of states have made fingerprinting a requirement for registration for welfare and other types of public aid. Since biometric systems were deployed, the number of individuals claiming benefits has dropped dramatically in several states that use such systems. Internationally, in the Philippines, South Africa, and Spain, programs to streamline or legitimize issuing government benefits have enrolled millions of citizens.

Licensing and Voter Applications

Several states have implemented biometric systems to stop drivers, particularly truck drivers, from maintaining duplicate licenses or swapping licenses when crossing state lines or national borders. Large-scale identification systems are also being used to register voters for national and local elections to prevent voter fraud. Mexico, for example, uses facial recognition technology to check voter rolls for duplicates in its national elections. Brazil, Costa Rica, the Dominican Republic, Panama, and Italy use fingerprints to verify voters at polling stations.

Criminal Identification and Surveillance

Criminal identification is far and away the oldest, most widespread, large-scale identification use of biometric systems. Automated fingerprint recognition systems are employed around the world to identify suspects

within local, state, or federal databases of known offenders. Facial recognition is also being used for criminal identification, although the technology does not provide the same high degree of accuracy as the older technology. Employee background checks are another application of large-scale systems. The governments of Argentina, China, Nigeria, and Yemen are all planning to implement biometrics in their national identification programs.

Surveillance is one of the most recent applications of biometric systems. Although the majority of the major casinos in North America have deployed facial recognition surveillance systems for some time to spot known cheaters, systems are now publicly deployed in Newham Borough, England; Tampa, Florida; and Canada's Lester B. Pearson International Airport in Toronto. More recently, they have been used sporadically at such major events as the 2001 Super Bowl in Tampa, Florida, and the winter Olympics at Salt Lake City in 2002.

Performance Issues

Biometric technologies are maturing but are still not widespread or pervasive because of performance issues, including accuracy, the lack of applications-dependent evaluations, their potential susceptibility to deception, the lack of standards, and questions of users' acceptance. These issues should be kept in mind when considering biometrics for U.S. border control.

Accuracy

Biometrics is a very young technology, having only recently reached the point at which basic matching performance can be acceptably deployed. It is necessary to analyze several metrics to determine the strengths and weaknesses of each technology and vendor for a given application.

The three key performance metrics are false match rate (FMR), false nonmatch rate (FNMR), and failure to enroll rate (FTER). A false match occurs when a system incorrectly matches an identity, and FMR is the probability of individuals being wrongly matched. In verification and positive identification systems, authorized people can be granted access to facilities or resources as the result of incorrect matches. In a negative identification system, the result of a false match may be to deny access. For example, if a new applicant to a public benefits program is falsely matched with a person previously enrolled in that program under another identity, the applicant may be denied access to benefits. The FMR, sometimes called the false positive rate, is sometimes confused with the false accept rate. The FMR is the probability of an erroneous match in a

single template comparison while the false accept rate is a system measure that a person is erroneously matched, combining the results of all template comparisons. For example, in an identification match, the FMR would be the probability that the trial template erroneously matches a single selected reference template. The false accept rate would be the probability that the trial template erroneously matches any of the reference templates.

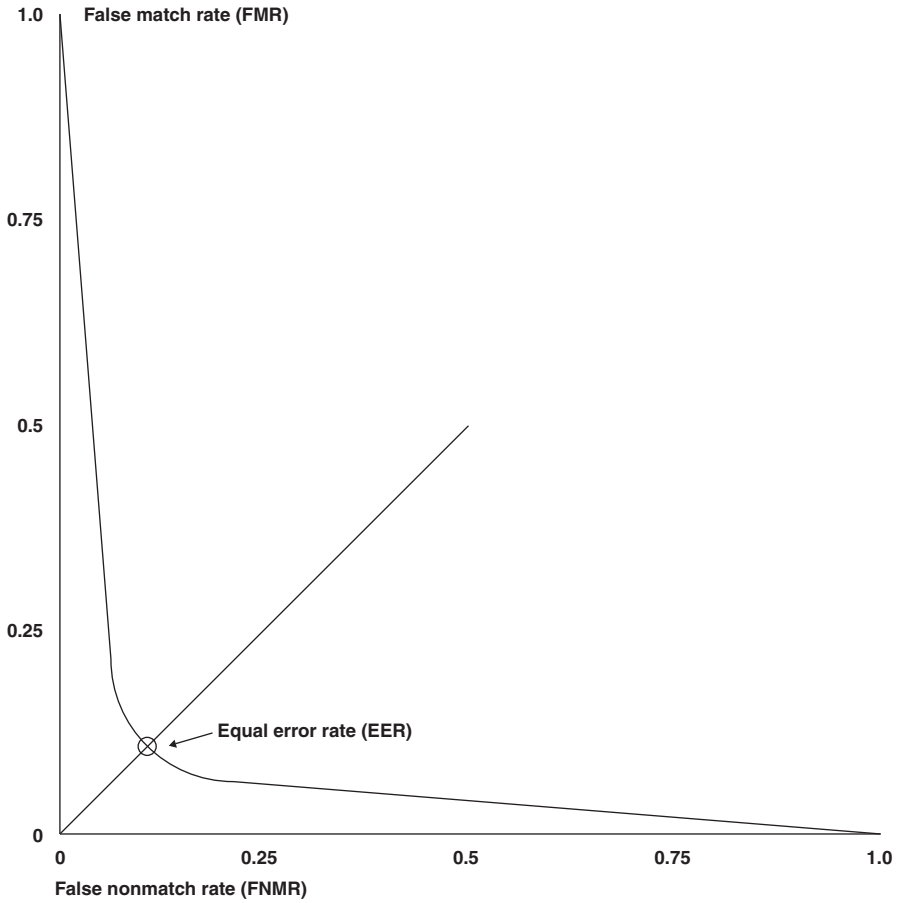
A false nonmatch occurs when a system rejects a valid identity, and FNMR is the probability of valid individuals being wrongly not matched. In verification and positive identification systems, people can be denied access to some facility or resource as the result of a system's failure to make a correct match. In negative identification systems, the result of a false nonmatch may be that a person is granted access to resources to which she should be denied. For example, if a person who has enrolled in a public benefits program under another identity is not correctly matched, she will succeed in gaining fraudulent access to benefits. The FNMR, sometimes called the false negative rate, is sometimes confused with the false reject rate. The relationship between FNMR and the false reject rate is similar to the relationship between the FMR and the false accept rate. The FNMR is the probability of an erroneous nonmatch for a single template comparison, while the false reject rate is a system measure that a person is erroneously not matched, combining the results of all template comparisons.

False matches may occur because there is a high degree of similarity between two individuals' characteristics. False nonmatches occur because there is not a sufficiently strong similarity between an individual's enrollment and trial templates, which could be caused by any number of conditions. For example, an individual's biometric data may have changed as a result of aging or injury. If biometric systems were perfect, both error rates would be zero. However, because biometric systems cannot identify individuals with 100 percent accuracy, a trade-off exists between the two.

False match and nonmatch rates are inversely related; they must therefore always be assessed in tandem, and acceptable risk levels must be balanced with the disadvantages of inconvenience. For example, in access control, perfect security would require denying access to everyone. Conversely, granting access to everyone would result in denying access to no one. Obviously, neither extreme is reasonable, and biometric systems must operate somewhere between the two.

For most applications, how much risk one is willing to tolerate is the overriding factor, which translates into determining the acceptable FMR. The greater the risk entailed by a false match, the lower the tolerable FMR. For example, an application that controlled access to a secure area would require that the FMR be set low, which would result in a high FNMR. However, an application that controlled access to a bank's ATM might have to sacrifice some degree of security and set a higher FMR (and hence a lower FNMR) to avoid the risk of irritating legitimate customers by wrongly rejecting them. This is displayed in figure 11.

Figure 11: The General Relationship between FMR and FNMR



Note: Equal error rate is the point at which FMR equals FNMR.

Source: GAO.

As figure 11 shows, selecting a lower FMR increases the FNMR. Perfect security would require setting the FMR to 0, in which case the FNMR would be 1. At the other extreme, setting the FNMR to 0 would result in an FMR of 1.

The expectations regarding FMR and FNMR are very different for verification and identification systems. In a verification system, a user is checked against one or a few reference templates to confirm the user's claimed identity. A much higher standard is required for identification systems where checks are made against all reference templates in the database. Consequently, a much lower FMR is required for a large-scale positive identification system than for a similar size verification system, simply because even a small percentage of false matches for a system that performed billions of comparisons a day would overwhelm the resources dedicated to investigating positive matches. The larger the identification database, the lower the false match rate needs to be to maintain the number of false positives at a manageable amount.

Vendors often use equal error rate (EER), an additional metric derived from FMR and FNMR, to describe the accuracy of their biometric systems. EER refers to the point at which FMR equals FNMR (see figure 11). Setting a system's threshold at its EER will result in the probability that a person is falsely matched equaling the probability that a person is falsely not matched. However, this statistic tends to oversimplify the balance between FMR and FNMR, because in few real-world applications is the need for security identical to the need for convenience.

FTER is a biometric system's third critical accuracy metric. FTER measures the probability that a person will be unable to enroll. Failure to enroll (FTE) may stem from an insufficiently distinctive biometric sample or from a system design that makes it difficult to provide consistent biometric data. The fingerprints of people who work extensively at manual labor are often too worn to be captured. A high percentage of people are unable to enroll in retina recognition systems because of the precision such systems require. People who are mute cannot use voice systems, and people lacking fingers or hands from congenital disease, surgery, or injury cannot use fingerprint or hand geometry systems. Although between 1 and 3 percent of the general public does not have the body part required for using any one biometric system, they are normally not counted in a system's FTER.

Multimodal Biometrics

Because biometric systems based solely on a single biometric may not always meet performance requirements, the development of systems that integrate two or more biometrics is emerging as a trend. Multiple biometrics could be two types of biometrics, such as combining facial and iris recognition. Multiple biometrics could also involve multiple instances of a single biometric, such as 1, 2, or 10 fingerprints, 2 hands, and 2 eyes. One prototype system integrates fingerprint and facial recognition technologies to improve identification. A commercially available system combines face, lip movement, and speaker recognition to control access to physical structures and small office computer networks. Depending on the application, both systems can operate for either verification or identification. Experimental results have demonstrated that the identities established by systems that use more than one biometric could be more reliable, be applied to large target populations, and improve response time.

The Lack of Applications-Dependent Evaluations

Biometric companies have primarily been concerned with testing the accuracy of their technologies in highly controlled environments, using static or artificially generated templates, images, and data. The results of their tests, as quoted by vendors, are quite extraordinary, such as claims of FMRs of 1 in 100,000, 1 in a billion, or even 1 in 10^{78} and FNMRs in the vicinity of 1 percent, 0.1 percent, and 0.01 percent. However, because the performance of a technology depends greatly on how and where it is deployed, such numbers have proven to be far more impressive than real-life performance data.

Until recently, there was no set methodology for testing the same technologies in different applications. A recently developed methodology uses a three-step evaluation protocol: a technology evaluation, followed by a scenario evaluation and an operational evaluation of biometric systems.[1] Each of the methodology's three types of evaluation requires a different protocol and produces different results. A technology evaluation compares competing algorithms from a single technology to identify the most promising approaches. A scenario evaluation tests overall system performance for a class of applications under conditions that model real-world applications. An operational evaluation measures performance for a specific biometric system for a specific application in the actual operating environment with actual users of the system. The Facial Recognition

[1]P. Jonathon Phillips and others, "An Introduction to Evaluating Biometric Systems," *IEEE Computer* 33:2 (2000): 56–63.

Vendor Test 2000 (FRVT 2000), which assessed the capabilities of commercially available facial recognition systems, was based on this evaluation methodology and included elements of technology and scenario evaluations.[2]

Studies by respected organizations in the United States and the United Kingdom have provided a number of effective measures of the actual performance of biometric systems in different real-world environments. Sandia National Laboratories' 1996 evaluation of an iris recognition identification system in an access-control environment included FNMR-FMR results. The International Biometric Group (IBG) has since 1999 conducted side-by-side comparative performance testing of leading biometric identity verification systems under real-world operating conditions. Test results have included FNMRs, FMRs, and FTERs for fingerprint, iris, facial, voice, keystroke, and signature systems. In 2000, the British National Physical Laboratory (NPL) tested biometric identity verification systems, including fingerprint, hand, iris, facial, voice, and vein, in real-world environments.[3] FNMRs, FMRs, and FTERs were reported. The U.S. Army Research Laboratory's pilot study of iris and facial recognition systems in 2000–01 reported performance results that included error rates as well as user perception and acceptability. Table 7 lists the significant independent tests and their results since 1991.

[2]FRVT 2000 was sponsored by the DOD Counterdrug Technology Development Program Office, Defense Advanced Research Projects Agency, and National Institute of Justice. The test goals were to know the strengths and weaknesses of each individual system, understand the current state of the art for facial recognition, and educate the community and general public on how to present and analyze results.

[3]NPL in the United Kingdom is analogous to the National Institute of Standards and Technology (NIST) in the United States.

Table 7: Independent Biometric Test Results, 1991–2002

Test name	Who conducted	Date	Technology	Type	Performance measure
Test of Biometric Technologies	Sandia National Laboratories	1991	Fingerprint, hand, retina, signature, speaker	Technology	FMR, FNMR, accept time
Hand Geometry Field Application	Sandia National Laboratories	1995	Hand	Scenario	Varied lighting, maintenance
IriScan Prototype Identifier	Sandia National Laboratories	1996	Iris	Scenario	FMR, FNMR, enrollment time, transaction time
Speaker Recognition Evaluations	National Institute of Standards and Technology	1996 to present	Speaker	Technology	Handset variation, test segment duration, speaker tracking, 1-speaker and 2-speaker, cellular data
Philippine AFIS Benchmark Test	National Biometric Test Center	1997	Fingerprint	Technology	FMR, FNMR
SENTRI Test	INS	1998	Facial, speaker	Scenario	FNMR
Comparative Biometric Testing	IBG	1999 to present	Facial, fingerprint, iris, keystroke, signature, speaker	Scenario	FMR, FNMR, enrollment rate, ergonomics, ease of use, temporal
Biometric Product Testing	NPL	2000	Facial, fingerprint, hand, iris, vein, speaker	Scenario	Failure to enroll and acquire, FMR, FNMR, transaction time, male versus female
FRVT 2000	DOD, National Institute of Justice, NIST	2000	Facial	Scenario, technology	Probability of identity, probability of verification, distance, temporal, expressions, pose, resolution, media
Fingerprint Verification Competition 2000	University of Bologna, Michigan State University, San Jose State University	2000	Fingerprint	Technology	Enrollment time, matching time, EER
Facial Recognition Technology	Department of State, Bureau of Consular Affairs	2001	Facial	Technology	FNMR
Personnel Identification Pilot Study	Army Research Laboratory	2001	Facial, iris	Operational	FMR, FNMR
Fingerprint Identification Device	Federal Aviation Administration and Safe Skies	2001	Fingerprint	Operational	FMR, FNMR, enrollment and transit time, abnormal conditions (oil, grease, powder, injury, moist or dry skin, offset angle, contact pressure, backlighting, attempts to defeat)
Hand Geometry Identification Device	FAA and Safe Skies	2001	Hand	Operational	FMR, FNMR, enrollment and transit time, abnormal conditions (rings, injuries, backlighting, attempts to defeat)

Test name	Who conducted	Date	Technology	Type	Performance measure
Facial Recognition Device	FAA and Safe Skies	2002	Facial	Operational	FMR, FNMR, enrollment and transit time, abnormal conditions (glasses, facial hair, backlighting, bandages, false photograph)
Iris Recognition Device	FAA and Safe Skies	2002	Iris	Operational	FTE, FNMR, enrollment and transit times
Biometric Security Test	*c't Magazine*	2002	Iris, fingerprint, facial	Technology	Attempts to defeat
Fingerprint Verification Competition 2002	University of Bologna, Michigan State University, San Jose State University	2002	Fingerprint	Technology	Enrollment time, matching time, EER, FMR
Facial Recognition Vendor Test 2002	15 agencies and organizations, including DOD, National Institute of Justice, and NIST	In progress	Facial	Scenario, technology	In progress

Source: GAO analysis of independent biometric test results.

A rash of new tests of biometric systems has recently been initiated. The results are likely to provide more sound means of evaluating the strengths and weaknesses of the different technologies and vendors' products.

Susceptibility to Deception

Can biometric systems be defeated? Many vendors claim that their systems cannot be fooled because they are able to detect whether or not an individual's presented biometric is a live sample. Many biometric devices can, in principle, determine whether a live characteristic is being presented. Some fingerprint systems, for example, test for "liveness" by relying on the unique conductive nature of live fingers. Others measure blood flow or ensure that the ridges at the periphery of a print are arrayed the same as in normal finger placement.

Although hand geometry systems do not actually check for a live biometric, fingers have to be positioned so that they put pressure on the correct pegs. Facial recognition checks for "liveness" by requiring users to change their facial expression—by blinking their eyes or smiling, for example—in order to successfully generate a template. With iris recognition, light shone on the eye can be varied for recording pupil dilation. Some speaker recognition systems can generate a random sequence of numbers for each verification to ensure that a recorded voice is not being played back. Moreover, low-fidelity recording devices are generally not able to capture the high and low frequencies necessary for verification.

Nevertheless, recent tests are casting doubt on vendors' claims regarding the maturity and security of their technologies. German technology magazine *c't* carried out tests on 11 commercially available biometric systems used to control access to computers.[4] Facial, fingerprint, and iris recognition systems were defeated by testers using photographs and videos, reactivated latent images, and forgeries.

They spoofed one fingerprint recognition system by reactivating latent fingerprints left on the surface of its capacitive sensor, simply by breathing on the prints, placing a thin-walled water-filled plastic bag on the sensor's surface, and dusting the prints with graphite powder and gently applying pressure to an adhesive film stretched over them. They outfoxed another fingerprint recognition system whose optical scanner required that an object be resting on its surface by creating a silicone copy of a fingerprint of an enrolled person from a candle wax mold.

They spoofed an iris recognition system by using a high-resolution printed picture of an enrolled person's iris with a live person's pupil shining through a miniature hole cut out of the picture's pupil. They beat a well-known facial recognition system by using a laptop computer to play back "live" images of an enrolled person to the camera. They fooled another facial system by holding up a photograph of an enrolled person.

In another recent test, an engineering professor demonstrated how 11 commercially available fingerprint biometric systems could all be fooled with a molded gelatin finger. A further recent test revealed that biometric systems could be defeated by cracking the code of the templates stored inside them. Using manufactured images that displayed the characteristics required by the matching software, the tester defeated commercially available fingerprint and retina recognition systems. These tests certainly call into question the claim that biometric systems cannot be deceived.

The Development of Biometric Standards

Identifying, exchanging, and integrating information from different and perhaps unfamiliar sources and functions are essential to an effective biometrics application. Without predefined standards, system developers may need to define in detail the precise steps for exchanging information,

[4]Lisa Thalheim, Jan Krissler, and Peter-Michael Ziegler, "Body Check: Biometric Access Protection Devices and Their Programs Put to the Test," trans. Robert Smith, *c't Magazine* 11 (2002): 114.

a potentially complex, time-consuming, and expensive process. The risks associated with not adopting standards for a system are significant, because of the length of time the system must remain operational and the rapid pace of technological change. The proprietary technology of choice today may not be cost-effective or even supported tomorrow.

Attempts to standardize biometrics are under way in various areas, such as the mechanics of image capture, the accuracy of data as they are extracted, and device interoperability. However, the majority of biometric devices and their software are still proprietary in many respects. For example, the method for extracting features from a biometric sample such as a fingerprint differs among most, if not all, vendors. Templates containing biometric data, time stamps, encryption features, and device information are also not standard. Devices from company A do not necessarily work compatibly with devices from companies B and C. Incompatibility is also an issue for communication between devices and host computers, since programs are developed from vendors' software development kits. Each vendor designs a software development kit for its own products, so that the programs developed for one vendor's product generally cannot be used with another vendor's products.

The biometrics community does employ several standards, however. We list seven:

- The wavelet scalar quantization (WSQ) gray-scale fingerprint image compression algorithm is the standard for exchanging fingerprint images within the criminal justice community. WSQ defines a class of encoders and a single decoder with sufficient generality to decode compressed image data produced by any compliant encoder.

- The National Institute of Standards and Technology (NIST) issued the Common Biometric Exchange File Format (CBEFF) on January 3, 2001. The standard is designed to (1) facilitate biometric data interchange between different system components or between systems, (2) promote the interoperability of biometric-based application programs and systems, (3) provide forward compatibility for technology improvements, and (4) simplify the integration of software and hardware from different vendors.

- BioAPI™ Consortium has developed BioAPI, a specification for a high-level generic biometric authentication model suited for any form of biometric technology. It covers the basic functions of enrollment, verification, and identification and includes a database interface to

allow a biometric service provider to manage the identification population for optimum performance. It also provides methods that allow an application to manage the capture of samples on a client and the enrollment, verification, and identification on a server. While it does not define security requirements for biometric applications and service providers, it does explain how the application programming interface (API) is intended to support good security practices.

- In May 2000, Microsoft Corp. and I/O Software Inc. announced that they would cooperate to foster the widespread growth of biometrics through the integration of biometric authentication technology in future versions of the Microsoft Windows operating system. The resulting biometric application programming interface (BAPI) is expected to define a standard software protocol and API for communication between software applications and biometric devices running on Microsoft Windows platforms. BAPI is expected to standardize the way different biometric devices, such as fingerprint scanners and facial recognition devices, communicate with the application software that uses them. It is also expected to be a comprehensively modular architecture that covers a variety of hardware interfaces, encryption, biometric algorithms, and application interfaces.

- Established by the Joint Photographic Experts Group (JPEG), the JPEG specification can be used in facial recognition systems.[5] It describes an image compression system that allows great flexibility not only for the compression of images but also for access to the compressed data. The specification is designed for compressing either full-color or gray-scale images of natural, real-world scenes, although the decompressed images are not quite the same as the originals. JPEG's algorithm is designed to exploit known limitations of the eye, notably that the eye perceives small color changes less accurately than small changes in brightness. This is a limitation if an application uses a JPEG image to machine-analyze images, since the small errors JPEG introduces may be a problem even if they are invisible to the eye.[6]

[5]JPEG members are experts nominated by national standards bodies and major companies to produce standards for continuous tone image coding. "Joint" refers to the group's status as a committee working on standards for both the International Organization for Standardization and International Telecommunication Union–Telecommunication.

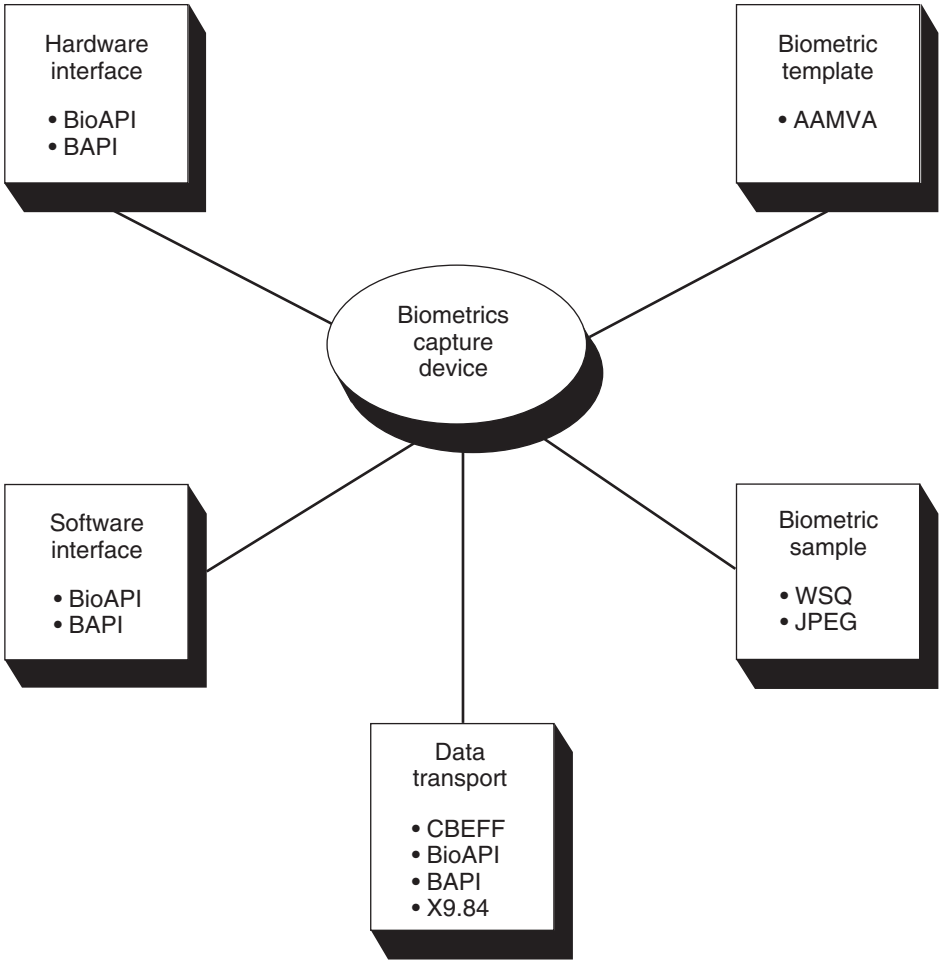
[6]According to a February 2001 study conducted for the FBI, WSQ and JPEG 2000 formats are similar enough that questions may emerge about migration of the FBI standard to the JPEG 2000 standard. Such questions would include weighing some advantages against other disadvantages of changing an accepted standard that is already widely used.

- In February 2001, the American National Standards Institute (ANSI) approved the Biometric Information Management and Security (ANSI X9.84-2001) standard. This standard specifies the minimum security requirements for effective management of biometric data. The standard defines message formats for carrying biometric data in a secure way and also defines many concepts and procedures for the creation of a secure biometric system. The message formats specified by X9.84 are more flexible than the BioAPI data format because they allow a richer description of the biometric data and are extensible. Moreover, the X9.84 standard addresses the issue of integrity and privacy of biometric samples and templates in a flexible way, by providing several different security mechanisms among which the user can choose.

- The American Association for Motor Vehicle Administration (AAMVA) included a format for fingerprint minutiae data in its Driver License and Identification (DL/ID-2000) Standard, which provides a uniform means to identify issuers and holders of driver's license cards within the United States and Canada. The standard describes required and optional data elements to be placed on a driver's license card. Required elements include the name, address, and photograph of the driver. While fingerprints are classified as an optional data element, the standard describes a way to record minutiae data based on the type, position, angle, and quality of the minutiae point. A field is also provided for recording vendor-specific data about the fingerprint. The biometric portions of this standard are compatible with the BioAPI specification and CBEFF.

Figure 12 shows the relationship of these standards to the individual functional components necessary to make up a comprehensive biometric system.

Figure 12: Standards for Biometric Systems



Note: AAMVA = The American Association for Motor Vehicle Administration's Driver License and Identification (DL/ID-2000) Standard. WSQ = wavelet scalar quantization. JPEG = a specification of the Joint Photographic Experts Group. CBEFF = the National Institute of Standards and Technology's Common Biometric Exchange File Format. BioAPI = the BioAPI™ Consortium's BioAPI specification for a high-level generic biometric authentication model. BAPI = biometric application programming interface. X9.84 = the American National Standards Institute's ANSI X9.84-2001 standard.

Source: GAO analysis of biometric standards.

Although a number of such standards have been developed, those required for integrating all vendors' products are not yet available for all types of applications. For example, the standard for how to store biometric templates is not yet available. While the AAMVA standard describes a common way to record fingerprint minutiae, it still allows for including

data in a vendor-specific format. Biometric templates, which capture only the critical data needed to make a positive confirmation, are small and can be stored on smart cards, but the template one vendor uses cannot generally be used by another for some biometric technologies, such as fingerprints. Working with other groups—the Biometric Consortium, the BioAPI™ Consortium, the Biometric Foundation, and the International Biometric Industry Association (IBIA), among others—the InterNational Committee for Information Technology Standards (INCITS) is reviewing draft project proposals for standardizing biometric templates.[7] Without a biometric template standard, it could be necessary to store the larger biometric sample as well as the biometric template for each user during enrollment. Such a standard would also allow for changes to the biometric capture device (i.e., a change in equipment) or algorithms without reenrolling all system users.

In November 2001, the executive board of INCITS established Technical Committee M1, Biometrics, for the rapid development and approval of formal national and international generic biometric standards. The goal of M1's work is to accelerate the deployment of significantly better, standards-based security solutions for purposes such as homeland defense and the prevention of identity theft, as well as other government and commercial applications based on biometric personal authentication. INCITS approved the BioAPI Specification, Version 1.1, as the ANSI/INCITS 358-2002—Information technology—BioAPI Specification, on February 13, 2002. It is now considering CBEFF for fast track processing in the near future. Additionally, M1 is now reviewing contributions of draft project proposals for the standardization of biometric templates. M1 is also anticipating contributions of draft project proposals for the development of application profiles and implementation profiles, as required for homeland defense applications, for example, as well as for financial services, health care, civil aviation, and the use of biometrics for preventing identity theft.

User Acceptance

The overall success of biometric systems depends on how well people who use biometric systems accept them and how easy they are to use. If enrollment and matching procedures are too cumbersome, data-capture

[7]From 1997 to 2001, INCITS operated under the name Accredited Standards Committee NCITS, National Committee for Information Technology Standards. From 1961 to 1996, NCITS operated under the name Accredited Standards Committee X3, Information Technology.

errors can lead to high error rates, including FMRs and FNMRs. Moreover, if people perceive a technology as being too intrusive, their lack of cooperation or even resistance can affect a system's performance. Privacy concerns may be a barrier to the widespread adoption of biometric technologies.

Some people find biometric technologies difficult, if not impossible, to use. Still others resist biometrics in general as intrusive, inherently offensive, or just uncomfortable to use. They consider it to be physically intrusive to have to pause and position themselves in relation to a capture device while presenting their biometric. Or they even consider being required to verify their identity through a hardware device rather than a human interaction to be too impersonal. Fingerprint systems, in particular, face even stronger opposition because of their association with criminal applications.

Some biometric devices also carry concerns about hygiene. For example, some people object to hand geometry scanners because they do not like to put their palms on the same surfaces where many other people have placed theirs. Other people fear that devices that scan particularly sensitive areas of the body, such as the eyes, will damage them. Generally, the less intrusive people perceive a biometric to be, the more readily they accept it.

Much public concern about biometrics arises from fears that the technology can be misused to invade or violate personal privacy. Among these fears are that biometric information will be

- gathered without permission or knowledge or without explicitly defined purposes,
- used for a variety of purposes other than those for which it was originally acquired (sometimes called "function creep"),
- shared without explicit permission, or
- used to track people across multiple databases to amalgamate information for the purpose of surveillance or social control.

Technologies Viable for U.S. Border Control

No biometric technology is best for every situation, but it is possible to determine which technologies are more accurate and easier to deploy for border control applications. Last year, the International Civil Aviation Organization (ICAO) assessed fingerprint, facial, and iris recognition as the top three biometrics meeting the requirements for biometric identification in machine-readable travel documents. Table 8 summarizes the performance characteristics of the four technologies that are most viable for border control. The performance factors such as error rates, template sizes, and transaction times can vary greatly, depending on whether the biometric technology is being used for 1:1 verification or 1:N identification.

Table 8: Four Viable Biometric Technologies Compared

Characteristic	Facial	Fingerprint	Iris	Hand
False nonmatch rate (FNMR)	3.3–70%	0.2–36%	1.9–6%	0–5%
False match rate (FMR)	0.3–5%	0–8%	Less than 1%	0–2.1%
User acceptance issues	Potential for privacy misuse	Associated with law enforcement; hygiene concerns	User resistance; usage difficulty	Hygiene concerns
Enrollment time	About 3 minutes	About 3 minutes 30 seconds	About 2 minutes 15 seconds	About 1 minute
Transaction time	10 seconds	9–19 seconds	12 seconds	6–10 seconds
Template size	84–1,300 bytes	250–1,000 bytes	512 bytes	9 bytes
Number of major vendors	2	More than 25	1	1
Cost of device	Moderate	Low	High	Moderate
Factors affecting performance	Lighting, orientation of face, or sunglasses	Dirty, dry, or worn fingertips	Poor eyesight, glare, or reflections	Hand injuries, arthritis, or swelling
Demonstrated vulnerability	Notebook computer with digital photo or false photographs	Artificial fingers or reactivated latent prints	High-resolution picture of iris	None
Variability with age	Affected by aging	Stable	Stable	Stable
Commercially available	1990s	1970s	1997	1970s

Source: GAO analysis.

Recognizing that technology performance is least supported by substantive real-life test data, ICAO has asked its member states to perform scenario and operational evaluations with fingerprint, facial, and iris recognition technologies. It plans to evaluate the results of the testing and to select one or two biometric technologies for standardization in machine-readable travel documents.

Retina, speaker, and signature recognition have certain drawbacks that make them impractical for border control. Retina recognition is

considered too intrusive because the systems require users to position their eyes very close to devices, which some users find very discomforting. Also, because using these systems requires prolonged effort and concentration, a high percentage of people are unable to enroll. Speaker recognition was piloted for border control use but has been found unreliable. In fact, this technology has several disadvantages. Speech quality is affected by a person's health, such as a cold or sore throat, stress, and emotions. In addition, speaker recognition systems do not perform well in noisy environments because surrounding noise interferes with their ability to extract the distinctive characteristics of an individual's speech. Moreover, because speaker recognition technologies have large templates, they require longer processing times and use more storage. Finally, the voice does not appear to be sufficiently distinctive to permit identifying one individual within a large database of identities. Signature recognition has a high FNMR because most people do not sign their names consistently. Since the resulting nonmatches would require many secondary inspections, signature recognition is probably not practical for border control. Moreover, travelers from some countries may not be accustomed to signing their names, to writing their names in roman letters, or to writing at all.

Facial Recognition Performance

The two leading vendors of facial recognition technology have their own methods for analyzing a facial image and converting it to a digital template. Enrolling in a facial recognition system seems relatively easy. Results from Britain's NPL product testing produced a 0 percent FTER. But the performance of facial recognition technology appears to depend on the operational setting and specific application. Pilots of facial recognition surveillance at airports have resulted in FMRs between 0.3 percent and 5 percent and FNMRs between 5 percent and 45 percent. In a State Department Bureau of Consular Affairs test involving data sets of 10,000 to 100,000 images, fewer than 30 percent of intentionally seeded duplicate images were correctly matched—an FNMR of around 70 percent. Although facial recognition performs much worse than fingerprint and iris recognition, it remains attractive because facial images are used in a wide variety of identification documents.

The performance of facial recognition technology is affected greatly by environmental factors, especially lighting conditions. Variations in camera performance and facial position, expression, and features (hairstyle, eyeglasses, beards) further affect performance. Accurate image alignment is necessary for the leading facial recognition algorithms, which rely on identifying eye positions. One algorithm is rendered ineffective when a

person tilts the head from a direct frontal pose to more than about 25 degrees horizontally or more than about 15 degrees vertically.

Performance is also degraded significantly as the stored facial recognition template ages. When a match was attempted a year after initial enrollment, some facial recognition technologies correctly verified as little as 41 percent of the faces; this translates to an FNMR of 59 percent.

In tests conducted by the Federal Aviation Administration (FAA) from November 2001 through January 2002, the average enrollment time was 3 minutes and 2 seconds. When the device was in use, the time increased by approximately 9.5 seconds to pass through a door.

Facial recognition systems can be quite costly. A facial recognition server controlling access at a facility with up to 30,000 persons would cost about $15,000. Depending on the number of entrances installed with facial recognition devices, the cost of software licenses would range from about $650 to $4,500. As the size of the database and the number of attempted matches increased, so would a system's cost. In addition to the server and software licenses, a live-scan facial recognition surveillance system includes closed-circuit television (CCTV) surveillance. A fully integrated CCTV system for physical access surveillance can cost from $10,000 to $200,000, depending on the size of the entrance and the degree of monitoring required. For additional CCTV equipment, cameras can cost between $125 and $500. Cameras with advanced features can cost up to $2,300.

Although users typically consider facial recognition technology less intrusive than other biometric technologies, some are concerned that it can track them without their consent. Successful attempts to spoof live-scan facial recognition systems would not work in a border inspection where a border inspector is monitoring the equipment. (See appendix IV for more details on facial recognition technology.)

Fingerprint Recognition Performance

The majority of the leading vendors of fingerprint recognition technology sell scanners based on optical or silicon technology. The companies' techniques for converting a fingerprint image to a digital template are proprietary. The basic performance of fingerprint recognition technology depends on the type of application and the type of scanner capturing the fingerprint image. For about 2 to 5 percent of people, fingerprints cannot be captured because they are dirty or have become dry or worn from age, extensive manual labor, or exposure to corrosive chemicals.

The time to enroll a person in a fingerprint recognition system depends on the number of fingerprints used and the details of the enrollment process. For example, in FAA testing, enrollment averaged 3 minutes and 30 seconds. In contrast, in the first 7 months of the CANPASS–Airport pilot at Vancouver International Airport, roughly 1,000 travelers registered in an average of 15 minutes.

The time required to match a fingerprint and verify an individual's identity can vary from sensor to sensor and from one application to another. For example, in FAA testing, users took an average of about 10 seconds to pass through the door, compared to an average of about 2 seconds before the device was installed. NPL found that an optical fingerprint system had a mean transaction time of 9 seconds, while a silicon sensor system had a time of 19 seconds.

A fingerprint recognition device can typically be set for different security levels, with higher FMRs at lower levels of security. For example, the FBI's Integrated Automated Fingerprint Identification System (IAFIS) has a 1.5 x 10^{-12} FMR with an FNMR between 1.5 and 2 percent. In contrast, FAA testing from September 2000 to February 2001 produced FNMRs that ranged from about 6 percent to about 17 percent for closely controlled test subjects. For actual airport employees accessing the door in a less-controlled environment, the FNMR ranged from about 18 percent to about 36 percent. The FMR ranged from 0 percent at the highest security level to about 8 percent at the lowest security level.

The cost of each fingerprint reader designed for physical access control ranges from about $1,000 to about $3,000. Software licenses are listed for about $4 per enrolled user. For smaller fingerprint scanners, maintenance is between 15 percent and 18 percent of cost. A larger live-scan 10-print fingerprint reader costs about $25,000. Maintenance of the larger machines is approximately 14 percent of the cost of the reader.

Because law enforcement agencies have used fingerprints to identify criminals, the technology's similarity to forensic fingerprinting causes some people discomfort. Privacy advocates fear that fingerprint recognition systems may collect data for one purpose but then use the data to track people's private activities or for other purposes. Also, people may have hygiene issues with having to touch the plate of the scanner that many other people have touched.

The fingerprint recognition technologies have been shown to be susceptible to deception, but this can be prevented if fingerprints are

scanned in a monitored environment. (See appendix II for more details on fingerprint recognition technology.)

Iris Recognition Performance

The sole provider of iris recognition technology developed the first commercially viable system in 1997. Enrolling in an iris recognition system requires a person to gaze steadily at a camera for a short time. Some people find this difficult to do and therefore fail to enroll. The FTER in an NPL test was 0.5 percent. While iris technology does not require touching any device, some people resist the scanning of their eyes.

However, iris recognition technology has good performance characteristics. Testing at the U.S. Army Research Laboratory resulted in FMRs of less than 1 percent and an FNMR of 6 percent. In 1996, Sandia National Laboratories, testing a prototype iris recognition system, found that the FNMR was 10.2 percent and the average enrollment time was 2 minutes and 15 seconds. In a more recent test by NPL, the iris recognition system showed an FMR of 0 percent, FNMR of 0.2 percent, and a mean transaction time of 12 seconds.

Colored or bifocal contact lenses can affect system performance, as can exceptionally strong glasses. Poor eyesight may also hinder some people from lining their eyes up with the camera. Glare and reflection can also cause interferences. People with glaucoma or cataracts may not be reliably identified by iris recognition systems.

Iris recognition systems cost approximately $2,000 for physical access units. The overall cost of a comprehensive iris recognition system would be much higher.

Certain iris recognition devices have been spoofed by holding up to the camera a high-resolution picture of an iris with a tiny hole cut out to allow the pupil of a live eye to shine through. Such deceptions could be prevented at a border inspection station monitored by inspectors. (See appendix V for more details on iris recognition technology.)

Hand Geometry Performance

Hand geometry, in use for almost 30 years, is a relatively mature biometric technology with only one primary vendor. The shape and size of our hands are reasonably diverse but not highly distinctive. Thus, hand geometry is not suitable for identifying one individual among many. Because border control applications require checking for duplicate enrollment before travel documents are issued, hand geometry is not viable for that aspect of

border control. However, hand geometry can be used to verify identity after performing the enrollment checks with a more distinctive biometric technology.

Typically, everyone with a hand can enroll in a system—FTER is 0 percent. In FAA testing from March through July 2001, time for enrolling with a hand geometry device averaged 57 seconds. The FNMR for airport employees using the system ranged from approximately 5 percent at a high security-level setting to less than 1 percent at a low security-level setting. The FMR ranged from 0 percent at the high security-level setting to about 2 percent at the low security-level setting. The FAA test also found that using the hand geometry device increased the time to open a door by 6 seconds. However, an NPL test found a mean transaction time of 10 seconds for a hand geometry system. The performance of hand geometry technology is affected by jewelry, arthritis, water retention, and swelling from pregnancy or hand injury.

Hand geometry devices generally cost between $2,000 and $4,000. Staff training is minimal, with no personnel costs, since most hand geometry devices are unattended. It is considered easy to use, although a minimal amount of training may be required for individuals to learn to align their hands in the device. Hand geometry is generally perceived as not intrusive, not threatening, and not invasive, and it bears very little of the stigma of other biometric technologies. (See appendix III for more details on hand geometry technology.)

Biometric Technology Applied to Border Control Today

Applying biometric technologies to customs and immigration in the United States and other nations is growing rapidly. Fingerprint, facial, and iris recognition and hand geometry systems are being planned or have been implemented to different degrees, ranging from piloted tests to operational usage. We summarize some of these projects and their applications, particularly to trusted air travel, land border crossing, obtaining and verifying travel documents, and surveillance.

Trusted Air Travel

Trusted air travel programs permit frequent travelers to circumvent customs procedures and immigration lines. To participate, users undergo a background screening and registration. Once enrolled, they can present their biometric at an airport kiosk for comparison against a template stored either on a storage card in their possession or in a central database.

INSPASS, a pilot program in place since 1993, has more than 35,000 frequent fliers enrolled at nine airports, with more than 250,000 transactions every year. It is open to citizens of the United States, Canada, Bermuda, and visa waiver program countries who travel to the United States on business three or more times a year.

A hand recognition system similar to INSPASS at Ben Gurion Airport in Tel Aviv, Israel, since 1998 verifies international travelers and all Israeli citizens. By April 2002, more than 100,000 travelers had enrolled in the program, and the system was processing about 50,000 passengers each month.

The Expedited Passenger Processing System (EPPS), based on iris recognition technology, is being launched at eight major international airports in Canada. Positive verification against the template at an airport kiosk entitles travelers to circumvent customs and immigration lines. The first kiosks are expected to be installed in Vancouver and Toronto airports in 2003.

In July 2001, frequent travelers on British Airways and Virgin Atlantic Airways transatlantic flights began clearing immigration through iris recognition verification at London's Heathrow Airport. Once registered and enrolled, landing passengers can proceed directly to special lanes to verify their identity against an iris template stored in a central database. If successful, they are issued a ticket that admits them directly to the United Kingdom.

A program to expedite immigration processing for frequent travelers at Amsterdam's Schiphol Airport, the Netherlands, is based on a combination of iris recognition and smart card technology. About 2,000 smart cards have been issued to nationals from 18 different European countries.

Land Border Crossing

In a joint INS and State Department effort to comply with the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, every border crossing card issued after April 1, 1998, contains a biometric identifier and is machine-readable. The cards, also called laser visas, allow Mexican citizens to enter the United States without being issued further documentation for the purpose of business or pleasure and stay for 72 hours or less, going no farther than 25 miles from the border. If a Mexican citizen plans to stay for longer than 72 hours or to go more than 25 miles from the border, additional documentation is required. Consular staff in Mexico photograph applicants and take prints of the two index fingers and

then electronically forward applicants' data to INS. Both State and INS conduct checks on each applicant, and the fingerprints are compared with prints of previously enrolled individuals to ensure that the applicant is not applying for multiple cards under different names. The cards store a holder's identifying information along with a digital image of his or her picture and the minutiae of the two index fingerprints. Figures 13 and 14 show the front and back of the laser visa. As of May 2002, State had issued more than 5 million cards. However, INS has not yet deployed fingerprint readers or card readers, so inspectors examine cards at the points of entry as they would a travel document.

Figure 13: The Front of a Laser Visa



Source: INS.

Figure 14: The Back of a Laser Visa



Source: LaserCard Systems Corporation, Mountain View, California.

The government of Israel is implementing a biometrics system that uses hand and facial scans to facilitate passage through border checkpoints between the Gaza Strip and other areas of Israel. The system will verify the identity of 60,000 Palestinian workers who cross the border at 42 automated checkpoints daily. The workers' biometrics will be compared with templates stored on a central server and backed up on smart cards that the workers can present.

An iris recognition system in Singapore processes motorbike passengers crossing the border from Malaysia each day to work. Approximately 50,000 travelers cross this border each day.

Hong Kong plans to introduce a fingerprint scanning system in 2003 at the Shenzhen border in China to accelerate immigration for the 250,000 people who cross the border every day. Travelers will be able to swipe a smart card bearing personal data along with a photograph and the template of a thumbprint through an optical reader while presenting the thumb to a scanner.

Obtaining and Verifying Travel Documents

The Department of State has been running pilots of facial recognition technology at 23 overseas consular posts for several years. As a visa applicant's information is entered into the local system at the posts and

replicated in State's CCD, the applicant's photograph is compared with the photographs of previous applicants stored in CCD to prevent fraudulent attempts to obtain visas. Some photographs are also being compared to a watch list.

Australia's Sydney Airport is assessing facial recognition technologies in one-to-one comparisons of individuals' facial features with their passport pictures to identify people traveling with false passports.

Saudi Arabia installed iris scanning and fingerprinting devices in the King Abdul Aziz Airport in the Red Sea port city of Jeddah during this year's annual Hajj pilgrimage to Mecca to verify that individuals entered and exited the country under the same travel documents.

Surveillance

Sydney Airport in Australia is using facial recognition technology to identify wanted faces within the airport's crowds. Iceland's main international airport at Keflavik scans passengers with facial recognition technology as they pass through boarding gates, comparing their facial characteristics with a watch list of suspected terrorists and criminals.

Chapter 4: Scenarios for Border Control with Biometrics

In the previous chapter, we described how biometric technologies work, their performance, and some of their applications. In this chapter, we outline how fingerprint, facial, and iris recognition technologies could help improve the procedures now used to secure U.S. borders. We identify four possible scenarios:

- Making a watch list check before issuing travel documents.
- Making a watch list check before travelers enter the United States.
- Issuing U.S. visas with one or more of these biometrics.
- Issuing U.S. passports with one or more of these biometrics.

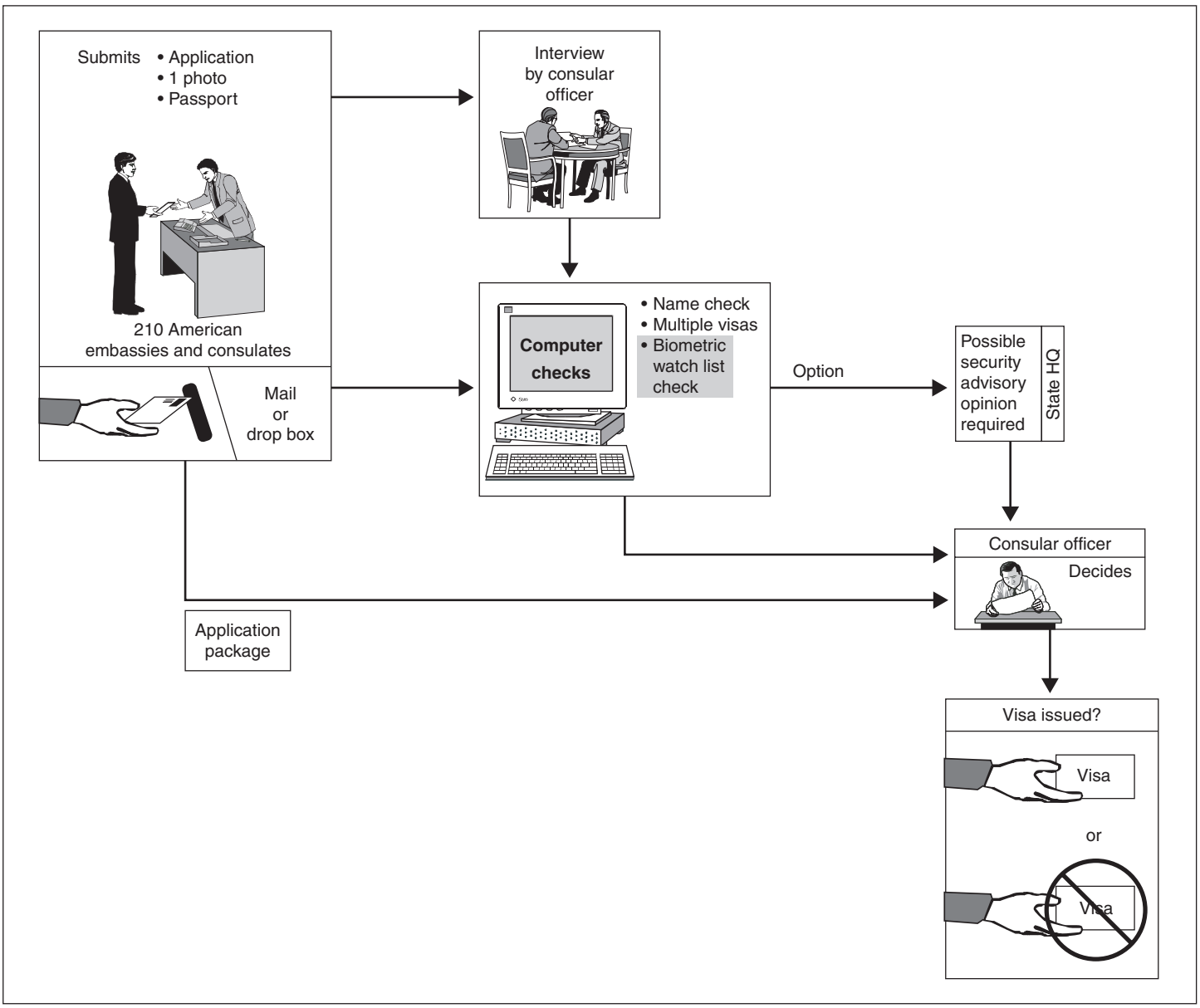
These scenarios do not represent all the ways to use biometrics for border control, but they do reflect some elements of pilots that have implemented biometric technologies for border control, as well as options discussed in legislation and by agencies responsible for border security. While hand geometry cannot be used for conducting a watch list check, it can be used in conjunction with one of the other technologies to verify identities using visas or passports.

The first two scenarios could help identify individuals who are ineligible to receive a U.S. visa or passport or who cannot be admitted to the United States. Both of these scenarios use an identification match to compare the traveler's biometric against a database of stored biometrics. The two other scenarios could help link an individual's identity to U.S. travel documents and could help reduce document counterfeiting and impostors' fraudulent use of legitimate documents. The four scenarios are not mutually exclusive; they could be implemented individually or in combination. In the next chapter, we analyze costs, benefits, and implications associated with implementing the scenarios.

Watch List Check before Issuing Travel Documents

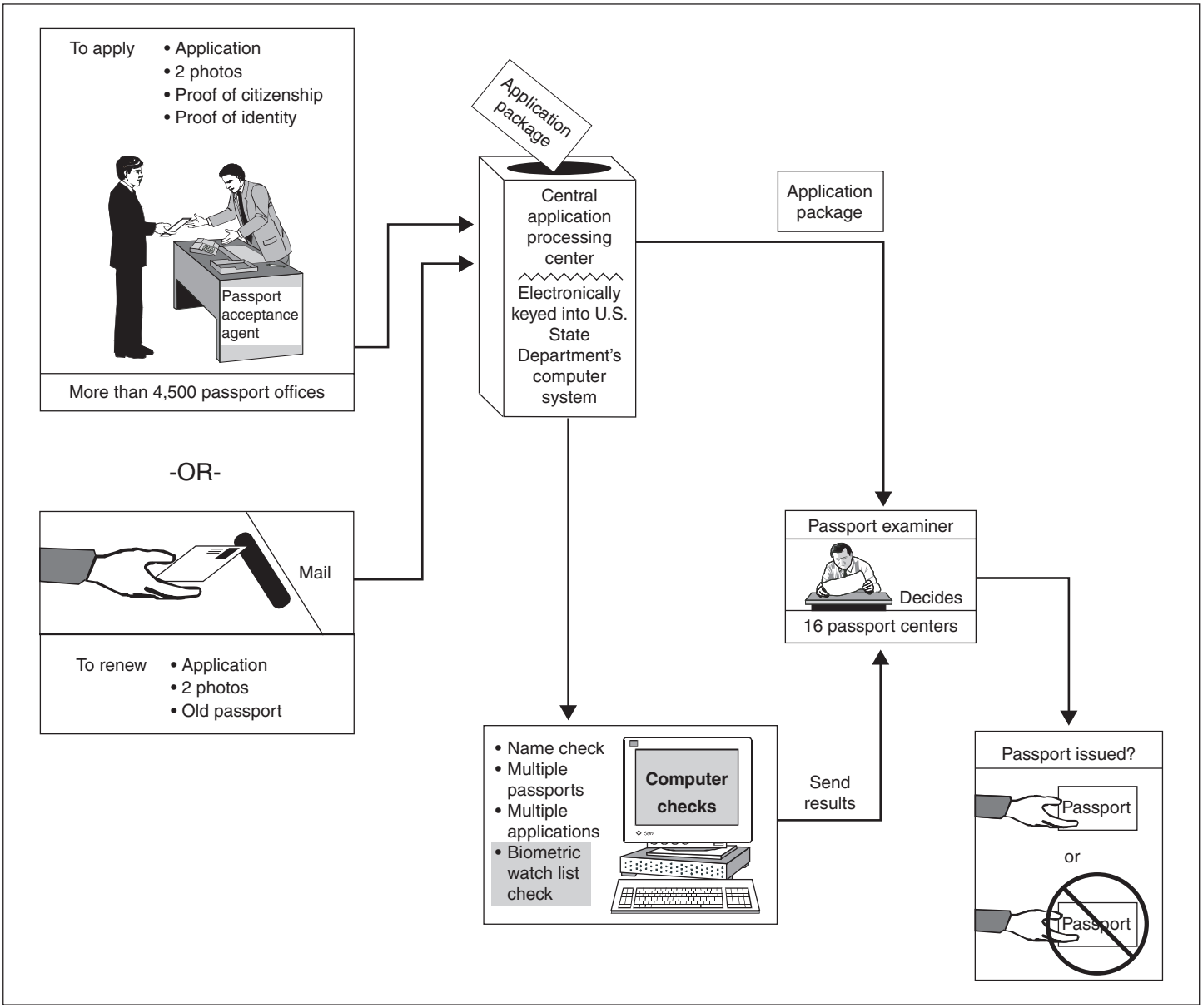
Making a watch list check before issuing travel documents could identify individuals ineligible to receive a U.S. visa or passport when their biometric was compared during the application process against a database of the biometrics of individuals on a watch list. This scenario would have the least effect on current operations and would require the least development of new systems. As depicted in figure 15 for visas and figure 16 for passports, the watch list check would essentially be an additional computer check conducted much as the name check that is conducted through CLASS today.

Figure 15: Issuing U.S. Visas by a Watch List Check Process



Source: GAO analysis.

Figure 16: Issuing U.S. Passports by a Watch List Check Process



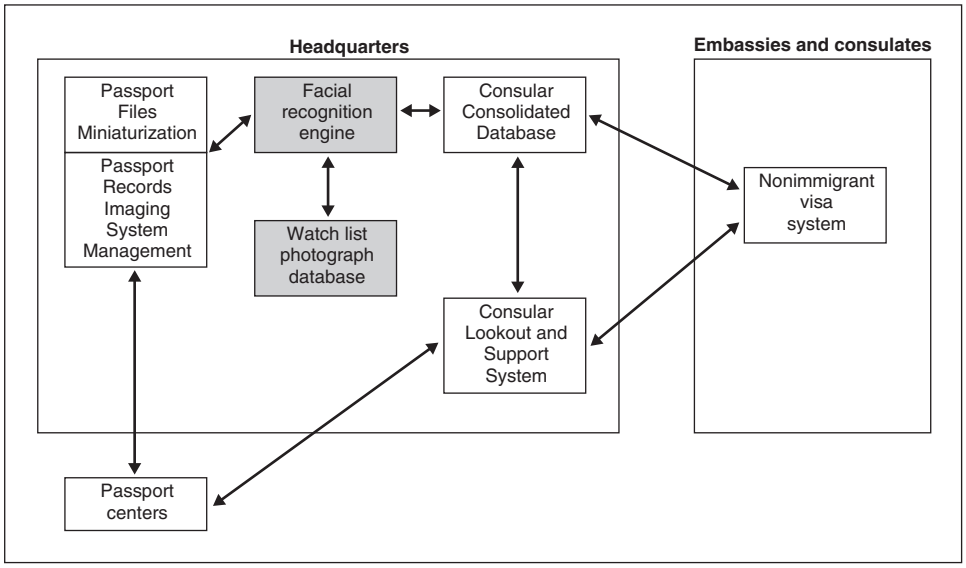
Source: GAO analysis.

Policies for the contents of the watch list would have to be developed, including criteria for names to place on the watch list—whether those of terrorists, criminals, violators of immigration law, or others. The biometric technology would most likely be based on facial recognition from

photographs that applicants for documents submit. Often, a photograph is the only biometric available for certain people who are not admissible to the United States. Criteria for the quality of the stored biometric for those on the watch list would probably have to be developed in order to enhance the performance of the matching process.

Implementing this scenario would probably require two additional computer system units to house the watch list and to match applicants' photographs and the photographs on the watch list. Figure 17 depicts one possible construct for this scenario's architecture. Existing systems, such as CCD and Passport Files Miniaturization (PFM), could require significant changes and corresponding time and resources to accommodate this scenario.

Figure 17: System Architecture for a Biometric Watch List Check before Issuing Travel Documents



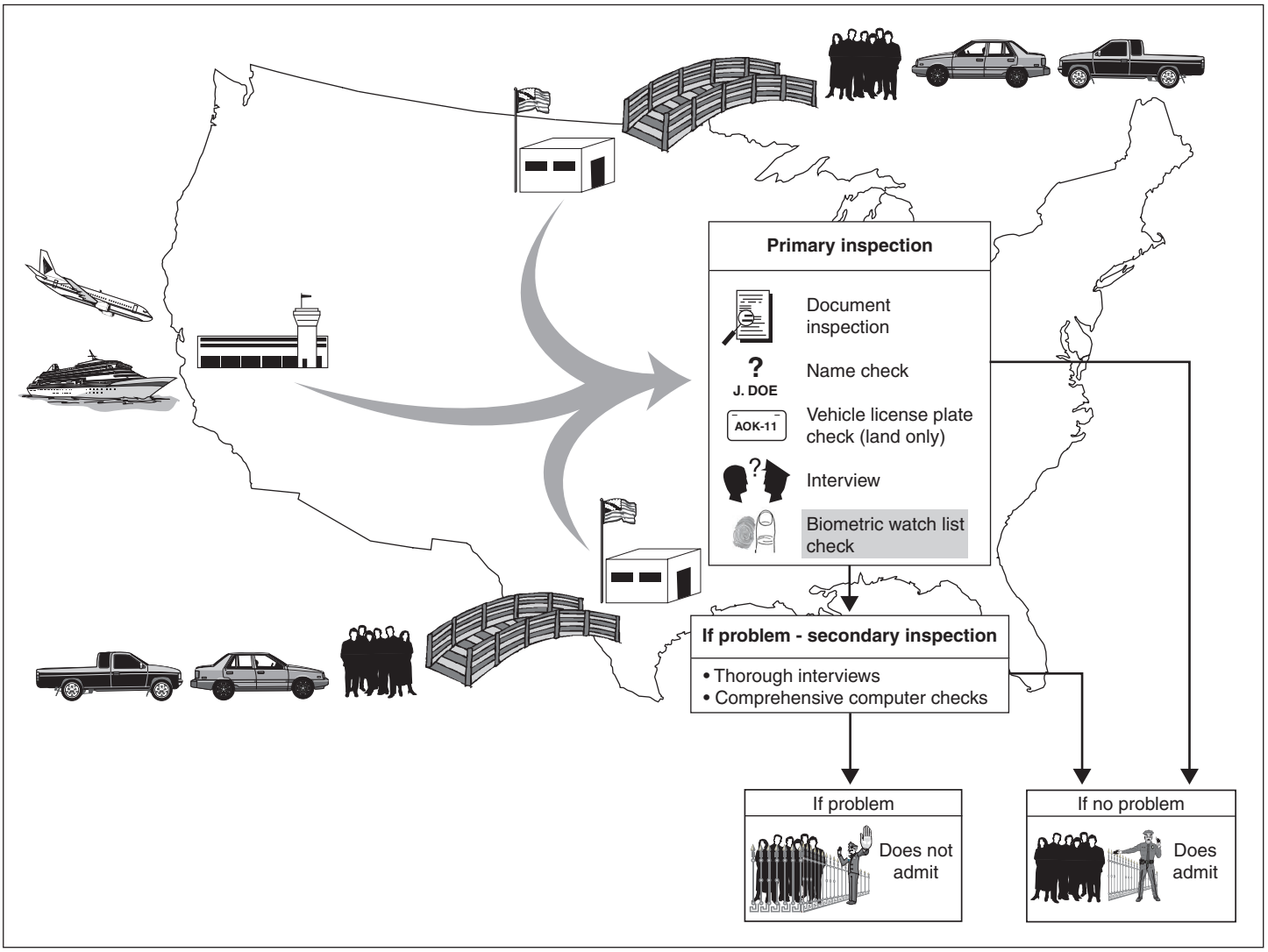
Source: GAO analysis.

Depending on the watch list criteria, it might be possible to use fingerprint or iris recognition to perform the match. Using fingerprints or the iris as the watch list biometric would complicate data collection. Instead of just submitting a photograph, applicants would have to submit fingerprint or iris biometrics. This information would then have to be stored centrally and read by readers installed at embassies, consulates, and passport acceptance offices.

Watch List Check before Entering the United States

Individuals who are not eligible to enter the United States could be identified before they could enter if, during inspection, their biometrics are checked against a database of the biometrics of people on a watch list. As depicted in figure 18, this watch list check—which would be similar to the IBIS check at ports of entry—would be an additional computer check conducted during inspection.

Figure 18: Entering the United States by a Watch List Check Process

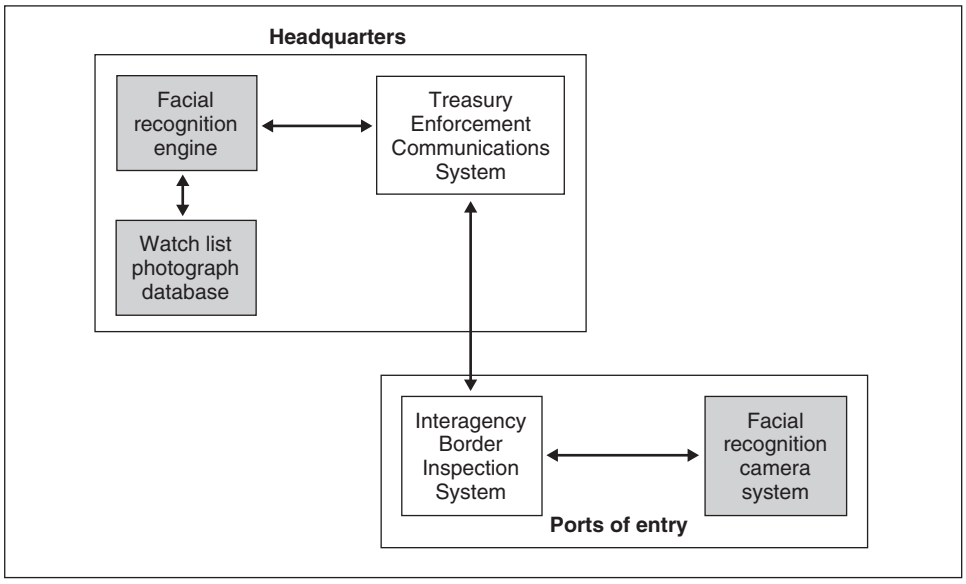


Source: GAO analysis.

As with the watch list scenario for issuing travel documents, policies would have to be developed for a watch list for entering the country, including the list's contents and the quality of the stored biometric. Facial recognition based on images collected as travelers presented themselves before INS inspectors would be the likely biometric technology. Often, a photograph is the only biometric available for certain people not admissible to the United States.

As with the scenario we described above, a database to store the watch list would have to be developed. The primary difference in cost between these two scenarios would be the cost of biometric readers for the ports of entry and the corresponding infrastructure and personnel to use the readers. The readers would require access to the database of the biometrics of the individuals on the watch list. Figure 19 depicts one possible construct for this scenario's architecture. Existing systems, such as IBIS and the Treasury Enforcement Communications System (TECS), could require significant changes and corresponding time and resources to accommodate this scenario.

Figure 19: System Architecture for a Biometric Watch List Check before Entering the Country



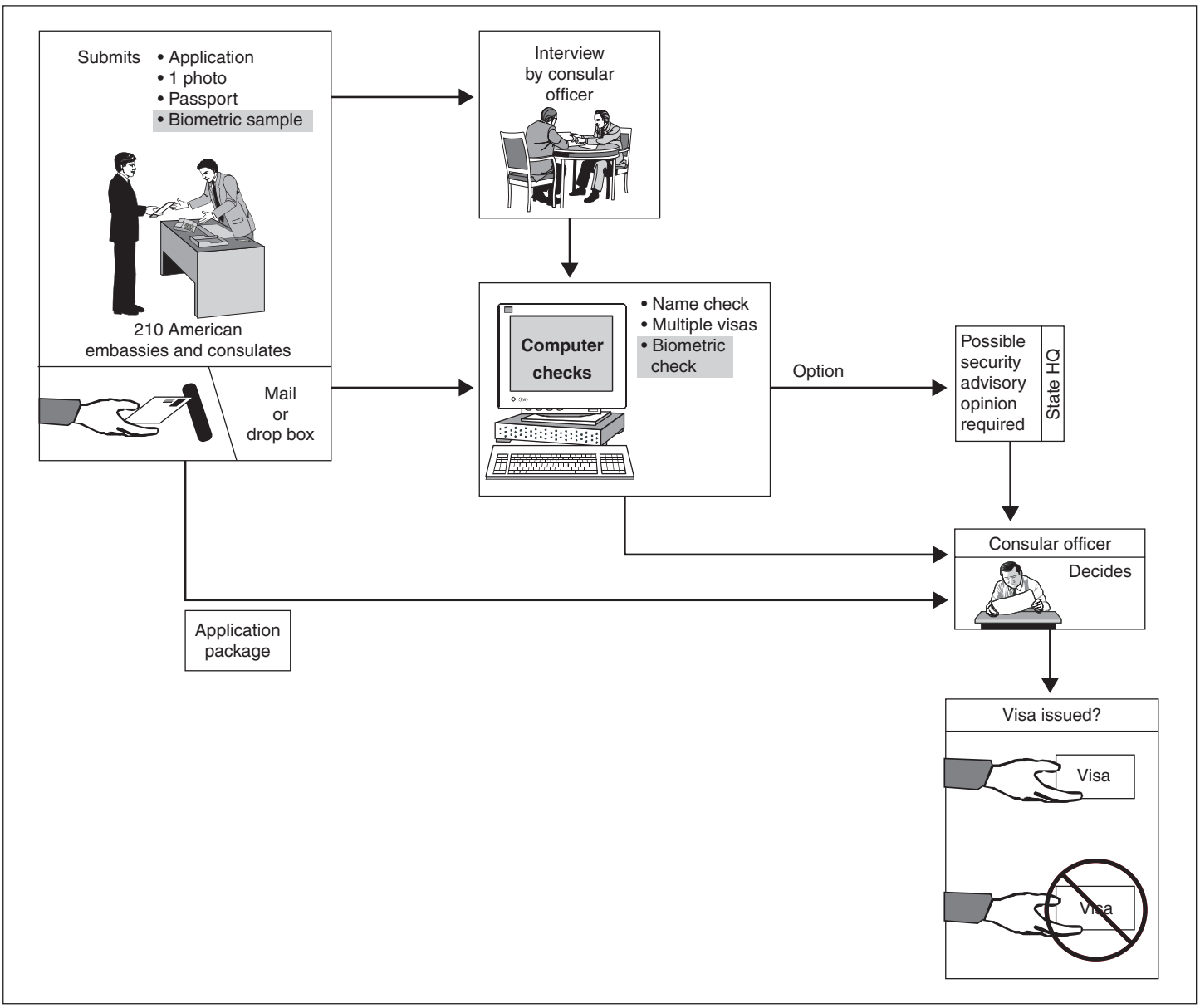
Source: GAO analysis.

U.S. Visas with Biometrics

In a scenario in which U.S. visas contained biometrics, two of the border control processes would be affected. First, applicants for U.S. visas would submit a biometric with their applications at American embassies and consulates. During the application process, the applicant's biometric data would be stored and an identification match would be conducted to compare the biometric information stored from other issued visas, as well as rejected visa applications, to check for duplicate and fraudulent applications. Second, at the ports of entry, the traveler's biometric would be verified as a part of the inspection process. The verification match compares the biometric data collected during the visa application process with the data collected during the inspection process.

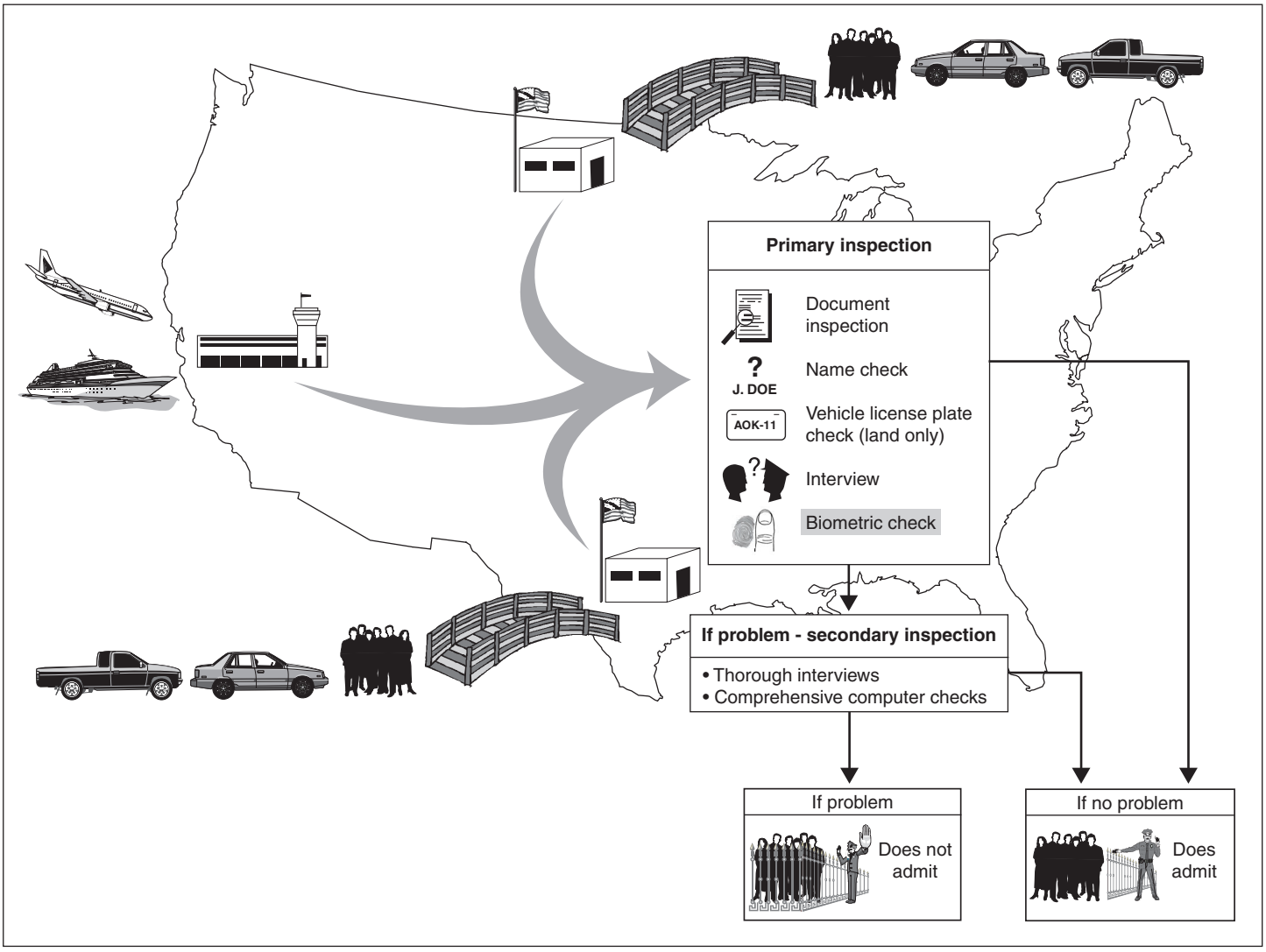
Figure 20 shows how collecting the biometric would change current visa issuing procedures and the additional computer check necessary to determine whether the new biometric had been previously enrolled. Figure 21 shows how port of entry inspection would change—essentially by adding a computer check to confirm travelers' identities.

Figure 20: Issuing U.S. Visas with Biometrics



Source: GAO analysis.

Figure 21: Port of Entry Visa Inspection with Biometrics

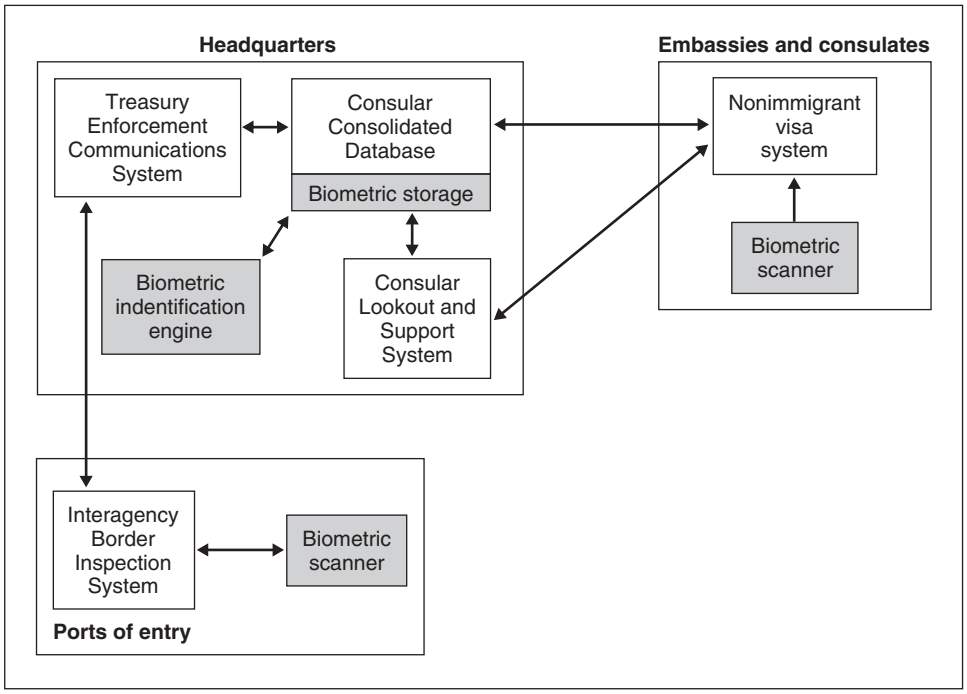


Source: GAO analysis.

This scenario would require buying biometric readers for the embassies, consulates, and ports of entry. A database would be required for storing biometric information. This database could be integrated with CCD, which stores visa application and issuance information. To properly link a biometric with an individual, live capture of the biometric would be required, eliminating some, if not all, of the benefit of mail-in and drop-box visa applications. Figure 22 shows one possible construct for this

scenario's architecture. Fingerprint, facial, or iris recognition could be used for this scenario. Hand geometry can be used only in combination with another technology because it is not effective in identification matches. Existing systems, such as IBIS, TECS, and CCD, could require significant changes and corresponding time and resources.

Figure 22: System Architecture for Issuing Visas with Biometrics

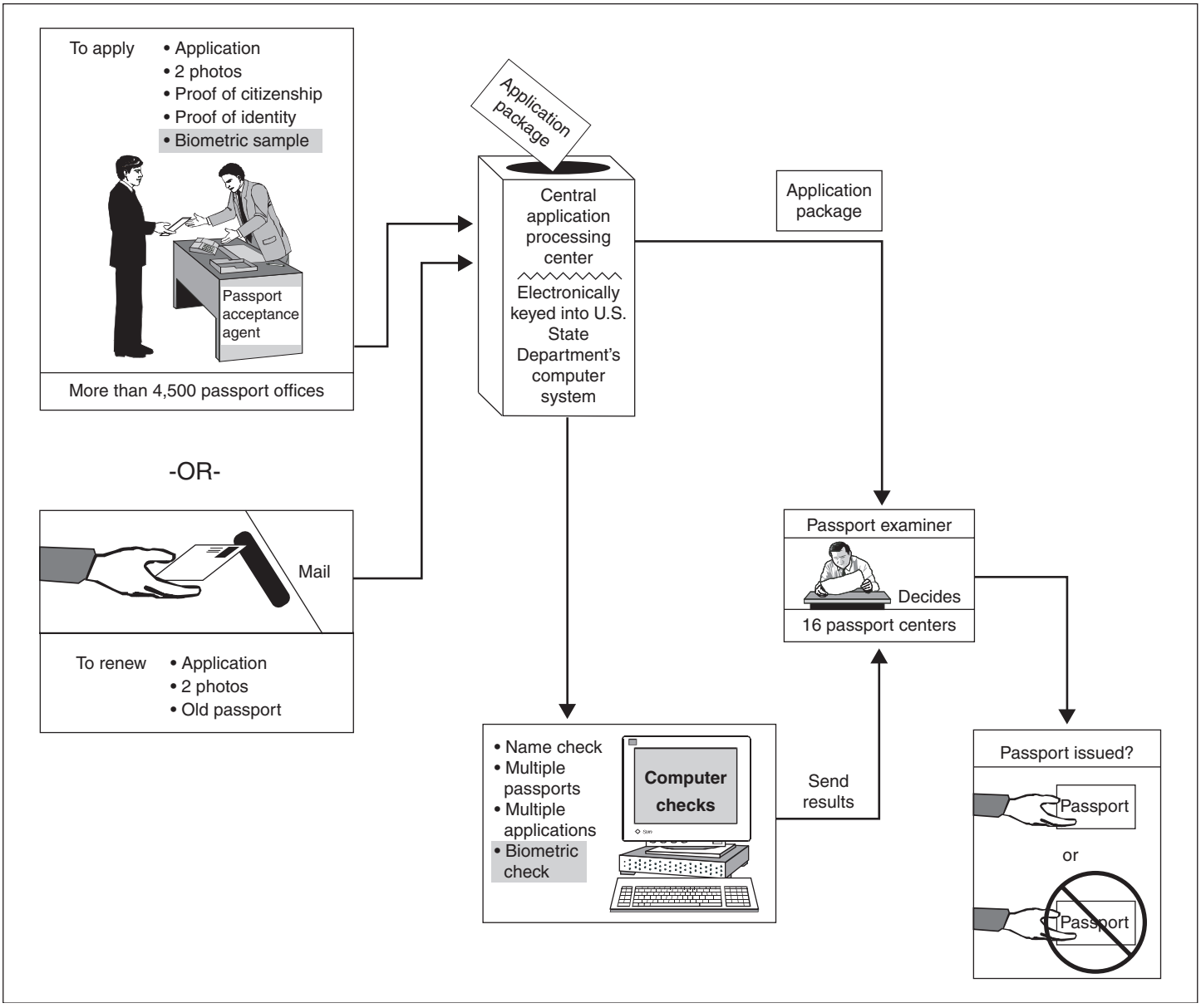


Source: GAO analysis.

U.S. Passports with Biometrics

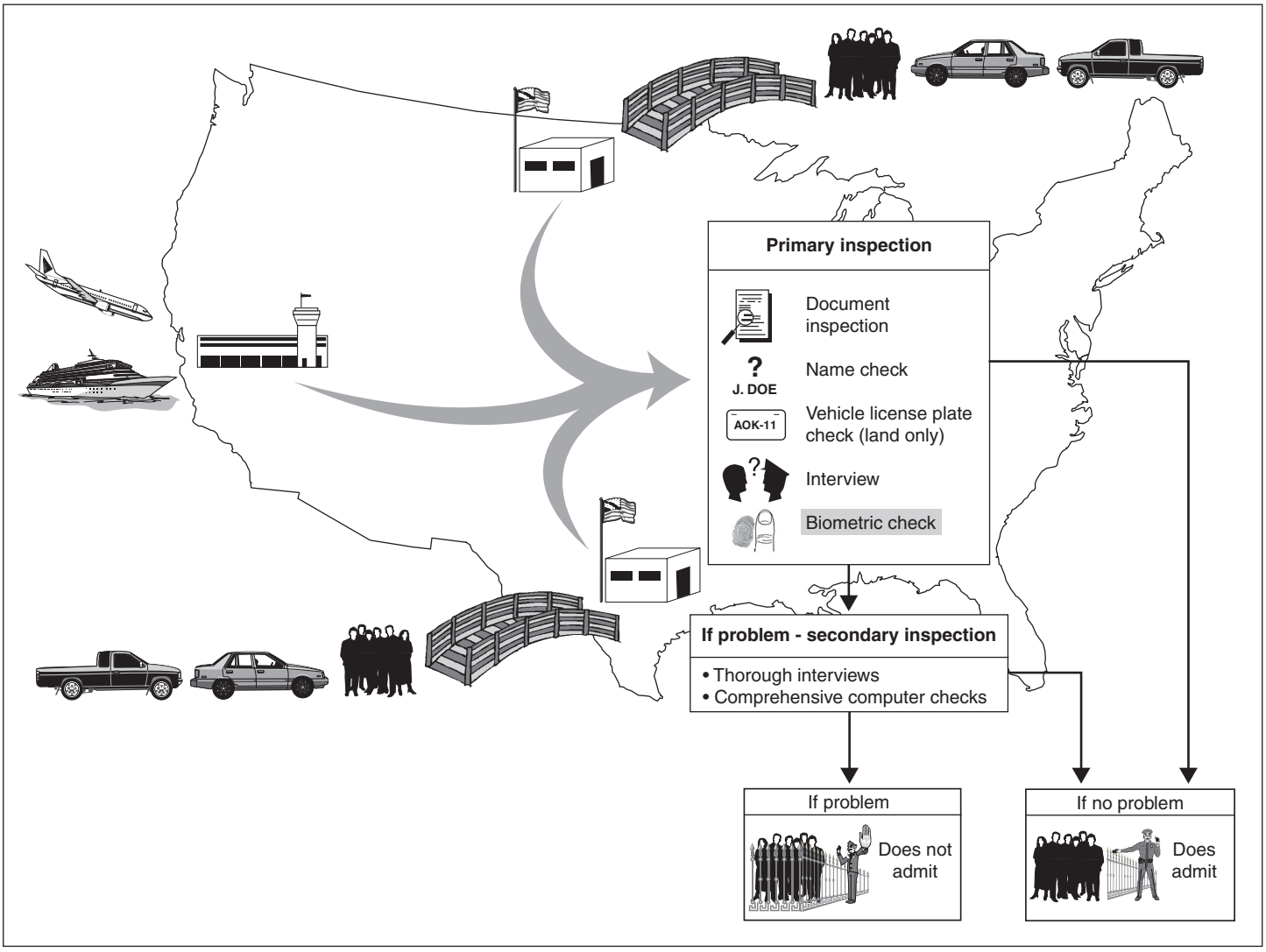
Two border control processes would be affected also in a scenario that issued U.S. passports containing biometrics. First, passport applicants would submit a biometric with their applications. The applicant's biometric data would be stored and an identification match would be conducted to compare the biometric information stored from other issued passports, as well as rejected passport applications, to check for duplicate and fraudulent applications. Second, the traveler's biometric would be verified during inspection at ports of entry. The verification match compares the biometric data from the passport application with the data collected during inspection. Figure 23 shows the biometric collection and the computer check to determine whether travelers' biometrics had been previously enrolled. Figure 24 shows the port of entry inspection, essentially adding a computer check to confirm travelers' identities.

Figure 23: Issuing U.S. Passports with Biometrics



Source: GAO analysis.

Figure 24: Port of Entry Passport Inspection with Biometrics

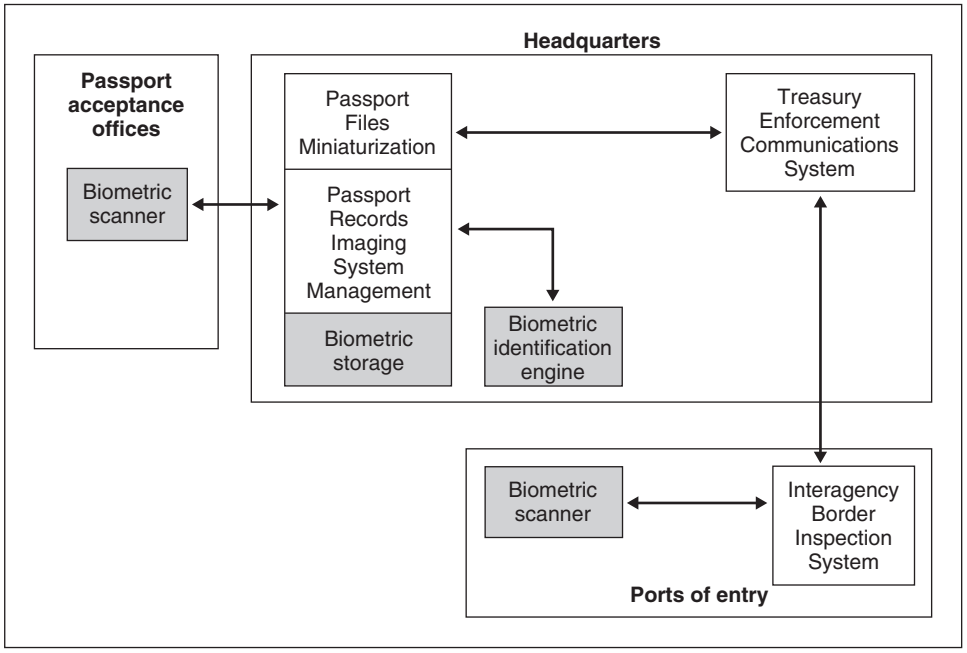


Source: GAO analysis.

This scenario would require purchasing biometric readers for passport acceptance offices and ports of entry. It would require the database for storing biometric information. The database could be integrated with the State Department's Passport Records Imaging System Management (PRISM) and PFM, which store passport application and issuance information. To properly link biometrics with individuals, live capture of biometrics would be required, and this might eliminate some of the

benefits of mail-in renewal applications. Figure 25 shows one possible construct for this scenario's architecture. Fingerprint, facial, or iris recognition could be used for this scenario. Hand geometry can be used only in combination with one of the other technologies because it is not effective in performing identification matches. Existing systems, such as IBIS, TECS, and PFM, could require significant changes and corresponding time and resources to accommodate this scenario.

Figure 25: System Architecture for Issuing Passports with Biometrics



Source: GAO analysis.

Implementing Multiple Scenarios

Two or more of these scenarios could be implemented in combination. Implementing scenarios in combination would not necessarily mean that costs would be additive. For example, the same biometric readers could be used to read biometrics from visa holders and passport holders at U.S. ports of entry. Similarly, the same watch list database could be used for checking before issuing travel documents and for checking before allowing entry into the United States.

It would also be possible to implement multiple biometric technologies. For example, it might be desirable for performance reasons to have both facial and fingerprint biometrics captured on visas so that either or both could be verified when people seek entry to the United States. It might be

possible to integrate the match algorithms so that they take in results from both biometric readers and use them in combination to determine matches. The incremental costs associated with the additional biometric readers would have to be considered, as well as the costs of any additional labor and space required in order to capture the biometrics and any additional server capacity to store the additional biometrics. We discuss costs in the next chapter.

Chapter 5: Applying Biometrics to Border Control: Challenges and Implications

While biometric technology is currently available and used in a variety of applications, questions remain regarding the technical and operational effectiveness of biometric technologies in applications as large as border control. In addition, before implementing any biometric border security system, a number of other issues would have to be considered, including

- The system's effect on existing border control procedures and people. Technology is only part of an overall security solution and only as effective as the procedures within which it operates.
- The costs and benefits of the system, including secondary costs resulting from changes in processes or personnel to accommodate the biometrics.
- The system's effect on privacy, convenience, and the economy.

In this chapter, we present our analysis of the costs and benefits of the four scenarios as they could be applied to current border control procedures.

The Performance of Biometric Technologies

Ideally, a biometric should be universally present, unique to the individual, and stable over time. The cost and ease of using a biometric technology also weigh into its selection. Of the four biometrics we examine in depth for border control, only a person's face is universally present, while other biometrics are not—people can lose or damage fingers, hands, and eyes. Estimates are that 1 to 3 percent of the population might be physically unable to use these biometrics.

Hand geometry and fingerprint, facial, and iris recognition have not been formally proven unique. Therefore, a biometric's uniqueness within a large population can be established only by its historical use. Table 9 shows the sizes of some of the larger biometric systems.

Table 9: The Enrollment Size of Seven Operational Biometric Systems

Biometric database	Technology	Enrollment
Mexican Federal Electoral Institute	Facial recognition	60,000,000
Integrated Automated Fingerprint Identification system	Fingerprint	40,000,000
INS Automated Biometric Fingerprint Identification System	Fingerprint	4,500,000
Ben Gurion International Airport	Hand geometry	100,000
INS Passenger Accelerated Service System	Hand geometry	35,000
King Abdul Aziz Airport, Saudi Arabia	Iris recognition	30,000
Schiphol Airport, Amsterdam	Iris recognition	2,000

Source: GAO analysis.

As table 10 shows, the sizes of the biometric systems specified in the four scenarios are large. The system required to issue visas with biometrics far exceeds in size the largest biometric database created so far. While fingerprint and facial recognition have been used in large systems, the size of each scenario far exceeds the largest iris recognition system of 30,000. As we have previously described, hand geometry is not highly distinctive and therefore cannot be used for border control where identification of one individual among many will be required. To be used for verification, hand geometry will need to be used in combination with one of the other technologies that can perform the initial identification match.

Table 10: Estimated Number of Biometric Matching Transactions in Four Border Control Scenarios

Scenario	System size	Matching transactions per year
1. Making a watch list check before issuing travel documents	Depends on criteria used to develop the watch list: CLASS has about 10 million records for foreigners and U.S. citizens	17 to 31 million applications: • 10 million visas; • 7 million passports; • possibly 14 million visas from visa waiver countries
2. Making a watch list check before travelers enter the United States	Depends on criteria used to develop the watch list: CLASS has about 10 million records	500 million primary inspections
3. Issuing U.S. visas with biometrics	100 million to 240 million visa records over 10 years	48 to 63 million
4. Issuing U.S. passports with biometrics	70 million passport records over 10 years	Up to 175 million[a]

[a]About 175 million U.S. citizens were inspected at ports of entry in fiscal year 2001. Because a passport is not required in returning from countries such as Canada and Mexico, it is not clear how many of these citizens had passports.

Source: GAO analysis.

In testing and operation, some fingerprint and iris recognition technologies have proven fairly accurate. Fingerprint recognition has achieved a low FMR but a variable FNMR. According to the FBI, the FMR for IAFIS is about 1.5×10^{-12} with an FNMR of between 1.5 and 2.0 percent.

In testing NPL conducted, at an FMR of about 2 percent, the FNMR was about 4.3 percent. In pilots FAA sponsored, FNMR ranged from 6 percent to 36 percent and the FMR was between 0 percent and 8 percent.

Iris recognition has also shown it can achieve a low FMR but with a variable FNMR. In NPL's testing, the FMR was 0 percent with an FNMR of 1.9 percent. The U.S. Army Research Laboratory found an FMR below 1 percent with an FNMR of 6 percent. Sandia National Laboratories' test showed 0 percent FMR and 10.2 percent FNMR.

Facial recognition has had more mixed results. In verification testing NPL conducted, at an FMR of about 1 percent, the FNMR was about 3.3 percent. In a pilot FAA sponsored, an FMR of 0.19 percent was achieved with an FNMR between 3 percent and 26 percent. In preliminary testing NIST conducted this year, facial recognition achieved an FMR of 1 percent and an FNMR of 25 percent. For identification testing, facial recognition fared worse. A State Department pilot encountered an FMR of 15 percent. Tests conducted at U.S. airports have found FMRs between 1 and 5 percent and FNMRs between 5 and 15 percent. At one airport where the objective was to achieve an FMR as close to 0 as possible, an FMR of 0.3 percent was achieved but with an FNMR of 45 percent. The U.S. Army Research Laboratory found an FMR of 49 percent.

The final primary factor to consider when evaluating biometrics is stability over time, but little work has been done to establish this. Fingerprints are believed to be persistent from birth throughout life. It is believed that irises are stable from before birth until death. FRVT 2000 tested facial recognition with images collected a year before identification or verification. The FMR for verification was 44 to 59 percent, while for identification it was 52 to 69 percent.

Fingerprint recognition appears to be the most mature of these biometric technologies. Fingerprint recognition has been used the longest and has been used with databases containing up to 40 million entries. Iris recognition is young and has not been used with populations approaching the size entailed in border control. While facial recognition has also been used with large databases, its accuracy results in testing have lagged behind those of iris and fingerprint recognition. IBG believes that further research, costing between $50 million and $100 million, would be required to determine whether iris or facial recognition could perform at the same level as fingerprint recognition.

How Introducing the Technology Affects People and Procedures

The success of any border security technology depends on the border control procedures as well as the people engaged in those procedures. Technology is not a solution in isolation. Technology and people must work together to execute the border control process—from issuing travel documents to inspecting them at official ports of entry.

Introducing biometrics would affect people and processes differently, depending on the specific scenario. Further, the performance of the biometric technology can also affect the overall process. To check a watch list before issuing travel documents, the following would need to be considered:

- Installation of readers at consulates and embassies for visa operations and at passport acceptance offices for passport operations would require hiring additional staff and, in some cases, leasing additional space.
- While the watch list identification check is essentially just an additional computer check, high FMRs could increase the work of consular officers and passport examiners and could delay the disposition of applications if significant time were required to reconcile false hits.
- Consular staff, passport acceptance agents, and passport examiners would have to be trained.
- Mail-in and drop box applications could be expected to fall off considerably, if not completely.

Similar concerns would need to be addressed to check a biometric watch list before travelers enter the country.

- Installing readers at ports of entry would require hiring additional staff and, in some cases, leasing additional space.
- Because the watch list identification check is essentially just an additional computer check, similar to an IBIS check, hits would probably result in secondary inspection of the traveler. High FMRs could increase the work of inspectors and delay the passage of travelers if significant time were required to reconcile false hits.
- Inspectors would have to be trained to collect the biometric from travelers and to resolve watch list hits in secondary inspection. An outreach campaign would likely be necessary to educate travelers about the new biometric program.

One key impact, the increased time required to conduct an inspection with a biometric watch list, would result from three key factors. First, to check all identities through IBIS using a biometric watch list would be a more substantive security check that would lengthen primary inspection. As we have previously described, not all travelers are now subjected to an IBIS name check. Second, while some have suggested that biometrics could speed inspection, FAA tests suggest biometrics would slow it down. FAA tests with biometric technology in a physical access environment showed that transit time increased by 6 to 9 seconds when biometrics were added to a magnetic card entry system. Third, an FMR that is too high could lead to excessive referrals of travelers to secondary inspection and could increase workload to resolve the false matches. For example, using facial recognition with a watch list of 10 million people and just a 1 percent FMR would result in an average of 100,000 false matches per traveler. Clearly, if the watch list will be large, the FMR will need to be extremely low to maintain workload at a manageable level.

For both watch list scenarios, policies and procedures would have to be developed for adding and maintaining records in the watch list database. Key questions that have to be answered for a watch list database include who is added to the watch list, how someone is removed from the watch list, and how errors can be corrected. One of the biggest issues would be the selection of a biometric to identify individuals on the watch list. Today's watch lists are primarily name-based and frequently list only the individual's name, approximate age, suspected nationality, or other identifying data. The selection could be affected by who will be placed into the watch list because biometric information for some people is not available. Facial recognition could be the likely biometric technology for a watch list because often only photographs are available for certain people inadmissible to the United States. However, fingerprint recognition or iris recognition could also be used if the United States could collect records on those individuals.

To issue and verify visas with biometrics, changes would be required at embassies and consulates to issue the visas and at ports of entry to verify the identities of those traveling with visas. Specifically, the following would need to be considered:

- Installing readers at consulates and embassies for visa operations would require hiring additional staff and, in some cases, leasing additional space.

- While the biometric identification check for duplicate or rejected applications is essentially just an additional computer check, high FMRs could increase the work of consular officers and delay the disposition of visa applications if significant time were required to reconcile false hits.

- Consular staff would have to be trained.

- Mail-in and drop box applications could be expected to fall off considerably, if not completely.

Similarly, to issue and verify passports with biometrics, passport acceptance office operations could be dramatically modified. Because the vast majority of these offices are not State Department offices and do not have State Department personnel or equipment, policy decisions would have to be made regarding the installation of computers and biometric equipment at these offices. Specifically, the following would need to be considered:

- Installing readers at passport acceptance offices would require hiring additional staff and, in some cases, leasing additional space.

- Because there is not a State Department presence at passport acceptance offices, a mechanism would need to be developed to transmit the collected biometrics on removable media or through a network connection to the department.

- While the biometric identification check for duplicate or rejected applications is essentially just an additional computer check, high FMRs could increase the work of passport examiners and could delay the disposition of passport applications if significant time were required to reconcile false hits.

- Passport acceptance agents and passport examiners would have to be trained.

- Mail-in applications could be expected to fall off considerably, if not completely.

As we previously described for the use of a biometric watch list at the ports of entry, the use of biometrics with visas or passports would likely lengthen the inspection time. Although the matching operation conducted with visas or passports with biometrics would be a verification match instead of an identification match, the inspection time could still go up for

the same reasons. Checking that the bearer of a travel document is the proper bearer of the document is a more stringent check than is conducted today. Further, the performance of the biometric technology affects the number of secondary inspections conducted if travelers are not properly matched to their biometric. Other issues that would need to be considered include

- Installing readers at ports of entry would require hiring additional staff and, in some cases, leasing additional space.
- Because the biometric verification check is essentially just an additional computer check, similar to an IBIS check, hits would probably result in secondary inspection of the traveler. An FMR that is too high could lead to inadmissible people being allowed to enter the country. An FNMR that is too high could lead to an increase in the number of travelers referred to secondary inspection, adding to requirements for space and personnel.
- Inspectors would have to be trained to collect the biometric from travelers and to resolve watch list hits in secondary inspection. An outreach campaign would likely be necessary to educate travelers about the new biometric program.

The biometrics for visas and passports could be stored and verified with or without tokens. Biometric data could be stored on tokens travelers carried, to be compared with data from biometric readers at ports of entry. A token could be a traveler's visa or passport with the biometric data stored on it as a bar code, or it could be a separate memory storage card, such as a smart card or laser card.

In an approach without tokens, a traveler's biometric data would be stored in a central database to be queried during matching. The data in the central database could be indexed by the visa or passport number or simply by the traveler's name combined with other identifying information such as date of birth, Social Security number, or driver's license number.

Regardless of the comparison method for verification, the enrollment process would be the same, whether at a consulate, embassy, or passport acceptance office. It is critical that the biometric, once collected, be securely linked to the visa or passport application and stored in a central database for comparison to other records, ensuring that duplicate identities are not being created. The operational concepts are

- **Check against token containing biometric data**. The traveler enters a primary inspection area and presents to the inspector a token containing his or her biometric data. The token is read and the biometric data are decrypted and validated. The traveler's stored biometric data and the biometric data obtained from the biometric reader are compared. If the data match, and if the inspector has no other reason to deny admission, then the traveler is admitted to the United States.

- **Check against central database for biometric data**. The traveler enters a primary inspection area and presents to the inspector a travel document or some other identifying information. Lacking a visa or passport, the traveler must provide information detailed such that a single record can be pulled from the central database. The remaining steps are the same as in checking a biometric token.

Process flow issues must be considered. A central database of biometrics would be required to prevent people from getting multiple passports or visas under different identities and for verifying the identity of a traveler whose token has been lost or stolen or becomes unusable. In this case, it is important that the traveler be able to provide enough information so that the inspector can check for and find the appropriate records. It is also possible that an identification match, instead of a verification match, could be run on an individual.

If a token is used, how it is produced must be considered. If it is to be a modification of the current passport or visa—for example, if the biometric is a two-dimensional bar code stored on the travel document—redesigning the passport or visa foil would be required. If the token is to be a separate card, such as a smart card or a laser card, the capital investment in a production facility would have to be considered.

Using tokens for the biometric storage could affect the inspection process. No studies have yet determined whether tokens expedite inspection. Studies should be conducted to determine what effect local data comparisons would have, compared with central database lookups.

For the three scenarios with biometric scanners at ports of entry, the physical configuration at the ports of entry could pose a challenge for collecting travelers' biometrics and performing matches. Where there are terminals, such as at airports, some seaports, and pedestrian ports of entry, it would be relatively simple to install biometric readers and to read travelers' biometrics. An inspector checks travelers' identities and names

at booths equipped with IBIS. At most sea ports of entry, where IBIS is not used, inspectors board the vessels to conduct inspections of aliens, while U.S. citizens are inspected as they disembark. Biometric readers could not be installed in such circumstances, making collecting biometrics from travelers challenging. Similarly, at land ports of entry, a way to collect biometrics expeditiously from all occupants of a vehicle would have to be developed.

For all four scenarios, exception processing would have to be carefully planned. When an applicant fails to enroll in a biometric system or when a system fails to correctly identify a person, that person must be treated as an exception. Exception processing that is not as good as biometric-based primary processing could be exploited as a security hole. Exceptions include passport and visa applicants whose biometrics cannot be properly enrolled in the system because they may not have the physiological characteristic that the system recognizes. One solution might be to use two or more biometric technologies in the same system, reducing the number of people who could fail to be enrolled.

The failure of biometric scanners, failure to access the central biometric database, failure to access the watch list, and communications failure are other exceptions. Because it is unlikely that inspections would cease, appropriate contingency plans would have to be developed to ensure continuity of operations without sacrificing security. Further, an appropriate transition strategy will be required to handle simultaneously biometric travel documents and the current travel documents that will remain valid without biometrics for the next 10 years.

Biometrics and Information Security

Just as operational processes must be considered, infrastructure processes must also be examined, particularly with respect to information security. Binding an identity to the biometric features of a person is only an entry in a database. Lax information security can weaken or break that bond. Laws enacted over the past 15 years require each federal agency to provide security protections for information collected and maintained by or for the agency commensurate with the risk and magnitude of harm that

would result from unauthorized disclosure, disruption, modification, or destruction of the information.[1]

Despite these statutory requirements, we have previously reported that poor information security is a widespread federal problem with potentially devastating consequences.[2] Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. These weaknesses continue, as indicated by our analyses of 24 large federal agencies that considered the results of inspector general reports and our reports published between July 2000 and September 2001.[3]

The security challenges directly affect the ability to implement existing laws and policies for protecting personal, proprietary, law enforcement, and national security information. Such safeguards require the appropriate tools to maintain confidentiality and ensure only authorized access, sharing, and use. Without appropriate security tools, the protection of this information will be at risk.

The information security challenges involved with a biometric system deal with the protection of biometric data—whether they are a biometric watch list or biometric reference templates stored in a central database or on a token—and the transmission of those data. Table 11 gives examples of operational issues, risks, and techniques related to binding individuals to their biometric information when issuing them visas or passports with biometrics. The binding process between a user and biometric information is critical to the success of a biometric-based user-authentication system. A process that does not have strong binding mechanisms will provide little improvement over existing processes.

[1]Government information security reform provisions of the FY 2001 Defense Authorization Act—for example, 44 U.S.C. §3534(a); Clinger-Cohen Act of 1996—for example, 40 U.S.C. §11313(6); Paperwork Reduction Act of 1995—for example, 44 U.S.C. §3506(g); and Computer Security Act of 1987—for example, 40 U.S.C. §11332.

[2]U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: September 24, 1996).

[3]U.S. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: November 9, 2001).

Table 11: Security Risks and Mitigating Techniques

Event	Adverse effect	Mitigating technique
Unauthorized changes are made to data in the central database—e.g., the biometric data associated with S. Smith is changed so she can claim an identity such as A. Smith.	The binding of a person to her biometric data is lost—in effect, she can assume multiple identities.	Electronic signatures can ensure data integrity; system can periodically check to ensure that the data and associated signature still agree. Original data can be restored from a secure backup when a modification is detected.[a]
Unauthorized changes are made to a token's data—e.g., biometric data originally stored with a given identity are replaced with biometric data associated with an impostor.	The binding of a person to his or her biometric data is lost—in effect, he or she can claim the identity of another person or assume multiple identities, using the same token.	Electronic signatures generated by a central database at enrollment can ensure a token's data integrity. The data can be changed but changes would be detected, since the system would not validate the electronic signature generated during enrollment with the original data.
A rogue government official generates a false identity for a person with the correct biometrics but altered name or birth date to bypass the system's checks for detecting suspicious individuals.	The binding of the person to her biometrics is not compromised, but the system cannot ensure that travel documents are issued only to an authorized person.	Split knowledge and dual control techniques can ensure that at least two persons validate the identity data provided to the system. Also, once identified, the electronic signature of the official who authorized the token can easily be revoked.
Biometric data on a token or in a database are compromised by unauthorized disclosure.	Since the public may believe that biometric data are as confidential as a Social Security number, their unauthorized disclosure may lead to identity theft and a public relations problem.	A token's biometric data can be encrypted to ensure that its loss or theft does not compromise the data. Although encrypting the database might make searching for duplicate values unrealistic, other controls can reasonably limit access to biometric images to authorized persons and processes.

[a] Electronic signatures are commonly used to provide assurances that unauthorized changes are not made to data. They may also represent an individual or an entity. A system-generated electronic signature should be (1) unique to the signer, (2) under the signer's sole control, (3) verifiable, and (4) linked to the data in a way such that if the data are changed, the signature is invalidated on verification. See U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: February 26, 2001).

Source: GAO analysis.

Weighing Costs and Benefits

Before any significant project investment is made, the benefit and cost information should be analyzed and assessed in detail. A business case should be developed that identifies the organizational needs for the project. A clear statement of high-level system goals should drive the overall concept of a U.S. border control system. Every aspect of the overall system—from the selection of biometrics to the system architecture—depends on the overall system goals. The high-level goals should address the system's expected outcomes—for example,

- binding a biometric feature to an identity (information such as name, date of birth, place of birth) shown on a travel document,
- identifying undesirable individuals on a watch list,
- checking for duplicate enrollments,
- verifying identities at the borders,
- ensuring the adequacy of privacy protections, and
- ensuring the security of the biometric information.

Certain performance parameters should also be carefully specified, including, among others, the

- time required to enroll people,
- time required to verify each person's identity by comparing the biometrics against a stored template,;
- acceptable overall FMR and FNMR, and
- maximum population the system must handle.

Similarly, not only must the costs of the technology be considered but also the costs of the effects on people and processes. A biometric-based border control system is bound to require significant up-front investments and a certain level of recurring costs to keep it operating. Weighed against these costs are the security benefits that accrue from using the system. Analyzing this cost-benefit trade-off is crucial when choosing specific biometrics-based border control solutions. The consequences of performance issues—for example, accuracy problems, their effect on processes and people, and their costs—are also important in selecting a biometric technology.

The desired benefit of all the scenarios we describe is to prevent the entry of travelers who are inadmissible into the United States. More specifically, in both watch list scenarios, a biometric check could improve security by adding a watch list check to the name-based watch list checks already being performed. A biometric watch list could help detect travelers who are trying to evade detection and who have successfully established a separate name and identity. Biometrics that are unique to these individuals

should identify them in biometric checks against the entries in the watch list. A biometric watch list could help detect certain travelers, even when a name or other biographical information about an individual on a watch list is unknown.

The quantitative benefit of the watch list scenarios (i.e., the number of travelers prevented from obtaining U.S. travel documents or denied access to the United States) would depend on the performance of the biometric technology, the quality of the biometrics in the watch list, and the data in the watch list. As we have described, the performance of the biometric technology will determine the additional number of people apprehended as well as the additional number of people identified incorrectly. The performance of the biometric technology is also dependent on the size of the biometric watch list. As more people are added to the watch list, the probability of a false match for any given traveler increases. While apprehending more people increases security, further questioning people identified incorrectly increases the operational costs of implementing the technology. The better the quality of the biometric in the watch list, the more likely it is that the technology will correctly match a traveler to it. Finally, if effective policies and procedures are not implemented to populate the watch list, the system's effectiveness will not be as great as it could be.

For issuing passports and visas with biometrics, the key benefit is to positively identify travelers as they enter the United States and to cut down on the use of fraudulent travel documents, including counterfeit and modified documents and impostors' use of legitimate documents. Travel documents would continue to serve as evidence that the bearer has the right of entry. The addition of biometrics can link the individual to the travel document and serve as evidence that the present bearer of the document is indeed the proper bearer. At ports of entry, INS inspectors intercepted more than 114,000 fraudulent documents last year (see table 12). About one-third of the intercepted documents were U.S. passports or visas.

Table 12: The Number and Type of Fraudulent Documents INS Inspectors Intercepted, Fiscal Year 2001

Document type	Number intercepted
Border crossing cards	30,419
Alien registration cards	26,259
Nonimmigrant visas	21,127
U.S. passport and citizenship documents	18,925
Foreign passport and citizenship documents	15,994
Reentry permit and refugee travel documents	702
Immigrant visas	597
Total	**114,023**

Source: INS.

The Census Bureau has estimated that between 7.7 million and 8.8 million unauthorized immigrants were in the United States in 2000.[4] INS has estimated that the annual increase in the number of unauthorized immigrants is about 275,000.[5] Of this number, INS estimates that about 60 percent of illegal immigration occurred "between the borders" and not at a port of entry where people or documents could be inspected. INS estimates that the remaining 40 percent of the undocumented population are nonimmigrant overstays, meaning they entered legally on a temporary basis but failed to depart. While it appears that current border control processes reduced the annual number of unauthorized entrants by about one-third, it is not known how many other travelers used fraudulent documents to enter the United States. Today, inspectors check identity manually, comparing photographs in a travel document with the face of the person carrying the document.

Linking biometrics to visas and passports would help ensure that travelers could not obtain travel documents under alternative identities once they had already applied for initial documents and established a biometric identity in the system. It would also help ensure that travelers who crossed the borders were the persons depicted on their travel documents. These two benefits could potentially decrease document fraud by making it

[4]U.S. Bureau of the Census, *Evaluating Components of International Migration: Estimates of the Foreign-Born Population by Migrant Status in 2000*, Population Division Working Paper 58 (Washington, D.C.: December 2001).

[5]U.S. Immigration and Naturalization Service, *Statistical Yearbook of the Immigration and Naturalization Service, 2000* (Washington D.C.: U.S. Government Printing Office, September 2002), 271–74.

harder to obtain a visa or passport under an assumed identity. The scenario could also reduce the use of counterfeit visas and passports and the use of legitimate documents by impostors.

Limitations to this approach are that a visa or passport biometric cannot necessarily link a person to his or her true identity, although it can bind him or her to a single identity within a system. A visa or passport biometric system would make it more difficult for people to establish multiple identities. Nevertheless, if the one identity a person claimed were not his or her true identity, then the person would be linked to the false identity in the biometric system.

Issuing visas with biometrics may have a limited effect because of the relatively few travelers who must carry a visa to enter the United States. While nonimmigrant aliens made 239 million border crossings last year, many were not required to present a visa at the port of entry, including Canadians, Mexicans who possessed a border crossing card, and aliens entering through the visa waiver program. It is estimated that in only about 22 million crossings were aliens required to have a visa to enter the United States last year—about 15 million entered as visitors or with task-specific visas (e.g., students), and another 7 million entered as crew on airplanes or ships. Even though the current Mexican border crossing cards are issued with two fingerprint templates on the card, it is unclear how Mexicans would be affected by a decision to issue visas with biometrics.

Issuing passports with biometrics might also have limited effect because passports are not required of U.S. citizens when they enter the United States from Canada or Mexico. While U.S. citizens made more than 179 million border crossings last year, it is not clear how many of them needed or presented a passport to inspectors at the ports of entry.

While it is standard practice to quantify benefits in monetary terms, it is difficult to do so for security applications. The monetary benefits of keeping inadmissible people out of the country depend on the activities undertaken while these travelers are in the country. Some inadmissible people may simply affect the labor supply, while others may conduct criminal or terrorist activities. Further information, including behavioral assumptions, would be necessary in order to characterize the value of preventing the entry of inadmissible persons.

As we have already stated, biometric technology is not a panacea for all border security problems. For example, none of these scenarios addresses two other key problems with border security. Previous INS estimates of

illegal immigration were that about 60 percent of all illegal immigrants entered "between the borders," not at a port of entry where they could be inspected. The scenarios we describe also will not help address problems with aliens' overstaying their visits; aliens who overstay have already presented themselves at a port of entry and were admitted by an inspector.

System Life-Cycle Costs

For each of the four scenarios, we created cost models to estimate the cost of developing, implementing, and maintaining various biometric processes. Besides including in the models the cost of purchasing the biometric hardware, we estimated costs for additional hardware, software, maintenance, personnel, training, and effects on other procedures in order to derive life-cycle cost estimates. We used DOD's definition of life-cycle cost, which includes all costs the government incurs in designing, developing, and operating a system through its life cycle, from its initiation through disposal of the system at the end of its useful life. We followed the cost element structure that DOD uses at acquisition program milestone and decision reviews to assess major automated information systems costs. Tailoring this structure to reflect our four scenarios, we used it to standardize costs so that they could be compared at a high level.

We present the costs in two parts. Initial costs represent the costs required to plan, design, develop, and field the system. Recurring costs represent the annual costs required to operate and continually maintain the system to keep it in operation.

We estimated seven sets of initial cost elements: costs for systems engineering and program management; development, installation, and training; biometric hardware; biometric software; network infrastructure; renovating consular facilities; and hardware infrastructure upgrades. We estimated ten sets of recurring cost elements: program management; biometric hardware maintenance; software and system maintenance; network infrastructure maintenance; consular operating personnel; port of entry operating personnel; communications; training; consular facility maintenance; and annual supplies. (More details on the cost elements can be found in appendix VI.)

Assumptions

We prepared the life-cycle cost estimates using fiscal year 2002 constant dollars—that is, inflation was not considered for the multiple years over which funds would be required for acquisition—and they represent rough order of magnitude costs. In addition, the estimates in our technology assessment are best guesses and should not be considered "budget quality." They attempt to provide a high-level view of what costs could potentially be, given the assumptions we describe here. In order to

develop budget-quality estimates, more details about the system to be built are required, including an operational concept, detailed requirements, site surveys, and vendor proposal data. Following are the assumptions that frame the boundary of our cost estimates.

Scenario life-cycle cost estimates represent development and installation time plus 10 years' operational life. Phasing of costs over time is simplified, and actual schedules to both develop and install equipment and infrastructure will most likely differ.

Biometric technologies—fingerprint, facial, and iris recognition—represent standardization to a single vendor's protocols. Biometric technology costs represent the average costs of vendors' products. Four flat fingerprints will be collected for fingerprint recognition.

There are 210 visa-issuing embassies and consulates worldwide. There are 4,500 passport acceptance offices. There are 3,950 primary and secondary inspection stations at 400 ports of entry.

Personnel costs reflect both direct costs and indirect costs. Three personnel will be needed to troubleshoot equipment at each port of entry, or 1,200 additional staff.

No costs were estimated for

- additional inspectors at ports of entry,
- additional facility space for passport acceptance offices or at ports of entry for primary and secondary inspections,
- biometric equipment for exiting the United States,and
- biometric security technology (e.g., encryption of biometric data).

Costs for Scenarios 1 and 2: Watch List Checks

We used the following assumptions to create the cost estimates for the two biometric watch list scenarios:

- The watch list database will include 10 million records.
- Matches will be performed using facial recognition technology.

- To conduct watch list checks before issuing travel documents, facial images will be generated by capturing the physical photographs applicants present when they apply for a visa or passport.

- The images will be collected and scanned at consulates and embassies for visas and at passport acceptance offices and transmitted through telecommunications resources to a central facility in metropolitan Washington, D.C.

Estimates include costs for a primary central processing facility and a contingency processing site. Table 13 summarizes the costs for the two watch list scenarios.

Table 13: Estimated Costs for Watch List Checks

Scenario	Initial	Recurring
1. Watch list check before issuing travel documents	$52.8	$72.9
2. Watch list check before entering the United States	$330.2	$237.0

Note: Dollars are in millions.

Source: GAO analysis.

In scenario 1, the major cost is additional consular staff to review biometric watch list hits. It is assumed that each embassy or consulate will require at least one additional foreign service officer to review biometric watch list hits before visas are issued. If the performance of the biometric technology requires more reviews and consequently more staff, the cost of the scenario will increase. Of the $52.8 million initial cost, $33.1 million is for the placement of 221 additional foreign service officers. Only $19.8 million is for the system's development, installation, and associated costs. Similarly, of the $72.9 million recurring costs per year, $50.7 million is for additional foreign service officers. Because it is unclear how many additional passport examiners would be required to review biometric watch list hits for passports, we have not included costs for additional passport examiners.

In scenario 2, adding facial recognition technology at the 400 ports of entry greatly increases costs over scenario 1. The additional costs related to developing and installing equipment at 3,950 primary and secondary inspection stations at the ports of entry adds another $200 million to the system's initial cost. (More details on the estimated costs for conducting watch list checks with biometrics can be found in appendix VI.)

Costs for Scenarios 3 and 4: U.S. Visas and Passports with Biometrics

We used the following assumptions to estimate the costs of adding biometrics to visas and to passports:

- The number of visa applicants will remain constant at 10.3 million annually. The number of travelers in the visa waiver program will remain constant at 14 million annually.
- The number of passport applicants will remain constant at 7 million annually.
- Enrolling travelers using a single biometric (whether for fingerprint, facial, or iris recognition) is estimated at 6 minutes (10 applicants enrolled per hour).
- Enrolling travelers using multiple biometrics (e.g., fingerprint and facial combined, fingerprint and iris combined, or fingerprint, facial, and iris combined) is estimated at 10 minutes (6 applicants enrolled per hour).
- All current visa-issuing embassies and consulates and passport acceptance offices will be equipped to collect biometrics from visa and passport applicants, respectively.
- Biometric token cards will be used to verify identities.

We present cost estimates for six different combinations of biometric technologies under two different possibilities for issuing visas (see table 14). The State Department receives about 10.3 million visa applications each year. In fiscal year 2000, INS estimated that approximately 14 million individuals traveled under the visa waiver program. If these travelers must obtain a visa to travel to the United States, we assume that this same number would also be required to have their biometric sample collected. An additional 14 million applicants increases the initial costs of the biometric system by about 30 percent and annual recurring costs by about 50 percent. The costs differ between the different combinations of biometrics because of the different costs of the different types of equipment and the increased time required to enroll people if more than one biometric is used.

Table 14: Estimated Costs for Issuing Visas with Biometrics

	Annual visa applications			
	10.3 million with visa waiver program		24.3 million without visa waiver program	
Scenario 3: Issuing visas with biometrics	**Initial**	**Recurring**	**Initial**	**Recurring**
Fingerprint recognition	$1,422	$708	$1,879	$1,077
Iris recognition	1,419	707	1,876	1,075
Facial recognition	1,399	698	1,851	1,065
Fingerprint and iris recognition	1,926	863	2,509	1,331
Fingerprint and facial recognition	1,904	854	2,479	1,318
Fingerprint, iris, and facial recognition	2,243	970	2,845	1,482

Note: Dollars are in millions.

Source: GAO analysis.

Operating personnel and space at the embassies and consulates are a major component of the cost estimates. Table 15 shows the initial and recurring costs for consular operating personnel and space when using single biometric and multiple biometrics. Depending on the combination of biometric technologies, we estimate the costs of consular operating personnel and space at 21 to 31 percent of initial costs and 23 to 29 percent of recurring costs. We did not include costs at ports of entry for facility renovation or personnel to verify the biometrics of travelers with visas as they enter the country.

Table 15: Estimated Consular Costs for Issuing Visas with Biometrics

		Annual visa applicants			
		10.3 million		24.3 million	
Scenario 3: Issuing visas with biometrics		**Initial**	**Recurring**	**Initial**	**Recurring**
Operating personnel	Single biometric	$75.9	$111.6	$114.9	$150.6
	Multiple biometrics	95.0	130.7	160.0	195.7
Space	Single biometric	335.8	89.5	463.6	123.6
	Multiple biometrics	378.2	100.9	563.7	150.5

Note: Dollars are in millions.

Source: GAO analysis.

Another major recurring cost is storage media for the biometric. At a cost of about $15 per card for laser cards, this adds more than $150 million to the recurring costs for 10.3 million visa applicants, or more than $360 million for 24.3 million applicants.

Table 16 summarizes the costs of issuing passports with biometrics with six different combinations of biometric technologies. Scenario 4 is by far the most expensive. The primary cost difference between issuing visas with biometrics and passports with biometrics is in the number of issuing locations. While only 210 embassies and consulates can receive visa applications, and even though fewer passport applications are received annually than visa applications, there are more than 20 times more passport acceptance offices (4,500) than embassies and consulates that issue visas. This greater number of locations has a direct effect on the estimates of initial and recurring costs for this scenario.

Table 16: Estimated Costs for Issuing Passports with Biometrics

Scenario 4: Issuing passports with biometrics	Initial	Recurring
Fingerprint recognition	$4,491	$1,574
Iris recognition	4,486	1,572
Facial recognition	4,446	1,555
Fingerprint and iris recognition	6,694	1,978
Fingerprint and facial recognition	6,655	1,961
Fingerprint, iris, and facial recognition	8,766	2,363

Note: Dollars are in millions.

Source: GAO analysis.

As with the scenario in which visas are issued with biometrics, two major costs are the costs of cards to store the biometrics and the personnel required to collect the biometric sample from passport applicants. The cost of cards adds more than $100 million per year to the costs of the biometric system. While it is not clear how biometrics would be collected at passport acceptance offices, we assumed that collection at each office would require one additional staff person, for an additional annual cost of $443.8 million. We did not include costs for additional space at the offices.

In the scenarios where biometrics are added at the ports of entry (i.e., performing a watch list check before entering the United States and issuing visas and passports with biometrics), the cost of additional inspectors is not included. As we have previously described, the addition of biometrics at the ports of entry would likely increase the inspection time of each traveler. Without the addition of inspectors and the corresponding space (i.e., inspection stations or lanes), delays would go up at the ports of entry. We did not analyze how many additional inspectors would be required to maintain current service times. These

costs will have to be collected and analyzed as part of the preparation for a budget-quality estimate should the government wish to pursue one of these options. (More details on the estimated costs of issuing visas and passports with biometrics can be found in appendix VI.)

Uncertainty Analysis

Simulation is an analytical method meant to imitate a real-life system, especially when other analyses are too mathematically complex or too difficult to reproduce. Risk analysis uses both a spreadsheet model and simulation to analyze the effect of varying the inputs to a modeled system on the outputs. One type of spreadsheet simulation is Monte Carlo, which randomly generates values for uncertain variables over and over to simulate a model. The simulation results show not only the different result values but also the probability (or certainty) of values.

We used both the initial and recurring costs as the forecast values and ran the Monte Carlo simulation for each of the four scenarios. We applied a probability distribution to each parameter that we thought could vary, such as the costs for development and installation, annual operating personnel, and additional square feet in embassy or consular facilities. Table 17 shows our estimates, the level of certainty calculated by the simulation for our estimates, and the cost for each scenario at the 90 percent certainty level. For issuing visas and passports with biometrics, we simulated only two of the six possible combinations—one using a single biometric and one using multiple biometrics.

Table 17: Cost Estimate Uncertainty Analysis for Four Scenarios

	Initial			Recurring		
Scenario	Cost	% certainty	Cost at 90% certainty	Cost	% certainty	Cost at 90% certainty
1. Watch list check before issuing document	$52.8	50%	$53.3	$72.9	50%	$74.2
2. Watch list check and facial recognition	330.2	50	347.9	237.0	91	236.4
3. Visa						
Fingerprint recognition	1,879	70	1,923	1,077	91	1,059
Fingerprint and facial recognition	2,479	60	2,529	1,318	89	1,324
4. Passport						
Facial recognition	4,446	60	4,725	1,555	92	1,518
Fingerprint and iris recognition	6,694	70	6,892	1,978	91	1,953

Note: Dollars are in millions.

Source: GAO analysis.

Developing, integrating, deploying, and maintaining biometrics to help secure the nation's borders will be costly. For example, the cost to

implement visas with biometric technologies would be on a par with a major DOD weapons systems acquisition or FAA's Standard Terminal Automation Replacement System.

Effects on Privacy and the Economy

Privacy and Civil Liberties

Underlying much discussion about the deployment of biometric technology are questions about the sufficiency of information management laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, to protect civil liberties.[6] Periodic public surveys have revealed a distinct unease with the potential ability of the federal government to monitor individuals' movement and transactions.

The Privacy Act limits federal agencies' collection, use, and disclosure of personal information. The act's protections are keyed to the retrieval of personal information by an "identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph."[7] Accordingly, the Privacy Act generally covers federal agency use of personal biometric information.

As a practical matter, however, the act is likely to have a more limited application to biometric information in the context of border control. First, it applies only to personal information regarding U.S. citizens and lawfully admitted permanent resident aliens.[8] Second, the act includes a number of exemptions that permit the disclosure of otherwise covered information for internal agency use, for compatible "routine uses," and for law enforcement and national security purposes.[9]

Representatives of civil liberties groups and privacy experts are concerned about (1) the adequacy of protections for security, data sharing, identity

[6]The Privacy Act of 1974 (5 U.S.C. §552a) and the Computer Security Act of 1987, Public Law 100-235 (15 U.S.C. §278g-3 and 4, 40 U.S.C. §11331, and 40 U.S.C. §11332).

[7]5 U.S.C. §552a(a)(4).

[8]5 U.S.C. §552a(a)(2).

[9]5 U.S.C. §552a(b), (j), (k).

theft, and other identified uses and (2) secondary uses and "function creep." A significant number of concerns raised during our interviews and conferences relate to the adequacy of protections under current law for the large-scale data handling in a biometric system. Besides information security, concern was voiced about an absence of clear criteria for governing data sharing. The broad exemptions of the Privacy Act, for example, provide no guidance on the extent of the appropriate uses law enforcement may make of biometric information.

Of equal concern is a tendency for large organizations to develop secondary uses of information; information collected for one purpose tends over time to be used for other purposes as well. The history of the Social Security number, for example, gives ample evidence of how an identifier developed for one specific use has become a mainstay of identification for many other purposes, governmental and nongovernmental.[10] Secondary uses of the Social Security number have been a matter not of technical controls but, rather, changing policy and administrative priorities. Further, some are concerned that biometric information can potentially be linked to multiple databases or to a vast national database. Questions being raised include what data would be included or linked to a biometric identification card; who would have access to such information, legitimately or otherwise; and how people who can access such data could use them.

Still others mention major concerns under the three headings of tracking, profiling, and loss of anonymity. Tracking is real-time, or near-real-time, surveillance in which a person's movements are followed through her biometrics-enabled transactions. While none of the scenarios we discuss use biometric technologies for surveillance, we have heard concerns raised about ways in which anonymity is likely to be undermined by surveillance. For example, many civil liberties groups are extremely concerned about the application of facial recognition technology for surveillance, which, like video surveillance, could result in the loss of anonymity in public places.

Profiling is the reconstruction of a person's movements or transactions over a specific period of time, usually to ascertain something about her

[10]U.S. General Accounting Office, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (Washington, D.C.: May 31, 2002).

habits, tastes, or predilections. Profiling for race, ethnicity, or national origin has caused much public debate in recent years. Tracking and profiling can destroy anonymity. The lack of clear policy goals and any flaws in the operation of biometric technology could compound all these concerns.

Concerns have also been raised about whether certain biometric data might reveal medical predispositions or personal health histories whose use could result in denial of insurance coverage or employment. For example, while not currently viable, the use of DNA matching as a biometric technology would be of concern because of the personal medical information that could be gleaned from it.

Not only are there concerns with secondary uses, but there are also concerns with unauthorized uses. Our recent studies on identity theft and studies by others reflect the difficulty of accurately measuring identification theft.[11] Developing a large-scale interoperable system such as a watch list system or issuing visas or passports with biometrics could increase the risks of identity theft and other unauthorized uses of personal information if the biometric data are not properly protected.

Biometrics industry groups, while expressing their appreciation of privacy concerns, have responded by saying that biometric products are "privacy neutral" and that it is how they are used that reflects either privacy invasion or privacy protection. IBG has developed a framework for defining the potential privacy risks borne by specific biometric technologies and their deployment. IBIA is also advocating on behalf of the industry to create responsible use guidelines and public policy. Industry groups emphasize self-regulation, which some privacy groups assert is not enough because markets are erratic and because, they say, the high value placed on data means incentives for violation are too high. Nonindustry groups have also developed privacy frameworks. The Internal Revenue Service (IRS) published a guide to developing privacy impact assessments for information technology. Also, the RAND Corporation developed a four-step approach for responding to sociocultural concerns about biometrics. Table 18 combines some of the salient characteristics of the guidelines IBG, IRS, and RAND developed and outlines many of the

[11]U.S. General Accounting Office, *Identity Fraud: Prevalence and Links to Alien Illegal Activities*, GAO-02-830T (Washington, D.C.: June 25, 2002).

questions to be answered in assessing the potential effect on privacy from any new biometric system.

Table 18: Summary of Biometric Systems Privacy Guidelines

Issue	Guideline
Scope and capabilities	Does the system have a clearly and narrowly defined purpose? Who will use the system? Have potential system capabilities been evaluated? Has there been an evaluation of a range of alternative choices, including biometrics? What types of information will be available through the biometric? Will the biometric information be used as a universal unique identifier? Will the storage of biometric information include extraneous information? Will the system store the original biometric data?
Data protection	Will the system separate biometric information from other types of personal information? What procedures will limit access to the system? Who will have access? Do other systems or agencies share or have access to data in this system? If data are being consolidated, what controls protect them from unauthorized access or use? How will the system ensure accuracy? What are the sources of information in the system? How will data collected from other sources be verified for accuracy? Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? Can the system make determinations about individuals that would not be possible without the new data? How long will data be retained in the system? What are the procedures for eliminating the data at the end of the retention period? While the data are retained in the system, what are the requirements for determining whether the data are sufficiently accurate, timely, and complete to ensure fairness?
User protection	Will users have the ability to unenroll? Will users be able to access and correct their biometric information? Will there be procedures for anonymous enrollment? Will the system and its use ensure individuals' equitable treatment? If the system is operated in more than one site, how will consistent use of the system and data be maintained? Will the system be able to identify, locate, and monitor individuals or groups of people? What controls will prevent unauthorized monitoring?
Disclosure, auditing, accountability, and oversight	Will there be full disclosure of audit data? Will the system's purpose be disclosed? Will the enrollment, verification, and identification processes be disclosed? Will the names of the individuals and entities responsible for system operation and oversight be accessible? Will users be informed about optional versus mandatory enrollment? Will a board or committee assess biometric data policies? Will third parties oversee the system? Who will review requests for access to biometric data? Who ensures that the biometric program is responsive to privacy concerns?

Source: GAO summary of data from IBG, IRS, and RAND Corporation.

These guidelines can help decision makers and other stakeholders approach privacy issues and determine the appropriate balance of privacy and security to build into the system. However, because there is no general agreement on the answers to these guidance questions, further policy

decisions are needed. The range of unresolved policy issues suggests that questions surrounding the use of biometric technology center as much on management policies as on technical issues.

Convenience for Travelers

As previously described, implementing biometrics could lengthen the process of obtaining travel documents or entering the United States. At some posts, visas are issued the same day applications are received. If significant time is required to resolve biometric watch list or visa database hits, issuing visas could be delayed. At the ports of entry, in order to avoid long lines of pedestrians and vehicles, each inspection has to be fast—according to INS officials in El Paso, Texas, for example, any time longer than 15 seconds would cause staggering delays. Even so, the busiest ports of entry regularly have delays of 2 to 3 hours.

Checking the biometric identity of passengers in vehicles is especially challenging. In a biometric system, would passengers have to exit their vehicles in order to have their biometrics checked? Any increase in inspection times could compound delays. Delays inconvenience travelers and increase their costs. Studies have been conducted on the value of travel time, and further studies in this area could help determine whether the increased security could result in fewer visits to the United States or lost business to the nation.

Economic Impact

While biometrics-based border control would affect regional economies and various economic sectors, it is difficult to quantify its effect. However, we can postulate that the travel and tourism industry might be adversely affected. Spending by international travelers in the United States totaled about $103 billion in 2000 and $90 billion in 2001. This spending is particularly important for California, Florida, and New York, which together account for more than half of all spending by international overseas visitors. If a biometric system made it more difficult to obtain visas for whatever reason, from higher visa fees to longer time between application and issuance, international travelers might choose to visit other countries instead. Further, there are concerns that if fingerprint recognition technology were used, the number of visitors from countries such as Japan would decrease dramatically because of those societies' aversion to fingerprinting.

At the regional level, biometrics could significantly affect trade with Canada and Mexico, the nation's largest trade partners, with total trade amounting to $653 billion in 2000. More than 80 percent of all Canadian exports are destined for the United States. If biometric identification

checks increased waiting time at land crossings, local merchants on both sides of the border could lose sales. Biometric systems might also have a profound effect on Mexico's *maquiladora* industry—the most dynamic sector of the Mexican economy, adding 1,400 new plants and 640,000 new jobs since the 1994 implementation of the North American Free Trade Agreement (NAFTA).[12] U.S.–NAFTA partner trade is concentrated at a few ports. In 2000, 10 accounted for 73 percent of all North American trade by land. Biometrics-based border control would have to be implemented carefully at these ports to preserve the flow of trade.

International Relations

The use of biometrics in a border control system in the United States could affect the number of international visitors and how other countries treat visitors from the United States. Much visa issuance policy is based on reciprocity—that is, the process for allowing a country's citizens to enter the United States would be similar to the process followed by that country when U.S. citizens travel there. If the United States requires biometric identifiers when aliens apply for a visa, other nations may require U.S. citizens to submit a biometric when applying for a visa to visit their countries. Similarly, if the United States requires other countries to collect biometrics from their citizens and store the data with their passport for verification when they travel here, they may require the United States to place a biometric in its passports as well.

As more countries require the use of biometrics to cross their borders, there is a potential for different biometrics to be required for entering different countries or for the growth of multiple databases of biometrics. Unless all countries agree on standard biometrics and standard document formats, a host of biometric scanners might be required at U.S. and other ports of entry. ICAO plans to standardize biometric technology for machine-readable travel documents, but biometric data-sharing arrangements between this country and others would also be required.

[12]Maquiladora refers to a Mexican company that imports, on a duty-free basis, machinery, equipment, and materials for the manufacture of finished goods for subsequent export.

Chapter 6: Summary

In this report, we have considered a number of leading and emerging biometric technologies that could potentially be used for securing the nation's borders. The seven leading biometric technologies include facial recognition, fingerprint recognition, hand geometry, iris recognition, retina recognition, signature recognition, and speaker recognition. Among the emerging technologies, we considered vein scan, facial thermography, DNA matching, odor sensing, blood pulse measurement, skin pattern recognition, nailbed identification, gait recognition, and ear shape recognition. Our assessment is based on a snapshot of biometric technologies as they existed in early 2002.

Of the seven leading technologies, fingerprint recognition, facial recognition, iris recognition, and hand geometry appeared to be suitable for border security. These technologies could be used to associate a person's identity with travel documents and thus deter fraudulent use of travel documents. Some of these technologies could be used to check to see whether a person is on a watch list. Of the four technologies, hand geometry is not very good at identifying one person in millions and, therefore, is not suitable if we want to search the biometric database to determine whether a person has previously enrolled in the database. However, hand geometry can be used to verify identity in combination with another technology. We found that the emerging biometric technologies are in various stages of development and have not yet been used in border control applications.

When it comes to effectiveness, all biometric technologies share a common characteristic. Every time a biometric feature is captured, it is always slightly different from the feature that was originally captured and stored in the system. Also, sometimes the biometric device cannot capture the biometric feature at all. Thus, all biometric technologies suffer from three types of error—the failure to capture a biometric feature, falsely not matching a biometric even though the person's biometric is in the system, or falsely matching a biometric. Each biometric technology has different levels of these errors, and the errors depend on many different factors, including the operational environment and security-level setting. For example, it is possible to trade off the false match and false nonmatch errors against each other. Thus, the effectiveness of a biometric technology depends on how it is used in an overall system.

Key Considerations in Using Biometrics for Border Control

It is important to recognize that biometric technology would be but one component of the decision support systems that determine who is allowed to enter the United States and who is not. As we have described, these decisions are generally two-step processes. First, a decision must be made to determine whether or not to issue a traveler a U.S. travel document. Second, a decision is made at a port of entry on whether to admit the traveler into the country. While the first step is not always executed, depending on the nationality of the traveler, all legal entries into the United States must be through an official port of entry.

The task of sorting admissible travelers from inadmissible ones is now conducted by using information systems for checking names against watch lists and by using human, manual recognition capabilities to determine whether a photograph on a travel or identification document matches the person who seeks entry into the United States. The introduction of biometrics into this process could help automate the identification of travelers.

In this report, we explored the use of biometrics in two types of systems. In one system, biometrics can check a person's face against a watch list of facial images and provide alerts if there is a potential match. In another system, the identity of travelers can be verified by comparing their proffered biometrics (e.g., a fingerprint) against stored templates that are associated with their travel documents.

We have found that three key considerations must be addressed before a decision is made to design, develop, and implement biometric technologies in a border control system:

1. Decisions must be made on how the technology will be used.

2. A detailed cost-benefit analysis must be conducted to determine that the benefits gained from a system outweigh the costs.

3. A trade-off analysis must be conducted between the increased security, which the use of biometrics would provide, and the effect on areas such as privacy and the economy.

As we have described, technology and people each have a role in executing processes to achieve a goal. Before anything else can be defined, the high-level goals of a system with biometrics must be clearly articulated. System goals are based on business or public policy needs. For example, a goal could be to prevent known inadmissible people from

entering the country. Based on the high-level goals, a concept of operations can be developed that embodies the people, process, and technologies to achieve the goals. To put together the concept of operations, a number of inputs have to be considered, including legal requirements, existing processes and infrastructure used, and known technology limitations. Performance requirements should also be included in the concept of operations. For example, an average inspection time or an average time to issue a visa could be included as performance requirements. Any process reengineering that would be required to accommodate the new technology should also be handled during this stage. For a biometric system, this could include new processes to conduct inspection of passengers in vehicles and to maintain the database of biometric reference templates.

Once the concept of operations is complete, the requirements of the biometric technology system can be developed and a particular technology solution can be selected. The system requirements are derived from the role of the technology system as defined in the concept of operations. Detailed system requirements should include functional and performance parameters, interface requirements, usability requirements, system quality requirements, and security and privacy issues.

The primary question to be asked when selecting the technology solution is whether it can support the requirements specified in the concept of operations and the system requirements. Particular attention must be paid to error measures, such as the false match rate, false nonmatch rate, and the failure to enroll rate. Concerns about the distinctiveness and stability of the technology, as well as its adherence to industry standards, should also be addressed. Because biometric technologies have not been used in applications as large as border control, further research may be required to establish the distinctiveness and stability of the biometric features. Distinctiveness has two aspects—how distinct a biometric feature is across a population and how many different biometric features are needed to uniquely identify an individual in a given population. Stability refers to how the biometric features change as a person ages. It is unclear whether a biometric captured during enrollment will still be properly matched with an acceptable level of accuracy after 5 years, for example.

A cost-benefit analysis must be conducted to justify the investment in a biometric border control system.[1] The benefits gained from a biometric border control system should be based on how well the system achieves the high-level goals. For example, if a goal of the system is to prevent known inadmissible people from entering the country, one of the benefits should be based on an estimate of how many additional inadmissible people are intercepted or deterred from entering the country with this system. The performance of the biometric system measured by its error rates would directly affect the expected benefit.

All life-cycle costs for the biometric system should be included in the analysis. The costs of the system include design, development, implementation, operations, and maintenance costs. Costs associated with the new business processes needed to use the new system should also be included, such as the costs of personnel to enroll people in a biometric system and the office space required to conduct the operation. Additional people and processes, and their costs, required as a result of performance limitations of the technology also must be included.

Finally, a trade-off analysis must be conducted between increasing security and its effect on areas that are harder to quantify, such as privacy, convenience, and the economy. Even if the cost-benefit analysis shows that the benefits outweigh the costs, the effect of increasing security may affect these areas to such a degree that the biometric system should not be undertaken.

Complying with the legal requirements for privacy is necessary to implement the system. Further, a system that does not include adequate protections for privacy may encounter barriers from users, who may not accept it during operation. The historical trade-off in any security system is between security and convenience. If a security system is not easy to use, people will stop using it. Similarly, if the process to enter the United States becomes too hard or time-consuming, people may choose to stop coming. This effect may manifest itself as an economic impact on the country as retail and trade diminish. Finally, the effect on the nation's dealings with other countries and their citizens must also be considered. International travel involves not only U.S. citizens but also citizens from

[1]For more information on cost-benefit analysis, see Office of Management and Budget, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*, Circular A-94 (Washington, D.C.: October 29, 1992; rev. January 22, 2002).

other countries. Hardships imposed on those citizens may result in reciprocal procedures being imposed on our citizens.

High-Level Analysis of Four Scenarios Using Biometrics

We defined four different scenarios in which biometrics could be used in a border control system. We considered each of the key considerations for the different scenarios. We did not answer the questions of whether each scenario is cost-beneficial or whether the gains in security outweigh the effects on privacy and the economy, but we did describe some of the effects that introducing biometrics into each scenario would have on people and processes, the benefits to be gained from the system, and the limitations of biometric technologies. We also described the effect of these limitations on the benefits and the effects on privacy, the economy, and international relations.

In addition, we prepared rough order of magnitude costs for each scenario. As summarized in table 19, initial investments could range anywhere from less than a hundred million dollars for a watch list application to billions for biometrics-enabled passports. Many of the recurring costs would be for the salaries of personnel required to enroll people and operate and maintain the system.

Table 19: Estimated Costs for Implementing Border Security Scenarios

Scenario	Initial cost	Annual recurring cost
1, Watch list check before issuing travel documents	$53	$73
2. Watch list check before entering the United States	330	237
3. Issuing visas with biometrics	1,399–2,845	698–1,482
4. Issuing passports with biometrics	4,446–8,766	1,555–2,363

Note: Dollars are in million.

Source: GAO analysis.

These costs have to be weighed against the benefits, which include reducing the fraudulent use of travel documents and automating the determination of whether travelers are on a watch list as they arrive at a port of entry. By binding an individual's biometric features to a travel document—either by storing the features on a token, such as a smart card the traveler carries, or by associating the identity with the biometric in a central database—the border inspection process would allow travelers to enter only if the stored biometric matches the biometric the individual presents at inspection. In a typical watch list, photographs of undesirable

people would be in a watch list of facial images, and a facial recognition system would automatically compare the facial image of each traveler with that in the watch list and identify potential matches. Inspectors can then further investigate those matches.

While using biometric watch lists and incorporating biometrics into travel documents could improve border security, the use of biometrics alone will not prevent the illegal entry of foreign terrorists and others into the country. For example, biometrics cannot prevent the illegal entry of those who do not enter through official ports of entry. Further, even at the legal ports of entry, unless all travelers are required to have their biometrics checked, it is possible that a traveler could bypass the biometric check. For example, if U.S. citizens are not required to enroll their biometrics to travel internationally and an alien could convince the inspector that he or she is a U.S. citizen, he or she could avoid the biometric check.

The use of biometric technologies could also have a significant effect on many different areas, from privacy concerns to the economy. While it appears that the Privacy Act of 1974 generally covers federal agency use of personal biometric information, as a practical matter the act is likely to have a more limited application in the context of border control because the act includes exemptions for law enforcement and national security purposes and does not cover nonimmigrant aliens. Civil liberties groups and privacy experts expressed concern about the adequacy of protections under current law for the large-scale data handling in a biometric system. Besides information security, concern was voiced about an absence of clear criteria for governing data sharing. Another concern was raised about the potential for secondary uses of biometric data and what other data would be linked to a biometric identification; who would have access to such information, legitimately or otherwise; and how people who can access such data could use them.

When used in border control, biometric technologies also affect the economy and international relations. We can postulate that the travel and tourism industry might be adversely affected, because biometrics-enabled visas may take longer to issue and may be considered more trouble than they are worth. Spending by international travelers in the United States totaled about $103 billion in 2000. At the regional level, biometrics could significantly affect trade with Canada and Mexico, the nation's largest trade partners, with total trade amounting to $653 billion in 2000. If biometric identification checks result in increased waiting times at land crossings, local merchants on both sides of the border could lose sales.

Using biometrics in a border control system in the United States could affect how other countries treat visitors from the United States. The reciprocity of visa issuance policy implies that if the United States requires biometric identifiers when aliens apply for a visa, other nations may require U.S. citizens to submit a biometric when applying for a visa to visit their countries. Similarly, if the United States requires other countries to collect biometrics from their citizens and store the data with their passports for verification when they travel to the United States, these countries may require the United States to place a biometric in its passports as well. As more countries require the use of biometrics to cross their borders, there is a potential for different biometrics to be required for entering different countries or for the growth of multiple databases of biometrics. Unless all countries agree on standard biometrics and standard document formats, a host of biometric scanners might be required at U.S. and other ports of entry.

The Role of Biometrics in Border Security

To address the role of biometrics in the overall border security problem and the high-level goals that can be achieved by using biometrics, a risk-based approach could be used. As we have previously reported, risk management is the foundation of effective security.[2] The approach to good security is fundamentally similar, regardless of the assets being protected, whether information systems security, building security, or homeland security. The answers to five basic questions can help determine the role of biometrics in a border security solution:

- What am I protecting?
- Who are my adversaries?
- How am I vulnerable?
- What are my priorities?
- What can I do?

A decision to implement one or more of the scenarios we have defined and analyzed in this report should be founded on a risk-based approach that

[2]U.S. General Accounting Office, *National Preparedness: Technologies to Secure Federal Buildings*, GAO-02-687T (Washington, D.C.: April 25, 2002).

answers these questions. These scenarios are by no means the only ways to implement biometrics to assist in the border control mission. Some of these scenarios could be implemented partially, or brand new scenarios could be used. For example, it could be possible to check biometrically enabled travel documents only at air ports of entry instead of at all ports of entry. Some have suggested that only selected travelers' biometrics be checked at the ports of entry instead of all travelers' biometrics. The selection could be random or based on travelers who fit a particular description. Another possible implementation of biometrics is within optional programs similar to INSPASS, in which travelers voluntarily choose to have their biometrics enrolled. In such a system, travelers would enroll with the expected benefit that they would be able to cross into the United States more quickly. Regardless of the system concept, decisions must be made that determine how the biometric technology will be used, if the benefits outweigh the costs, and what the effects on areas such as privacy and the economy will be. While a partial implementation may be less costly, the security benefits gained from such a system may also be less.

We have also noted that biometric technologies are not a panacea for the border security problem. It is important to realize that even with biometrics, many system dependencies cannot be controlled wholly by a technological solution. For example, if biometrics are included with visas, the process will still require establishing a traveler's initial identity in the biometric system. Once that identity is established, the benefits of strongly binding the individual to that identity can be gained. However, the system depends on the process used initially to establish that identity—that is, the applicant's presentation of a passport from his or her country. If the foreign country does not have adequate controls over the way it issues passports or, worse, deliberately issues passports with false identities, an individual could obtain a U.S. visa with a biometric unless additional processes are in place to further verify the applicant's identity. These processes are not a part of the biometric system but are still important for border security.

The population of a biometrics-based watch list is also dependent on nontechnological processes. As we have previously stated, the policies and procedures governing the population of a biometric watch list are critical to the success of the program. The success of the program depends on the effectiveness of the law enforcement and intelligence community to identify individuals to place on the watch list. People who are not on the watch list cannot be intercepted when trying to obtain a travel document or entering the country. Further, biometrics cannot help in detecting

illegal entry into the United States through other than the official ports of entry. They also cannot help in detecting aliens who enter the country legally but then overstay the terms of their visit.

Using a risk-based approach should help in the development of a biometric system's high-level goals and its concept of operations. The answers will help point out the system's limitations and what it will not be able to provide. They could also play a role in determining the appropriate balance between increasing security and cost and operational considerations as well as the effect on issues such as privacy and the economy. With these answers, the proper role of biometric technologies in border security can be determined.

Agency Comments and Our Evaluation

We provided a draft of this report to the Department of State and the Department of Justice for their review.

Department of State

In written comments on a draft of this report, the Department of State stated that it appreciated the thorough and balanced approach we took in our assessment of the use of biometrics for border security. State found the overall thrust of the report to be in keeping with its own considerations of how biometrics could be used in admitting individuals to the United States and how it could be integrated into the existing process for visa and passport applications. State agreed with us on the need for high-level policy decisions such as defining the specific uses of biometric data and performing a cost-benefit analysis that weighs the effectiveness and security benefits of biometrics against costs and the probable implications or consequences of implementation, including economic, civil liberty, and foreign policy concerns. State believed that policy decisions must be made before the successful selection, execution, and implementation of a border security program involving biometrics.

State noted that it is developing additional options for the implementation of a biometric program whose final estimated costs may differ. State also provided written technical comments on the draft, which we incorporated as appropriate.

Department of Justice

In written comments on a draft of this report, the Department of Justice expressed concern that the report did not (1) properly consider an overall border security strategy; (2) adequately recognize the draft NIST certified

standards recommendations for biometrics, tamper-resistant travel documents, or interoperability; or (3) fully explore the advantages of some biometrics over others. Justice also said that the draft contained analytical weaknesses related to a misunderstanding of the false match rate metric and to performance data and levels.

First, on the subject of an overall border security strategy, Justice explained that it has prepared such a strategy and that the U.S. government is continuing to consider this strategy. Justice believed that the implementation of this strategy would require major improvement in border systems. Further, according to Justice, if the use of biometrics were limited to visa applicants, who cover only about 3 percent of visitors to the United States, the impact on preventing the entry of potential terrorists into the country would be marginalized.

We requested a copy of the strategy from Justice on October 11, 2002, but as of October 24, 2002, we had not received the strategy document from Justice. While we did not have the opportunity to review Justice's strategy document, we do agree with Justice's assertion that an overall border security strategy is needed. Concerning Justice's point that visa applicants comprise only 3 percent of visitors to the United States, it is pertinent to note that limiting the use of biometrics to visa applicants would still target individuals living among the countries that are a higher risk of directing terrorism at the United States. Whether the use of biometrics should be limited to visa applicants should be based on Justice's border security strategy. We have previously stressed the need to develop and implement a homeland security strategy in coordination with all relevant partners.[3] This strategy should be comprehensive and should encompass steps designed to reduce our vulnerabilities, deter attacks, manage the effects of any successful attacks, and provide for appropriate response. The strategy should involve all levels of government, the private sector, individual citizens both here and abroad, and other nations. The strategy should also use a risk management approach to focus finite national resources on areas of greatest need. In this report, we reiterate the need for a risk-based strategy for the use of biometric technology in border security.

[3]U.S. General Accounting Office, *Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs*, GAO-02-160T (Washington, D.C.: November 7, 2001).

Second, Justice was concerned that this report presents information about biometrics that is inconsistent with the results of a NIST study required by the USA PATRIOT Act. In particular, Justice stated that the intended application must (1) employ a biometric that is able to establish and verify a unique identity in a population of hundreds of millions, (2) be used to run a check against criminal records, and (3) operate with a very low risk of false positive reads and with a verification process that is not rendered ineffective in different border, lighting, and weather conditions.

The results of the NIST study were not available during our technology assessment. However, we provided a draft of this report to NIST and received comments from NIST reviewers, which we incorporated, where appropriate, into the report. Further, we do not see an inconsistency between our position and Justice's description of the NIST study results. We consider these to be examples of items that would be defined in a concept of operations or a system requirements specification. The thrust of our report has been to point out the possibilities and not to select a specific biometric for border security—primarily because the selection comes after the concept of operations and requirements is developed. The requirements Justice described are what the department, with NIST's assistance, is defining as the requirements for a biometrics border control system.

Third, Justice stated that there are certain advantages to using fingerprints over other biometrics. For example, Justice cited the requirement in the Immigration and Nationality Act for aliens to be registered and fingerprinted, unless waived at the discretion of the Secretary of State. Justice further cited the law enforcement value of using fingerprint recognition for biometric identification on a large scale. Justice stated that unlike other biometric data, fingerprints are left at crime scenes. Further, Justice stated that we do not consider that the use of fingerprints would allow for a search against records stored in IAFIS to check for criminal history.

We acknowledge the qualities of fingerprint recognition raised by Justice. However, as we have described, the additional benefits Justice described should be included in the cost-benefit analysis that weighs the security benefits gained from a biometrics border control system against the costs of building the system. A benefits assessment should be based on how well the system achieves the high-level goals defined for the system. For example, if the ability to collect biometric samples at crime scenes is a requirement, it should be factored into the goals and requirements definition of the system. An evaluation of the technologies against the

requirements would then show that fingerprint recognition is the only technology that can meet that particular requirement.

Justice also believed that the draft report contained analytical weaknesses related to an insufficient analysis of large systems, misuse of performance metrics, and the reporting of performance data. Specifically, Justice stated that the draft did not provide sufficient analysis of large systems and did not define and use the false match rate metric correctly. Justice pointed out that the report provided incorrect performance data on IAFIS. Justice further cited the problem of having to manually resolve false matches and how the size of the database affects the number of false matches.

In the report, we state that none of the biometric technologies have been used with databases containing hundreds of millions of individuals. We have clarified the definition of false match rate and, on the basis of written technical comments provided by Justice, we have incorporated the performance data on IAFIS. We acknowledge Justice's point of having to manually resolve false matches. We state in the report that the performance of the biometric technology and its effect on people and processes are important in the selection of the technology. We also describe the potential effects of poorly performing biometrics on the border control process.

Finally, Justice stated that the "draft report infers that any move toward biometrics be made slowly and cautiously." Justice agreed that it is important to proceed judiciously but pointed out the sense of congressional urgency raised in the USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act.

We appreciate the urgency in developing a biometric system for border security, but a timely decision to invest in such a system should still be made in accordance with applicable federal regulations and best practices for acquiring information technology systems.

Justice also provided written technical comments on the draft, which we incorporated as appropriate. We have included Justice's comments in their entirety in appendix VIII.

External Reviewers' Comments

We provided a draft of this report to 16 different organizations for their review. Individuals from these organizations were selected because of their assistance during the data collection phase of our work. In addition, several of them attended one of our two biometric and border security meetings, convened for us by the National Academy of Sciences. The reviewers represented government, industry, and academia. We received comments and suggestions from 10 reviewers. The comments ranged from correcting technical inaccuracies to highlighting certain aspects of the assessment that the reviewers considered important.

Several reviewers commended us for putting together such a thorough report in a short time. One reviewer said that the report contains a wealth of information that will be useful to all biometric practitioners and researchers. Another reviewer noted that we have been able to successfully develop a cohesive report despite the difficulties associated with the wide variety of information available from vendors and studies. A reviewer felt that this will be a milestone report—head and shoulders above any other report on biometrics for border security.

In their comments, several reviewers cited their agreement with specific findings in our report, particularly with the limitations of biometric technologies in helping to secure the nation's borders. Specifically, reviewers agreed that biometric technologies are not a panacea for the border security problem and that they are just one component of the decision support systems that determine who is allowed to enter the United States and who is not. Further, reviewers agreed that biometrics cannot necessarily link a person to his or her true identity, although it can bind an individual to a single identity within a system. One reviewer concurred with the report's point about the difficulty in quantifying the benefits of security improvements.

Regarding the accuracy of a biometrics system, reviewers were concerned that we had not clearly defined and used FMR and FNMR as performance metrics. Reviewers also mentioned that we should not always equate FMR to false accept rate and FNMR to false reject rate. Similarly, reviewers were concerned that we did not separate out the results of larger tests involving many enrolled individuals from smaller ones and that in tabulating the performance of the biometric technologies, we had mixed results from verification and identification into the same table.

On the basis of these comments, we clarified the definitions of FMR and FNMR, highlighted how the same technology can have different performance requirements for verification and identification, and selected

comparable test results when summarizing the performances of the biometric technologies in a table.

Reviewers commented on our conclusion that hand geometry was not suitable for border control, pointing to its current use in border control applications. We had ruled out hand geometry for border control because it is not distinctive enough to perform identification matches when checking watch lists or for duplicate enrollment. Reviewers explained that for issuing visas or passports with biometrics, a more distinctive biometric such as fingerprint could be used for the duplicate enrollment check, whereas a simpler biometric such as hand geometry could be used when performing one-to-one verification at ports of entry. We incorporated this idea into our report so that hand geometry is now listed as a viable technology for border security.

On the subject of biometric standards, reviewers commented that in order to avoid being tied to a vendor's proprietary biometric template format, any biometric system has to store the original biometric images. Reviewers also suggested that we include ANSI's Biometric Information Management and Security (ANSI X9.84-2001) standard in the report and the AAMVA driver's license standard that includes biometrics. Reviewers also stated we should mention the ongoing biometric standards activities of the InterNational Committee for Information Technology Standards Technical Committee M1, Biometrics, which was established in November 2001. We incorporated these suggestions into the report.

Some reviewers expressed concern that using biometrics as suggested in the scenarios would be ineffective in preventing terrorists from entering the United States. Some reviewers believed that the report needs to better emphasize the limitations and operational concerns associated with biometrics. For example, reviewers suggested that we highlight the fact that adding biometrics to a travel document can bind only a person's claimed identity to the document. Additionally, the claimed identity is only as good as the credentials that a person uses to claim that identity. They also mentioned that biometric systems are not perfect and that operational procedures must address weaknesses in any system implementation.

We state that the goals of any biometric system for border security need to be defined before any decision to design, develop, and implement it. We describe a risk-based approach to security that can help with the definition of goals. Part of this approach is an identification of adversaries and threats. Regardless of whether terrorists are considered the only adversary to border security, a vulnerability analysis is required to

determine how an adversary can illegally enter the country. As we state in the report, biometric technologies are not a panacea for border security problems. Technology and people must work together to execute border security processes. As reviewers have pointed out, increasing security at the ports of entry does not address problems with people illegally crossing into the United States at points other than official ports of entry. Biometric technologies can only help support a single task, the binding of an identity to an individual. Numerous other technologies and people are needed to support other border security processes that, together as a whole, protect the border. We have further adjusted the report, where appropriate, to make this point clear.

Reviewers commented that our report does not take a sufficiently forward-looking approach to the civil liberties problems. The reviewers believed that the report appears to downplay significant issues with the effectiveness of biometric technologies and the significant civil liberties issues surrounding the use of biometrics for border control. These reviewers suggested that civil liberties issues need to be better addressed, including the potential for unauthorized access to data, abuse by those with authorized access, bad data in the system, the consequences of false matches on individuals, the need for greater transparency, and the dangers of racial or other profiling.

In the report, we summarize guidelines for addressing privacy in biometric systems. Similar to the need to define the security goals of a biometric border control system, there is a need to define the privacy requirements for the system. The guidelines can help decision makers develop a policy consensus on the amount of privacy to build into such a system. As we point out, many of the issues surrounding the implementation of privacy are not technical issues. Instead, they surround the management policies governing the use of the technology and the information generated by such a system.

We also received numerous technical comments on topics such as the specific enrollment numbers for biometric applications, template sizes, the maturity of new technologies, and equipment costs. We have incorporated these comments, where appropriate, in the report.

Appendix I: Our Technology Assessment Methodology

The objectives of this technology assessment were to

1. Identify biometric technologies currently deployed, currently available but not yet deployed, or in development that could be deployed in the foreseeable future for use in securing the nation's borders.

2. Determine how effective these technologies are for helping provide security to our borders currently or are likely to be in the future.

3. Determine the economic and effectiveness trade-offs of implementing these technologies.

4. Identify the implications of biometric technologies for personal security and the preservation of individual liberties.

To identify and describe biometric technologies, we convened, with the assistance of the National Academy of Sciences (NAS), two meetings on biometrics and border control issues, which included manufacturers of facial, fingerprint, and iris recognition and hand geometry technologies.[1] The meetings also included informed representatives from academia, government, and industry groups; privacy and civil liberty advocates; and other stakeholders such as representatives of border communities and trade organizations. We interviewed manufacturers of biometric technologies and reviewed their publications to obtain descriptive information about their equipment. We interviewed officials from biometric industry organizations, including the Biometric Consortium and the Biometric Foundation. We also interviewed the consulting firm the International Biometric Group (IBG). We attended the biometrics session of the International Industrial Security Conference, where technologies were demonstrated, and we discussed various aspects of the technologies with industry representatives.

To identify the current deployment of biometric technologies, we conducted a literature search and reviewed reports of deployments, tests, and pilots of biometric technologies. We interviewed certain users of biometric technologies, including the Federal Bureau of Investigation (FBI), Immigration and Naturalization Service (INS), National Security

[1]We have a standing contract with NAS under which NAS provides assistance in convening groups of experts to provide information and expertise to our engagements. NAS uses its scientific networks to identify participants and uses its facilities and processes to arrange the meetings. Recording and using the information in a report is our responsibility.

Agency (NSA), National Institute of Standards and Technology (NIST), the Department of State, and the Canada Customs and Revenue Agency.

To determine how effective the technologies would be in helping to secure the nation's borders, we needed to understand the current border security environment. We reviewed relevant statutes and regulations and interviewed State Department and INS officials at headquarters and INS officials at three ports of entry: El Paso, Texas (land); Miami, Florida (air and sea); and Niagara Falls, New York (land). We reviewed and analyzed statistics from INS's Performance Analysis System for fiscal year 2001.

To determine the effectiveness of biometric technologies, we reviewed test documentation from academic, government, and industry sources. In particular, we interviewed and reviewed documentation from the Department of Defense (DOD), Federal Aviation Administration (FAA), INS, NIST, Sandia National Laboratories, the State Department, the United Kingdom's National Physical Laboratory (NPL), and IBG.

To determine the economic and effectiveness trade-offs of implementing biometric technologies, we identified four different scenarios for implementing them and built cost models to obtain life-cycle costs for each scenario. The cost models represent rough order of magnitude costs and are based on DOD's cost element structure for major automated information systems. To build the cost models, we used data provided by the FBI, IBG, Naval Center for Cost Analysis, State Department, and various vendors. We reviewed the cost model and assumptions associated with each model with IBG and the State Department and incorporated their feedback where appropriate.

In addition, we performed uncertainty analysis on the cost models, using a Monte Carlo simulation tool called Crystal Ball to analyze the effects of varying inputs and outputs of the modeled scenarios. This allowed us to try multiple what-if scenarios with our spreadsheet cost model values and cells. We used the results of this analysis to provide a probability value for our point estimates, as well as to provide a risk-adjusted life-cycle cost estimate for each scenario. Crystal Ball examines the degree of risk in forecasts by using Monte Carlo simulation techniques that forecast all statistically possible results for a given situation. We applied a probability distribution to each parameter that we thought could vary, such as the costs for development and installation, annual operating personnel, and additional square feet in embassy or consular facilities. Then, Crystal Ball generated random values for each cell, according to the parameters we

chose to represent the risk. The software displayed the distribution of results, showing the highest, lowest, and most likely values.

We analyzed the benefits of each scenario and described the effects on people and processes, based on our understanding of the technology and current border control processes.

To determine the implications of biometric technologies, we reviewed relevant statutes and regulations and interviewed officials from privacy and civil liberty groups. We also heard from representatives of these groups at our meetings convened by NAS. We met with the Greater El Paso Chamber of Commerce to obtain its thoughts on the introduction of biometrics and the potential economic effect in the El Paso area. We reviewed data from the Department of Commerce and Department of Transportation to determine the potential economic effect of implementing biometrics.

We provided a draft of this report to the Department of State and Department of Justice for their review. We include their comments in appendixes VII and VIII, respectively. In addition, we provided a draft of this report to selected attendees of the two meetings NAS convened for this work and other interested organizations.

Three recognized independent external reviewers reviewed our process for conducting our work. In addition to providing a sound analysis of this assessment, the reviewers made recommendations for improving and enhancing future assessments should the Congress ask us to do more in the future.

We conducted our work from March to October 2002 in Washington, D.C.; Clarksburg, West Virginia; El Paso, Texas; New York, New York; Niagara Falls, New York; Miami, Florida; and Philadelphia, Pennsylvania. We performed our work in accordance with generally accepted government auditing standards.

Appendix II: Fingerprint Recognition Technology

Fingerprint identification has two basic premises. The basic characteristics of fingerprints do not change with time—persistence—and each person's fingerprints are unique—individuality. Scientific studies in the mid-1800s established the persistence of friction ridge patterns on human fingers, beginning in the embryonic stage and extending throughout life, except for accidental damage.

Manual inspection of millions of fingerprints has led to the widely accepted notion of fingerprint individuality. However, it has not been formally established by scientific means that a person's fingerprints are unique. Because it is impossible to obtain the fingerprints of every person in the world, estimating fingerprint individuality requires statistical methods to project the probability that two people will have the same fingerprint. The FBI's Integrated Automated Fingerprint Identification System (IAFIS) is the largest biometric database in the world with its 400 million fingerprints. Although the FBI has never discovered matching fingerprints from two individuals, tests have not been performed to conclusively verify that the fingerprints in IAFIS are unique.

In response to the need for a study to rigorously test the scientific basis of fingerprint individuality, the National Institute of Justice issued a formal solicitation in March 2000 for "Forensic Friction Ridge (Fingerprint) Examination Validation Studies." The objectives were basic research to measure the amount of detail in a single fingerprint that can be used for comparison and the amount of similar detail between two separate fingerprints.

Fingerprint identification has been used in law enforcement over the past hundred years and has become the de facto international standard for positively identifying individuals. The FBI has been using fingerprint identification since 1928. The first fingerprint recognition systems were used in law enforcement about four decades ago. Advances in optical scanning technology since the 1980s have made the technology practical for noncriminal applications. Figures 26 through 28 illustrate some current applications of fingerprint recognition technology.

Figure 26: Using Fingerprint Biometrics for Physical Access



Source: National Coordination Office for Information Technology Research and Development.

Figure 27: Using Fingerprint Biometrics for Logical Access



Source: Identix Incorporated.

Figure 28: A Fingerprint Biometric Device for Personal Identification



Source: Sagem Morpho Inc.

The use of fingerprints for forensic evidence was challenged recently. In 1999, the defense in U.S. v. Mitchell pointed to the Daubert Opinion, established in a 1993 U.S. Supreme Court case, that prompted the scientific community to address questions about the reliability and validity of certain types of evidence, such as whether the evidence has been adequately tested, what its error rate is, and whether there are standards for what constitutes a fingerprint match.[1] The U.S. Court of Appeals in U.S. v. Mitchell held that fingerprinting meets the necessary criteria for admissibility as evidence. More recently, in January 2002, in U.S. v. Llera Plaza, the judge refused to allow fingerprint experts to express an opinion that a particular latent print matched or did not match the rolled print of a particular person.[2] However, in March 2002, the judge reversed himself and concluded that the court's use of expert fingerprint identification testimony, subject to careful trial court oversight, could be allowed.

[1]U.S. v. Byron C. Mitchell (Criminal Action No. 96-407-1, U.S. District Court for the Eastern District of Pennsylvania 1999).

[2]U.S. v. Carlos Ivan Llera Plaza, Wilfredo Martinez Acosta, and Victor Rodriguez (Criminal Action No. 98-362-10, 11,12, U.S. District Court for the Eastern District of Pennsylvania 2002).

How the Technology Works

Fingerprint recognition technology uses the impressions made by the unique ridge formations or patterns found on the fingertips.[3] The technology uses two main types of fingerprints: flat and rolled. A flat fingerprint is obtained by pressing the finger flat against the scanner, capturing an impression of the central area between the fingertip and the first knuckle. A rolled fingerprint is obtained by rolling the finger from one edge of the fingernail across to the other, capturing an impression of the side ridges as well. A flat fingerprint is quicker to capture, but a rolled fingerprint can provide up to 50 percent more surface area for future comparisons.

Whether flat or rolled, the image of the fingerprint is commonly captured by a scanner based on optical, silicon, or ultrasound technology. Optical technology is the oldest and most widely used; it requires that the finger be placed on a coated platen, typically made of hard plastic. In most devices, a charged coupled device converts the image, with dark ridges and light valleys, into a digital signal. The brightness is adjusted automatically or manually to produce a usable image. Although most companies use optical technology, the trend is toward silicon.

One type of silicon technology is based on capacitance, where the silicon sensor typically acts as one plate of a capacitor and the finger is the other. The capacitance between the platen and the finger is converted into an 8 bit gray-scale digital image. Although ultrasound technology is potentially more accurate than either optical or silicon, its performance has not been assessed in widespread use. It captures the fingerprint by transmitting acoustic waves and measuring the distance by the impedance of the finger, the platen, and air.

After a fingerprint image has been captured, it is enhanced to reduce image noise, formed when a fingerprint is converted into a digital image; the noise distorts the image, generally as repetitive patterns or random dots. A fingerprint image is one of the noisiest of image types, predominantly because fingertips become dirty, cut, scarred, creased, dry, wet, and worn. Image enhancement reduces this noise and enhances the definition of ridges and valleys. To allow for precise locations of ridge features, ridges are thinned from an original width of 5 to 8 pixels down to 1 pixel.

[3]Ridges are the upper skin layer segments of the finger; valleys are the lower segments.

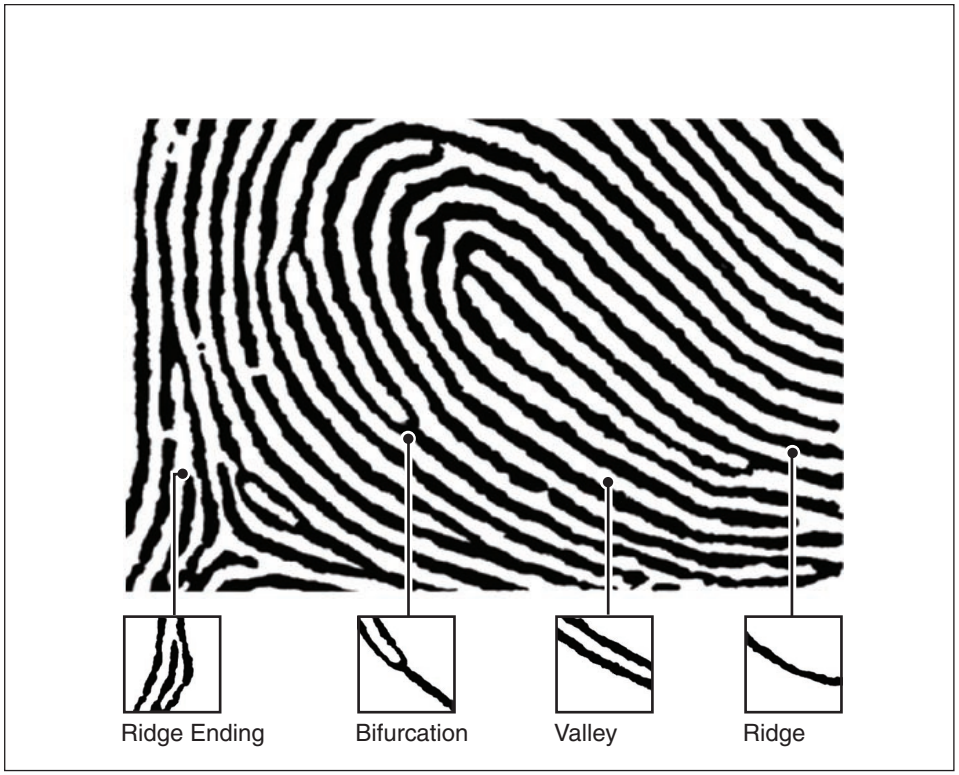
For a gray-scale image, areas lighter than a set threshold may be discarded, while darker areas may be made black. Image enhancement is relatively time consuming, since a 500 x 500 pixel fingerprint image has 250,000 pixels and each pixel is enhanced. Consequently, many fingerprint systems are designed to limit enhancement operations at this stage in order to reach a match result quickly, trading faster match time for poorer image quality.

Following image enhancement, several steps are required to convert a fingerprint's unique features into a template. Known as feature extraction, this is the basis of fingerprint recognition technology and the various vendors' proprietary algorithms. We discuss the different algorithms below. In none of these methods is the template a full fingerprint image, and a real fingerprint cannot be recovered from the digitized template. The generated template ranges from 250 bytes for minutiae-based templates to about 1,000 bytes for ridge-pattern-based templates.

Minutiae-Based Templates

Approximately 80 percent of fingerprint recognition vendors base their algorithms on minutiae points, or the breaks in fingertip ridges. A typical fingerprint image may produce between 15 and 50 minutiae, depending on the portion of the image captured. As shown in figure 29, the most basic minutiae are ridge endings (where a ridge ends) and bifurcations (where a single ridge divides into two).

Figure 29: Common Fingerprint Features



Source: GAO adaptation of FBI data.

Before minutiae can be identified, an algorithm must search the processed fingerprint image and filter out distortions and false minutiae. False minutiae can be caused by scars, sweat, or dirt and often create anomalies that can typically be detected. For instance, minutiae that seem out of place could include two ridge endings on a very short isolated line; the line would probably stem from image noise. Similarly, endings at the boundary of the fingerprint would be eliminated because they are not true endings but, rather, the edge of the image captured by the scanning device. A large percentage of minutiae candidates are discarded this way.

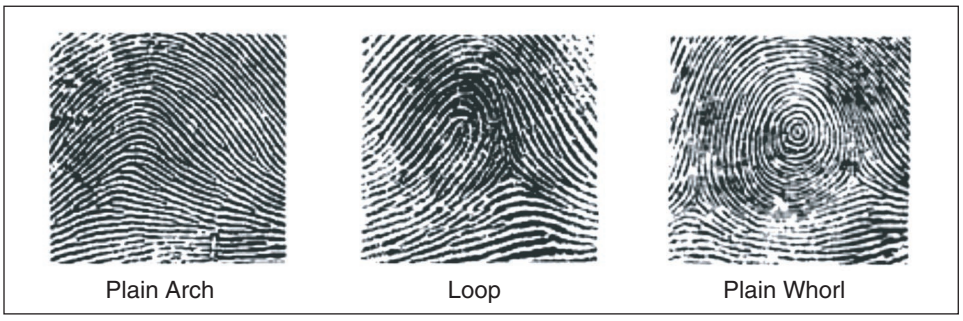
Once the minutiae are identified, their locations are usually set on an x,y axis and their angles are measured (typically by the direction of a ridge or valley ending). For each established minutiae point, neighboring minutiae and the number of ridges in between are recorded. The result of this stage is a minutiae template of the fingerprint. Because of differences in the

determination, placement, and analysis of minutiae points, no two algorithms can be expected to yield the same template from a given fingerprint.

In a verification system, templates are usually matched by comparing the neighborhoods of nearby minutiae for similarity. If a comparison indicates only small differences, the neighborhoods are said to match. Comparisons are performed exhaustively for all combinations of neighborhoods, and if enough similarities are found, the fingerprints are said to match. One result of this verification stage is a match score, usually a number between 0 and 1 (or 10 or 100). Higher values in the range indicate higher confidence in a match, and the match score is measured against a predetermined threshold. If the score is greater than the threshold, the match result is said to be true. The threshold can be lowered to reduce the number of false nonmatches, but the trade-off is a greater number of false matches. Some systems score the difference between two templates, in which case a lower score is considered a match.

In an identification system, which compares a trial fingerprint template to an entire database, the verification technique described above would be impractical. Making comparisons to every fingerprint in the database by neighborhoods would lengthen computation time extensively. Instead, a two-step process is typically used for 1:N matching. First, to provide an indexing method, the trial fingerprint and the reference template in the database are categorized according to an established fingerprint type (such as the plain arch, loop, or plain whorl shown in figure 30). This step is called binning, in which a pattern comparison quickly eliminates the bulk of the nonmatches. Care must be taken in binning. Errors in assigning images to bin categories increase the likelihood of a false nonmatch.

Figure 30: Established Fingerprint Types



Source: FBI.

In the second step for 1:N matching in identification, the trial template is compared by minutiae neighborhood to each reference template that closely matches the trial template pattern.

Ridge-Pattern-Based Templates

In matching ridge patterns, data are extrapolated from a particular series of ridges, to be used in enrollment for the basis of future comparisons. The ridge series are chosen so as to maximize the amount of unique information that is recorded—for example, those with an unusual ridge combination. At verification, a segment of the same area must be found and compared. The match result contains information on how well the stored images fit the verification image. This information is measured against a threshold to determine whether the match result is true.

The Leading Vendors

Fingerprint recognition technology companies number more than 75. There are more fingerprint recognition vendors than for all other biometrics combined. Some of the leading companies are listed in table 20.

Table 20: Leading Vendors of Fingerprint Recognition Biometrics

	Scanner for image capture			
Vendor	**Optical**	**Silicon**	**Ultrasound**	**Other[a]**
ActivCard	X			
Astro Datensysteme AG		X		
AuthenTec Inc.		X		
Bergdata Biometrics GmbH		X		
BIO-key International				X
BioLink Technologies International Inc.	X			
Biometric Access Corporation	X			
Bioscrypt Inc.	X	X		
Cogent Systems Inc.	X			
Cross Match Technologies Inc.	X			
Delsy		X		X
DigitalPersona Inc.	X			
Ethentica				X
Fingerprint Cards AB		X		
Identix Inc.	X			
Infineon Technologies AG		X		
Polaroid Corp.	X			
Precise Biometrics		X		
SAGEM Morpho Inc.	X			
SecuGen Corp.	X			
Siemens AG		X		
Sony Corp.	X	X		
STMicroelectronics		X		
Thales		X		
Ultra-Scan Corp.			X	
Veridicom Inc.		X		

[a]Includes middleware and emerging scan technologies that use polymer or fiber optic readers.

Source: GAO analysis of vendor data.

The Cost of Devices

Fingerprint readers designed for physical access control range from about $1,000 to $3,000 per unit. Software licenses for the fingerprint technology are about $4 per user enrolled. For smaller fingerprint scanners, maintenance costs are between 15 percent and 18 percent of cost. A live scan 10-print fingerprint reader costs about $25,000. The maintenance cost of the larger machines is approximately 14 percent of the cost of the reader.

Performance Issues

Although fingerprints are stable physiological characteristics, daily wear can cause the performance of some fingerprint recognition technologies to

drop drastically. Although high-quality enrollment improves long-term performance, the fingerprints of about 2 to 5 percent of people cannot be captured because the fingerprints are dirty or have become dry or worn from age, extensive manual labor, or exposure to corrosive chemicals. Also, IBG's comparative biometric testing has shown that certain ethnic and demographic groups (elderly populations, manual laborers, and some Asian populations) have fingerprints that are more difficult to capture than others'.

Optical and silicon scanning technologies have unique performance issues. Scanning fingerprints optically can be prone to error if the platen has a buildup of dirt, grime, or oil—producing leftover fingerprints from previous users, known as latent prints. Severe latent prints can cause the superimposition of two sets of prints and image degradation. Although silicon scanners generally produce a higher-quality image, high-quality fingerprint capture is more difficult because the sensor size is smaller than that used in optical scanners. Ultrasound scanning technology is designed to penetrate the dirt and residue on platens.

Optical and silicon scanners using minutiae-based and pattern-matching technologies have been tricked into accepting reactivated latent prints or artificial fingers with forged fingerprints. Latent fingerprints were reactivated by simply breathing on the sensor or by placing a water-filled plastic bag on the sensor's surface. Latent fingerprints could also be reconstructed and authenticated by dusting the sensor's platen with commercially available graphite powder and lifting with adhesive tape. Artificial fingers made with candle wax or gelatin and the fingerprints of enrolled individuals have also successfully fooled the system.

User Acceptance

Because law enforcement agencies identify criminals with fingerprints, the recognition technology's similarity to forensic fingerprinting causes some percentage of users discomfort. Privacy advocates fear that fingerprint recognition systems may collect data for one purpose but then use the data for other purposes, such as in forensic applications or for tracking people's activities. Also, people may have hygiene issues with touching the plate of a scanner that many people have touched.

The Technology's Maturity

Operational Uses

The FBI's IAFIS is an automated 10-fingerprint matching system that relies on rolled fingerprints. The more than 40 million records in its criminal master file are connected electronically with all 50 states and some federal agencies. IAFIS was designed to handle a large volume of fingerprint checks against a large database of fingerprints. It processes, on average, approximately 48,000 fingerprints per day and has processed as many as 82,000 in a single day. IAFIS's target response time for criminal fingerprints submitted electronically is 2 hours; for civilian fingerprint background checks, 24 hours. According to FBI data from August 2002, the majority of criminal fingerprints were answered in less than 7 minutes and the majority of civilian fingerprints were answered in less than 4 minutes; 88.2 percent of criminal prints and 66.1 percent of civilian prints were completed in less than 2 hours. For fingerprint submissions in paper-card format, the response time is 3 days between receipt and mailed-back response. The FBI claims that IAFIS has a false match rate (FMR) of about 1.5×10^{-12} with a false nonmatch rate (FNMR) of about 1.5 to 2.0 percent. The failure to enroll rate (FTER) is about 0.5 percent for criminal searches and about 2.5 percent for civilian background searches.

INS began developing the Automated Biometric Fingerprint Identification System (IDENT) around 1990 to identify illegal aliens who are repeatedly apprehended trying to enter the United States illegally. INS's goal was to enroll virtually all apprehended aliens. IDENT can also identify aliens who have outstanding warrants or who have been deported. When such aliens are apprehended, a photograph and two index fingerprints are captured electronically and queried against three databases (see figure 31). One database stores the fingerprints and photographs of approximately 300,000 aliens INS has previously apprehended; it tracks the number of apprehensions. The second database stores the fingerprints and photographs of approximately 240,000 criminal aliens convicted of an aggravated felony, among other criteria. The third database stores the fingerprints and photographs of more than 4 million illegal aliens who were apprehended, enrolled in IDENT, and then permitted to voluntarily depart the United States or to withdraw their applications for admission at ports of entry. The fingerprint query of the three databases normally takes 2 minutes. In March 2002, the FMRs for the four fingerprint search types were 4.05 percent for flat to flat, 2.60 percent for flat to roll, 0.70 percent for roll to roll, and 1.19 percent for roll to flat.

Figure 31: An IDENT Workstation



Source: INS.

A number of states (including Arizona, California, Connecticut, Illinois, Massachusetts, New Jersey, New York, and Texas) require applicants for welfare benefits to submit their fingerprints in order to eliminate duplicate participation and to deter fraud. The first social service fingerprint recognition system in the nation was the Los Angeles County Automated Fingerprint Image Reporting and Match system, which enrolled 311,000 clients between 1992 and 1995. On the basis of a study group of 24,000 fingerprint recipients, it was determined that about 7 percent of the cases on the benefit rolls in Los Angeles were multiple identities. As of January 2001, this was the only substantial finding of multiple identity fraud in any of the various state welfare fingerprint programs.

Since January 31, 2002, immigrants seeking asylum in the United Kingdom are issued an application registration card to allow for quick and positive identification of all asylum applicants. The smart cards, manufactured by SAGEM Morpho Inc., store two fingerprint templates on a memory chip. An extension of the Immigration and Asylum Fingerprint System (IAFS), they are intended to prevent fraudulent behavior, such as impersonations to avoid removal or to make false benefits claims. The United Kingdom plans to adopt the Eurodac Convention and Protocol, which assists European Union members in applying the provisions of the Dublin Convention, a framework for ensuring that an asylum claim is heard within the European Union only once. Once the United Kingdom has

adopted the Eurodac Convention and Protocol, British IAFS fingerprint data will be transmitted electronically to a central database, accessible to other members for fingerprint comparisons. The data will be retained for 10 years, with the exception of fingerprints from asylum seekers who are granted citizenship by European Union members. The prints of these new citizens will be immediately erased.

Pilots

FAA Fingerprint Recognition Testing

In 2001, FAA conducted operational testing of a fingerprint recognition reader for access control by different groups of people in various operating environments. Following the test, the biometric system was removed. Enrolling users in the fingerprint reader system took an average of 3 minutes and 30 seconds. Two of 38 users were unable to enroll because of the poor quality of their fingerprints. Passing through the door took about 10 seconds using fingerprint recognition, compared to an average of about 2 seconds before the device was installed. Performance rates varied at the three different security-level thresholds tested. The FNMR ranged from about 6 percent to about 17 percent for closely controlled test subjects. For actual airport employees using the door in a less controlled environment, the FNMR ranged from about 18 percent to about 36 percent. The FMR ranged from 0 percent at the highest security level to approximately 8 percent at the lowest security level.

O'Hare International Airport, Chicago

In 1998, FAA funded an operational test at Chicago's O'Hare International Airport involving smart cards and fingerprint recognition identification devices to screen employees of motor carrier and air cargo companies at access control points to cargo areas. Truck drivers were instructed to insert a smart card into the smart card reader and to confirm their identity by placing the enrolled fingers on the fingerprint reader.[4] Fingerprints were chosen over other biometrics because of the users' operational requirements, the perception that fingerprint recognition was one of the least intrusive technologies, and the results from a 1997 study that determined that fingerprints could be used in a variety of applications in the trucking industry.

[4]To allow for scarred or injured fingers, drivers typically enrolled two digits.

Because all users' verification attempts were voluntary, only some of the users who were initially rejected by the system chose to try again. For 65 users, the first-try FNMR was 28 percent. Of the seven users who chose to try again, 71 percent successfully accessed the system. If all rejected users had retried with this rate of success, only 8 percent of the users would have been rejected after two tries.[5] Testing of impostors' fingerprints against the operational database was not performed, so an FMR could not be obtained for the O'Hare databases.

Tests

Fingerprint Verification Competition 2000

The Fingerprint Verification Competition 2000 (FVC 2000) tested relative technology performance in a one-to-many application and was not intended to predict performance of fingerprint recognition technology in a real environment. Eleven algorithms were submitted, seven from academic groups and four from companies (one from Ditto Information & Technology Inc., one from FingerPin AG, and two from SAGEM Morpho Inc.). Three databases in this competition were acquired in a laboratory environment, using a variety of sensors (both optical and silicon), while the fourth contained synthetically generated images. Enrollment time averaged 0.20 to 10.42 seconds, 10 of the algorithms requiring no more than 3.18 seconds. Matching time averaged 0.20 to 2.67 seconds, 9 of the algorithms requiring no more than 1.58 seconds. The most accurate algorithm had an average equal error rate (EER) of 1.73 percent, while the least accurate algorithm had an average EER of 47.84 percent. These data are depicted in table 21.

[5]FNMR analysis from system performance testing by Jim L. Wayman, U.S. National Biometric Test Center, College of Engineering, San Jose State University, San Jose, California.

Table 21: Summary of Results from the Fingerprint Verification Competition 2000

Participant	Type	Average EER	Average enroll time	Average match time
SAGEM SA, France (Algorithm 1)	Company	1.73%	3.18	1.22
SAGEM SA, France (Algorithm 2)	Company	2.28	1.11	1.11
Centre for Signal Processing, Nanyang Technological University, Singapore	Academic	5.19	0.20	0.20
CEFET-PR/Antheus Technologia LTDA., Brazil	Academic	6.32	0.95	1.06
Centre for Wavelets, Approximation, and Information Processing, Department of Mathematics, National University of Singapore, Singapore	Academic	7.08	0.27	0.35
Kent Ridge Digital Labs, Singapore	Academic	10.94	1.08	1.58
University of Twente, Electrical Engineering, Netherlands	Academic	15.24	10.42	2.67
FingerPin AG, Switzerland	Company	15.94	1.22	1.27
Inha University, Korea	Academic	19.33	0.71	0.76
Ditto Information & Technology Inc., Korea	Company	20.97	1.24	1.32
Natural Sciences and Mathematics, Institute of Informatics, Macedonia	Academic	47.84	1.44	1.71

Note: Time is in seconds.

Source: FVC 2000.

Fingerprint Verification Competition 2002

Researchers from University of Bologna, Italy; San Jose State University, California; and Michigan State University, East Lansing; jointly conducted Fingerprint Verification Competition 2002 (FVC 2002), a large-scale evaluation of fingerprint recognition technology that was a follow-up to FVC 2000. There were 31 participants—21 from companies, 6 from academic institutions, and 4 others. As in FVC 2000, three databases were acquired in a laboratory environment, using both optical and silicon sensors, and a fourth contained synthetically generated images.

Enrollment time averages ranged from 0.11 to 7.05 seconds, 24 of the participants requiring no more than 1 second. Matching time averages ranged from 0.18 to 5.01 seconds, 21 of the participants requiring no more than 1 second. The most accurate algorithm had an average EER of 0.19 percent, while the least accurate algorithm had an average EER of 50 percent. Table 22 depicts these data.

Table 22: Summary of Results from the Fingerprint Verification Competition 2002

Participant	Type	Average EER	Average enroll time	Average match time
Bioscrypt Inc., United States (Algorithm 1)	Industrial	0.19%	0.11	1.97
Anonymous	Industrial	0.33	2.12	1.98
Anonymous	Industrial	0.41	1.23	1.13
Bioscrypt Inc., United States (Algorithm 2)	Industrial	0.77	0.07	0.22
Siemens AG, Germany	Industrial	0.92	0.48	0.52
Neurotechnologija Ltd., Lithuania	Industrial	0.99	0.56	0.56
SAGEM, France (Algorithm 1)	Industrial	1.18	4.05	1.65
Andrey Nikiforov (Independent Developer), United States	Other	1.31	0.81	1.23
SAGEM, France (Algorithm 2)	Industrial	1.42	0.77	0.66
Deng Guoqiang (Independent Developer), China	Other	2.18	0.17	0.48
IDENCOM AG, Switzerland	Industrial	2.22	0.52	0.62
Suprema Inc., Korea	Industrial	2.50	0.54	0.63
Anonymous	Industrial	3.31	0.53	0.65
Biometrics System Lab, Beijing University of Posts and Telecommunications, China	Academic	3.76	0.57	0.59
Anonymous	Industrial	4.19	0.18	0.18
HZMS Biometrics Co. Ltd., China	Other	4.24	0.65	0.66
ActivCard Canada, Canada	Industrial	5.21	0.68	1.76
Antheus Tecnologia Ltda, Brazil	Industrial	5.46	0.20	0.54
TeKey Research Group, Israel	Industrial	5.72	0.01	3.15
FINGERPIN AG, Switzerland	Industrial	6.05	0.48	0.77
Inha University, Korea	Academic	6.07	0.80	0.84
Aldebaran Systems, United States	Industrial	6.16	1.81	1.81
Digital Fingerpass Corporation, China	Industrial	6.40	0.49	0.50
DATAMICRO Co. Ltd., Russia	Industrial	6.72	0.33	0.56
Anonymous	Industrial	7.12	0.24	0.28
Department of Computer Science and Information Engineering, Da-Yeh University, Taiwan	Academic	9.04	0.13	0.15
Anonymous	Industrial	12.09	0.68	0.70
AILab, Institute of Automation, The Chinese Academy of Sciences, China	Academic	14.66	0.57	0.65
University of Tehran, Electrical and Computer Department, Iran	Academic	16.79	1.16	1.19
Anonymous	Other	39.10	0.52	0.63
Anonymous	Academic	50.00	7.05	5.01

Note: Time is in seconds.

Source: FVC 2002.

Biometric Product Testing

NPL conducted a performance evaluation of seven different biometric systems from May to December 2000. The fingerprint part of the test included two types of systems, one based on optical technology and the other on silicon technology. The vendor of the silicon sensor was VeriTouch Ltd., with alternative enrollment and matching algorithms provided by Infineon Technologies AG. The vendor of the optical sensor was not identified.

The silicon system's FTER was 1.0 percent, the optical system's 2.0 percent. FMR and FNMR measure the accuracy of the matching process. Adjusting the decision criteria can make for a trade-off between false match and false nonmatch errors. At an FMR of about 2 percent, the FNMR was about 4.3 percent for the silicon sensor with the alternative algorithm. Additional experimental results are summarized below:

- The silicon sensor system had a mean transaction time of 19 seconds, a median of 15 seconds, and a minimum of 9 seconds. The optical fingerprint system had a mean transaction time of 9 seconds, a median of 8 seconds, and a minimum of 2 seconds.

- The silicon sensor system could make 60 matches per minute, the alternative algorithm 2,500 matches per minute. The optical system could make only 50 matches per minute. These diagnostic programs had significant overheads, so the matching algorithm may be significantly faster than the results showed, perhaps by a factor exceeding 100.

- For both the silicon sensor and the optical system, younger people generally had a lower FNMR than older people, and the FNMR for attempts made immediately following enrollment were lower than those made on second or third visits.

Republic of the Philippines Social Security System Identification Card Benchmark Test

In May 1997, the U.S. National Biometric Test Center at San Jose State University conducted an automated fingerprint identification system (AFIS) benchmark test for the Republic of the Philippines Social Security System Identification Card Project. The test measured single comparison FMRs and FNMRs (among other metrics) for each of the four participating international AFIS vendors. The FMR and FNMR for each vendor were

determined by matching 4,128 test images against a database of 4,080 fingerprints. Flat prints of the thumb through the ring finger of each hand were collected from adult employee volunteers in the Social Security System. One vendor returned 16 million cross comparisons with only one false match, indicating a 95 percent statistical confidence in an FMR of fewer than 3 in 10 million prints but with an FNMR approaching 20 percent. Statistical analysis of the test results supports the feasibility of an AFIS system that could support 16 million flat fingerprint comparisons without a false match.

INS's IDENT Benchmark Test

In June 1998, an independent verification and validation test was conducted on the Cogent PMA3 Matcher configuration that was later installed for IDENT. This benchmark test used a fingerprint test database created by INS and provided to Cogent Systems Inc. that consisted of 129,712 rolled fingerprints, 951,956 flat fingerprints, and six different search fingerprint image input files. The data were highly representative of IDENT criminal alien records at the time. As about half of the search subjects in the input files had mates in the rolled or flat fingerprint database, the benchmark data were designed to obtain results with a high confidence level.

All four types of searches (flat-flat, roll-flat, flat-roll, and roll-roll) in operation in IDENT were tested during the benchmark. Two verification match tests (flat-flat and flat-roll) were also conducted. The results are displayed in table 23.

Table 23: INS's IDENT Fingerprint Benchmark Test Results, 1998

	Identification		Verification	
Match test	**FNMR**	**FMR**	**FNMR**	**FMR**
Flat to flat	0.4%	5.4%	0	0.1%
Roll to flat	8.4	1.5	[a]	[a]
Flat to roll	7.3	0.2	1.6%	0.1
Roll to roll	0.2	0.1	[a]	[a]

[a]Data not available.

Source: GAO analysis of INS data.

The results of the flat-to-flat and roll-to-roll search test were more accurate than those of the mixed media tests—roll-to-flat and flat-to-roll—because the mixed media searches resulted in a higher FNMR. The results of the verification match test supported the use of the algorithm for future INS verification applications.

Border Control Applications Piloted and Deployed

CANPASS–Airport

The CANPASS–Airport pilot at Vancouver International Airport was initiated in October 1995 using both fingerprint recognition and hand geometry technologies. The pilot used identity cards and biometric identification devices to allow previously screened travelers to bypass customs and immigration lines. Qualified Canadian and U.S. residents entered Canada through a special line by opening an automated gate with an encoded identification card and providing a fingerprint or hand geometry biometric for one-to-one authentication. Roughly a thousand travelers registered with CANPASS in the pilot's first 7 months, with an average enrollment time of 15 minutes. Of 1,385 authentication attempts, 87 percent were successful and 13 percent were falsely rejected by the technology and had to be processed manually. On the basis of these results, authorities decided to use solely hand geometry for CANPASS–Airport.

Border Biometric Program and Border Crossing Card

The biometric border crossing card project is a joint effort of the Department of State and INS to replace the paper-based card previously issued to Mexican citizens. The new card is a laser visa, a credit-card-like document, that permits the holder to enter the United States without being issued further documentation for business or pleasure and to stay for 72 hours or less, going no farther than 25 miles from the border. With additional documentation, the laser visa can permit longer stays and travel farther than 25 miles from the border. The laser visas are manufactured by LaserCard Systems Corp. and are made of polycarbonate material with a rectangular strip of optical memory for data storage. The cards store a frontal facial image and the templates of two index flat fingerprints. More than 5 million cards have been issued, but the performance of the fingerprint recognition technology has not been measured, because ports of entry have no scanners for reading travelers' fingerprints and matching them with the information on the laser visa. INS is buying and installing 30 readers at six ports of entry for a pilot test.

Hong Kong Resident Smart Cards

About 250,000 people cross the Hong Kong–Shenzhen border daily, causing long lines at the immigration checkpoint. The Hong Kong government plans to issue new identity smart cards to residents in 2003. The smart cards will hold a template of a rolled fingerprint to be matched against the bearer at a self-service kiosk. The $21 million smart card contract was awarded in March 2002, and distribution to the 6.8 million Hong Kong residents will be phased in over 4 years.

Processing Issues

The size of an identification system's projected database has a significant effect on the system's configuration and cost. The larger the database, the more storage devices are required. In addition, it takes longer to search a larger database unless matching processor power is also increased. Database size can also affect a system's accuracy. Some matching algorithms are effective only with relatively small databases and are simply not capable of accurate matching against the larger numbers of records found in forensic automated fingerprint identification systems.

Device Durability and Environmental Constraints

Capturing fingerprints has been a significant issue in border control pilots. In an unattended environment, trained users have generally skewed fingers or have not pressed hard enough on the platen. The difficulty of acquiring a usable fingerprint after three attempts has resulted in approximately a 50 percent rejection rate. In addition, fingerprint readers do not operate below freezing temperature, so the issues of freezing and condensation are significant in selecting biometric systems.

Appendix III: Hand Geometry Technology

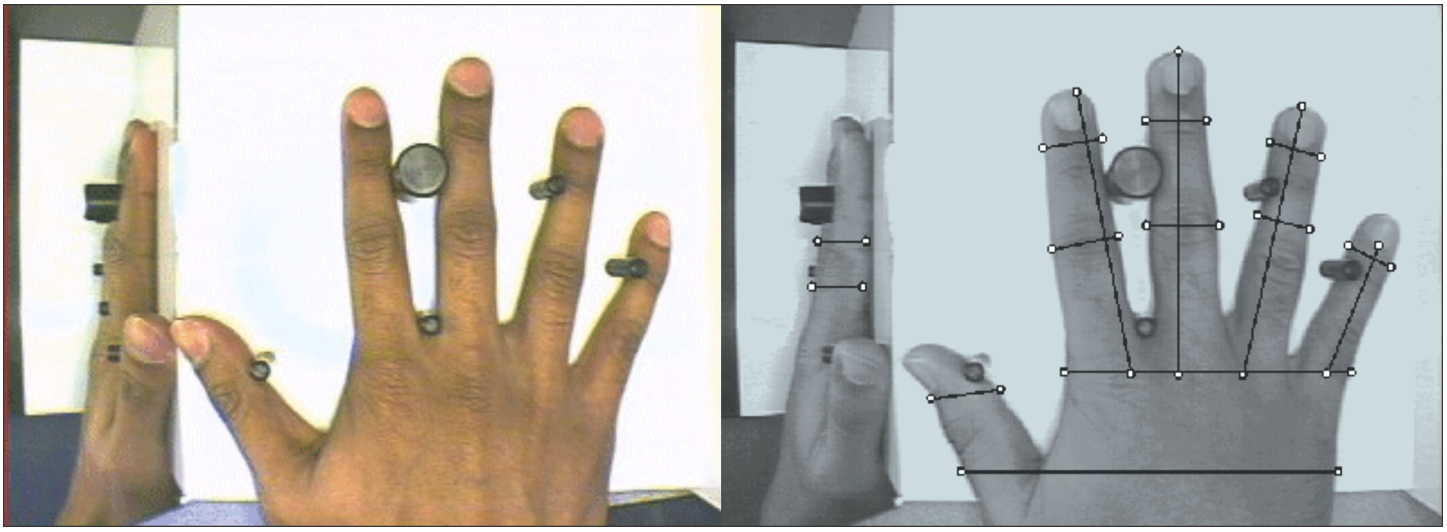
Patents for hand geometry technology were first issued in the late 1960s and early 1970s. The technology is based on the premise that the hand's bone structure, while changing over time, remains characteristically the same. The hand's shape usually stabilizes at age 13 or 14.

How the Technology Works

Hand geometry technology uses the hand's distinctive features, particularly the height and width of its back and fingers, to verify a person's identity. In measuring size and shape, a hand geometry system collects more than 90 dimensional measurements, including finger width, height, and length; distances between joints; and knuckle shapes. Although the shape and size of our hands are reasonably diverse, they are not necessarily unique. In larger populations, for example, it is almost certain that various people have very similar hand dimensions. Consequently, the technology cannot be used for 1:N identification.

In the measurement of the different features, a person places his or her hand flat on the device's metal surface, where pegs guide the fingers into position. Hand geometry systems require a person to squeeze his or her fingers against the pegs to prevent spoofing. Cameras capture two orthogonal two-dimensional images of the back and sides of the hand (see figure 32).

Figure 32: Fingers Guided by Pegs in a Biometric Hand Geometry Measurement



Source: Michigan State University, Biometrics Research Group.

Only the spatial geometry is acquired; prints of the palm and fingers are not taken. The derived template is 9 bytes in size, the smallest in the biometric industry. In a process known as template averaging, the template is automatically updated whenever the difference between the individual's hand and his or her reference template exceeds a designated threshold.

The Leading Vendors

Recognition Systems Inc. (RSI) dominates the market in hand geometry technology. Its systems are used in nearly every current implementation. Companies that integrate hand geometry technologies include Electronic Data Systems Corp. and ADT. However, Dermalog, a German company, is developing an alternative technology that uses a pegless device. Biomet Partners, a Swiss company, sells a finger geometry device that operates on the same basic principles as the RSI hand geometry devices.

The Cost of Devices

Hand geometry devices generally cost between $2,000 and $4,000. Training is minimal, and no personnel costs are incurred because most hand geometry devices are typically unattended.

Performance Issues

Hand geometry disregards fingernails and surface details such as fingerprints, lines, scars, and dirt. Except for jewelry, arthritis, water retention, and swelling from pregnancy or hand injury, the hand is not susceptible to major changes that would affect the technology's accuracy. However, because measurements of the hand are not distinct over a large population, false matches can occur. Therefore, hand geometry is not effective in large-scale1:N applications or in applications where resistance to impostors is essential.

User Acceptance

Hand geometry is generally perceived as nonintrusive, nonthreatening, and noninvasive, and it bears very little of the stigma of other biometric technologies. It lacks the forensic association that may affect users' perceptions of fingerprint recognition systems. It is considered easy to use, although a minimal amount of training may be required to learn how to align the hands in the device. However, some people are uncomfortable touching a device that many people have previously touched.

The Technology's Maturity

Operational Uses

Hand geometry is an established, mature, and reliable technology that has remained unchanged for several years. Hand geometry systems have been deployed since the 1980s in tens of thousands of locations for access and entry control, personal identification, and time and attendance applications. For example, hand geometry is the most commonly deployed biometric technology for controlling physical access and for processing time and attendance records. Devices used for time and attendance applications are often tied into physical access control systems. Hand geometry devices have been installed at the entrances to more than half the nuclear power plants in the United States. In 1991, San Francisco International Airport installed hand geometry devices to protect secure areas such as the tarmac and loading gates. At the 1996 Olympic Games in Atlanta, Georgia, athletes used a hand geometry system to gain access to Olympic Village.

Tests

FAA Hand Geometry Testing

In 2001, FAA and the National Safe Skies Alliance evaluated the effectiveness of hand geometry technology for the use of access control of airport employees. Following the test, the biometric system was removed. Of the 39 people who successfully enrolled, 27 enrolled in an average of 57 seconds. The hand geometry system had varying security-level settings, resulting in differing performance rates at verification. The FNMR ranged from approximately 5 percent at a high security-level setting to less than 1 percent at a low security-level setting. The FMR ranged from approximately 0 percent at the high security-level setting to about 2 percent at the low security-level setting. Before the biometric technology was installed, passing through the door was estimated at 2 seconds; after installation, the time increased to 8 seconds.

The results of testing under abnormal conditions are summarized below:

- At the default security level setting, adding or removing rings similar to the wide-band ring used in this test would very likely cause users to be rejected at a high rate. Smaller rings do not appear to cause a higher FNMR.

- Wearing gauze pads or splints to cover injuries would also probably cause a higher rejection rate. Standard adhesive bandages three-quarter inches wide do not appear to cause higher FNMRs.

- High backlight conditions did not noticeably affect FNMR.

Biometric Product Testing

From May to December 2000, NPL evaluated seven different biometric technologies in a real-world environment for positive verification comparative testing. The hand geometry portion of the test used RSI's Hand Key II, which had the fastest transaction time of the biometric technologies compared. With 200 people enrolled, the FTER was 0 percent. At an FMR of about 1 percent, the hand geometry system had an FNMR of approximately 1.4 percent. Additional experimental results were

- The Hand Key II had a mean transaction time of 10 seconds, a median of 8 seconds, and a minimum of 4 seconds.

- The matching algorithm could make 80,000 matches per minute when using a SunUltra5 with a SunOS5.8 operating system, 270 MHz processor, and 128 MB of memory.

- Males had a somewhat lower FNMR than females.

Sandia National Laboratories

In 1991, Sandia National Laboratories evaluated five biometric technologies, with nearly a hundred volunteers testing each technology. Nearly 20,000 transactions were recorded for RSI's ID-3D hand geometry devices. Overall, the hand geometry technology was the fastest, most accurate, and most user-friendly device. Average verification time was 5 seconds, and the EER was about 0.2 percent. At the test threshold value, the three-try FNMR was less than 0.1 percent, and the one-try FMR was 0.1 percent.

Sandia National Laboratories performed a field analysis with hand geometry for physical building access control from 1993 to 1995. RSI's model ID-3D HandKey biometric verifier was tested. Overall, 316 people used the device in more than 100,000 instances. Sandia concluded that the device operated differently in an exterior, unattended field installation than in previous laboratory experiments: 7.20 percent of the individuals failed in the first verification attempt, 53.48 percent in the second, and

66.49 percent in the third. These percentages are not equivalent to FNMRs, since not enough information was available to determine whether users who were rejected should have been accepted. They may have been correctly rejected because they may not have been who they claimed to be. Researchers also found that maintenance and cleaning were paramount; when the readers were not cleaned properly, performance was severely degraded.

Border Control Applications Piloted and Deployed

INSPASS

Hand geometry is being used in many border control environments. The INS Passenger Accelerated Service System (INSPASS), installed at seven U.S. and two Canadian airports, uses 29 hand geometry kiosks to reduce inspection time to less than 15 seconds for trusted travelers (see figure 33). INSPASS enrollment is open to all citizens of the United States, Canada, Bermuda, and visa waiver countries. To enroll, travelers must provide a passport or travel document and two fingerprints and present their hand geometry biometric.

Figure 33: A Traveler Using an INSPASS Hand Geometry Device



Source: IR—Recognition Systems.

Ben Gurion Airport

Since 1998, Ben Gurion Airport in Tel Aviv, Israel, has installed 21 hand geometry kiosks and enrolled more than 100,000 passengers. The implementation was initially offered only to frequent international travelers, but passenger demand led to its expansion to all Israeli citizens. Each month, more than 50,000 travelers use the automated passenger screening system to reduce the immigration process to about 15 seconds. When using the system, a traveler swipes a magnetic stripe card over a biometric reader (see figure 34). More than 2 million inspections have been performed, and they are growing at 2 percent a month. In addition to biometric authentication, the system checks the biometric against Israeli law enforcement and immigration databases.

Figure 34: A Traveler Using Ben Gurion Airport's Biometric Hand Geometry System



Source: IR—Recognition Systems.

Basel Project

Headed by Electronic Data Systems, the Basel Project will implement a system using facial recognition and hand geometry for day workers crossing into and out of Israel from the Gaza Strip. Fingerprint technology was rejected because the primary users are laborers whose fingerprints are not reliable for biometric matching. People will enroll at the Israel-Palestine land border, receiving a contactless smart card with a high-resolution picture and a hand geometry biometric. When entering or leaving Israel, they will be processed through 42 routing passages to unattended checkpoints at verification terminals inside a building. It is estimated that 60,000 verifications will be processed daily in one-to-one matches against stored templates in a central server, with a backup stored on the smart card.

Port of Rotterdam

In June 1999, the Port of Rotterdam, Europe's busiest container port, implemented a hand geometry system designed to speed cargo movement. Each truck driver's identity is verified with the biometric template stored on a radio frequency smart card, accessed through the truck's window. It has more than 6,000 users and has logged more than 3 million transactions.

CANPASS–Airport

The CANPASS–Airport pilot at Vancouver International Airport was initiated in October 1995 using both fingerprint recognition and hand geometry technologies. The pilot used identity cards and biometric identification devices to allow previously screened travelers to bypass customs and immigration lines. Qualified Canadian and U.S. residents entered Canada through a special line by opening an automated gate with an encoded identification card and providing a fingerprint or hand geometry biometric for one-to-one authentication. The system's use was discontinued on September 11, 2001.

Device Durability and Environmental Constraints

Hand geometry is well suited for most environments. The equipment is durable and can withstand most workload demands. Various types of hand geometry devices on the market are suitable for all types of climates (see figures 35 and 36). Most can withstand temperatures ranging from –45 degrees to 120 degrees Fahrenheit and can provide protection against snow, sleet, rain, splashing water, hose-directed water, falling dirt, and wind-blown dust.

Figure 35: A Typical Hand Geometry Recognition Device



Source: IR—Recognition Systems.

Figure 36: A Hand Geometry Recognition Device That Is Enclosed



Source: IR—Recognition Systems.

Appendix IV: Facial Recognition Technology

Every day, people identify other people by their faces. Much research has yielded evidence that people may recognize others' faces through a unique process that highlights the importance of the location and shape of eyes, nose, and eyebrows and face shape, chin, lips, and mouth, in decreasing order. Because this process differs from how we recognize other objects, the idea that machine recognition systems should also be face-specific may have been encouraged. However, just as some people may have difficulty differentiating between identical twins and other people with similar features, facial recognition technology also cannot effectively distinguish between people who resemble one another, and it still requires development to full maturity. Nevertheless, active research over the past 10 years has made the technology commercially available.

How the Technology Works

Facial recognition identifies people by the sections of the face that are less susceptible to alteration—the upper outlines of the eye sockets, the areas around the cheekbones, the sides of the mouth. Systems using this technology capture facial images from video cameras and generate templates for comparing a live facial scan to a stored template. Facial recognition technology can also be used to compare static images, such as digitized passport photographs.

The comparisons are used in verifying and identifying individuals. Verification systems compare a person's facial scan to a stored template for that person and can be used for access control. In an identification system, a person's facial scan is compared to a database of multiple stored templates. This makes an identification system more suitable for surveillance in conjunction with closed-circuit television (CCTV) to spot suspected criminals whose facial characteristics have been captured and stored in a database on a template. The face is the only biometric used in a viable recognition technology that is able to operate without a user's cooperation, since a CCTV camera need only capture a picture for the technology to generate a template. However, the technology is much more able to identify people who are motivated to use the system correctly than those who are uncooperative and can avoid recognition by, for example, using disguises or taking other evasive measures.

The primary facial recognition technologies are used for one-to-one as well as one-to-many matching. Whether used for verification or identification, the stored image templates must be kept up to date, since appearances naturally alter with age.

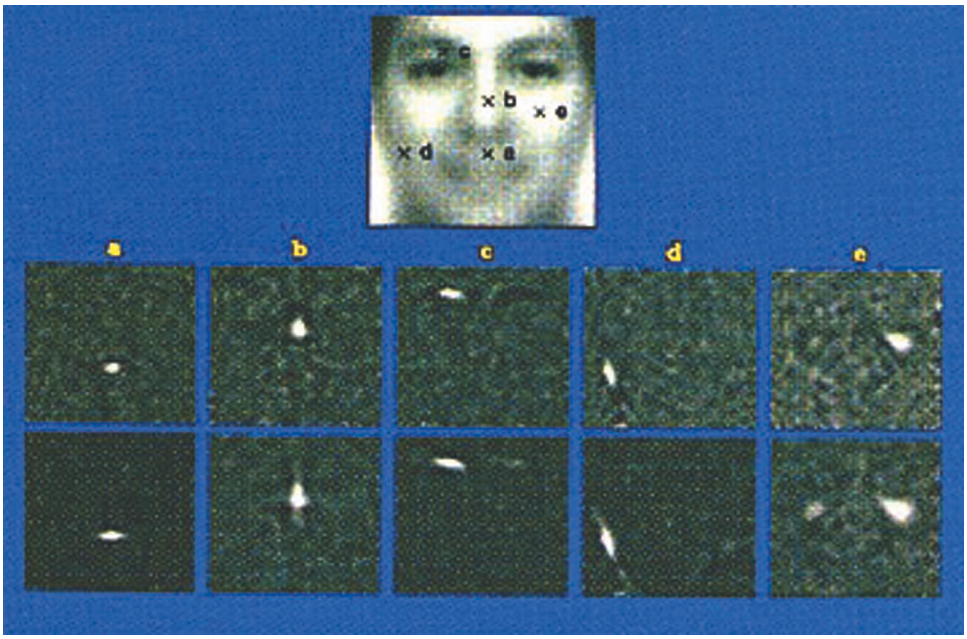
However, IBG's testing has found that the core technology is highly susceptible to falsely nonmatching users in one-to-one verifications and to failing to identify enrolled users in one-to-many identifications.

Two primary types of facial recognition technology are used to create templates.[1] Requiring as many as 1,300 bytes, or as few as 84 bytes, they are local feature analysis (LFA) and the eigenface method.

Local Feature Analysis

Patented by Visionics Corp.—now Identix Incorporated—LFA uses dozens of images from regions of the face, resulting in feature-specific fields—eyes, nose, mouth, cheeks. The fields' relative locations are incorporated so that the face can be represented as a topographical grid made up of blocks of features. The features represented by these blocks and their positions are used to identify or verify the face (see figure 37).

Figure 37: Local Feature Analysis: A Topographical Grid of Facial Regions



Source: Identix Incorporated.

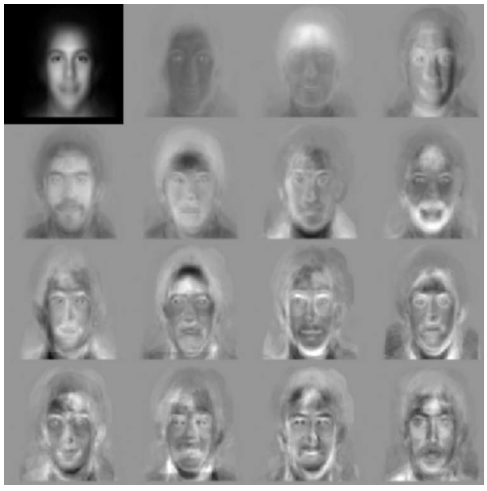
[1]Other facial recognition technologies based on thermal patterns below the skin are not yet commercially viable.

Just as Washington, D.C., can be identified by describing its landmarks' locations and their relative positions (e.g., the National Mall has the U.S. Capitol building to its east, the Lincoln Memorial to its west, and the Washington Monument and Smithsonian museums at its center), a person's face can be identified by the features defined by LFA. Small shifts in a feature may cause a related shift in an adjacent feature and the technology can accommodate these changes in appearance or expression (such as smiling or frowning). Since LFA does not provide a global representation of the face, it is rendered ineffective when a person tilts his or her head from a direct frontal pose to more than about 25 degrees horizontally or more than about 15 degrees vertically.

The Eigenface Method

Eigenface, meaning roughly "one's own face," is a technology patented at the Massachusetts Institute of Technology. Unlike LFA, the eigenface method always looks at the face as a whole. A collection of facial images is used to generate a set of two-dimensional, gray-scale images (eigenfaces) to produce the biometric template (see figure 38). The vast majority of faces can be represented by locating distinctive features from approximately 100 to 125 eigenfaces. When a live image of a person's face is introduced, the system represents the image as a combination of templates. This combination is compared with a set of stored templates in the system's database, and the degree of variance determines whether or not a face is recognized.

Figure 38: Two-Dimensional, Gray-Scale Images of an Eigenface Template



Source: Baback Moghaddam, MIT Media Laboratory.

Modifications of the algorithms used in LFA and the eigenface method can lead to variances that incorporate

- Neural network mapping: Comparisons of a live facial image with a stored template are based on unique global features rather than individual features. When a false match is made, the comparison algorithm modifies the weight given to certain features, such as shadows.
- Automatic face processing: Facial images are captured and analyzed from the distances and distance ratios between features, such as between the eyes.

The Leading Vendors

The leading algorithms are licensed by Identix Inc. (which merged with Visionics in June 2002) and Viisage Technology. Identix uses local feature analysis; Viisage's algorithm is based on the eigenface method.

The Cost of Devices

A facial recognition server controlling access at a facility with up to 30,000 persons would cost about $15,000. Depending on the number of entrances with installed facial recognition technology, the cost of the software licenses would range from about $650 to $4,500. As the size of the database and the number of attempted matches increased, so would a system's cost.

In addition to the server and software licenses, a live-scan facial recognition surveillance system includes CCTV surveillance (see figure 39). A fully integrated CCTV system for physical access surveillance can cost from $10,000 to $200,000, depending on the size of the entrance and the degree of monitoring required. For additional CCTV equipment, cameras can cost between $125 and $500. Cameras with advanced features can cost up to $2,300.

Figure 39: CCTV Surveillance Equipment



Source: Pelco.

Performance Issues

The effectiveness of facial recognition technology is influenced heavily by environmental factors, especially lighting conditions. Variations in camera performance and facial position, expression, and features (hairstyle, eyeglasses, beards) further affect performance. Accurate image alignment is necessary for the leading facial recognition algorithms, which rely on identifying eye positions. As a result, current facial recognition technology is most effective when used in consistent lighting with cooperative subjects in a mug-shot-like position—where hats and sunglasses are removed and everyone looks directly at the camera one at a time.

Attempts to spoof live-scan facial recognition systems have been successful. In one test, trial images were obtained by downloading unprotected reference facial images to a computer and by taking digital pictures of an enrolled person. These images were displayed on a notebook computer monitor and were successfully matched, granting testers access to the system. A video of an enrolled person moving his head slightly left and right also fooled the system.

User Acceptance

When used in a verification system for access control, facial recognition technology is typically considered by users to be less intrusive than fingerprint readers, iris scanners, and other biometric technologies. It can recognize people at a distance and does not require users to pause and interact with the equipment. However, some users are concerned that when used as a surveillance tool, facial recognition technology can facilitate tracking them without their consent. To address such concerns, specific policies for using facial recognition in a surveillance application have been suggested, including the following.

Transparency

As with any technology, public understanding of the operation and uses of electronic surveillance might mitigate fears that the government may be tracking people's whereabouts. Signs indicating the use of facial recognition in surveillance systems should be prominently displayed, and the government entity using facial recognition for surveillance should provide as much information as possible to the public about the technology's purposes and capabilities.

No Match, No Memory

Concerns have been raised about the possibility that facial recognition surveillance systems can identify law-abiding citizens, not only terrorists or violent criminals. A "no match, no memory" policy dictates that a person's image is saved only if a match is made to a record in a watch list database.

Data Retention

One issue that could arise is the government's handling of the data it collects. Even if a no match, no memory policy has been implemented, a retention policy should be followed that indicates the time period after which the data will be erased. Similarly, the data should be securely stored and maintained.

Oversight

Concern about how facial technology surveillance will be used is often related to fear that the technology's capabilities will be abused. Facial recognition systems must be used only for the purpose they were designed for, and some form of active oversight should be implemented. A cooperative effort between government officials and citizen oversight committees would provide accountability.

The Technology's Maturity

Operational Uses

The largest implementation of Identix's facial recognition technology is the Mexican Federal Electoral Institute's program to eliminate duplicate voter registrations. This system helps the Institute prevent citizens from voting more than once under different aliases. Facial recognition is used to compare people with matching names to determine whether the faces also match. The system's database, first used in Mexico's July 2000 presidential elections, contains about 60 million images.

The largest deployment of facial recognition for surveillance began in 1998 in Newham Borough, London, England, when Identix's facial recognition technology was introduced to 12 town center cameras to record activity and decrease street robbery in an unsafe neighborhood. With three hundred CCTV cameras, this system captures faces and compares them against a police database of about a hundred convicted street robbers known to have been active in the previous 12 weeks. When a face does not match, the image is deleted; when a match is found, an operator checks the result. In August 2001, 527,000 separate faces were detected and operators confirmed 90 matches against the database.

Public approval of Newham's system was judged by comparing the results of opinion polls over the course of the implementation. When Identix's facial recognition technology was first introduced, 50 percent of local citizens approved of the system. After about 2 years of operation, the technology was credited with a 34 percent reduction in street robbery, and the user approval rating rose to 90 percent. As the system has not led directly to any arrests, the effect of facial recognition technology appears to function largely as a deterrent to street crime in the monitored area.

In the United States, Viisage's facial recognition technology is deployed in 17 states to identify people with credentials or identification documents under more than one name. The majority of the states' databases consist of image templates from driver's license photographs. Illinois's driver's license database consists of about 10 million images and has the capacity for another 15 million images. The technology can perform a one-to-many match against this database in less than 15 seconds, and about 15,000 images are captured daily.

Facial recognition surveillance systems have been deployed in casinos worldwide, performing one-to-many matching against a database of casino offenders. Although the notable facial recognition implementations are in surveillance applications, facial recognition systems have been deployed in selected environments as a one-to-one verification solution for physical and logical access. Some casinos use facial recognition for employee time and attendance processing, while applications for automated teller machine fraud prevention and security have been implemented in grocery stores and gas stations.

Pilots: U.S. Airport Surveillance

Identix has been involved in four pilots that use facial recognition for surveillance at U.S. airports. The pilots had different operating scenarios to determine the relationship between the correct match rate—that is, the rate of actual matches—and the FNMR. Video cameras that were not hidden from travelers were set up near the airport metal detectors. The pilots were designed at some airports so that travelers were specifically instructed to stop and look at the cameras; travelers at other airports were not given such instructions.

From the four pilots, Identix concluded that lighting was the primary performance factor. It learned also that the correct match rate, and therefore the FMR, is quickly compromised as the threshold is adjusted to minimize the FNMR. The data are shown in table 24.

Table 24: Identix Airport Facial Biometric Pilot Results

Airport	Status	False match rate	False nonmatch rate	Notes
Boston Logan International, Mass.	Completed	Not reported	~10%	Viisage technology was also piloted.
Dallas/Fort Worth International, Texas	Completed	1.2%	6–15	Two cameras were used; when a match was made, the person's image was dispatched to a central control room for further investigation.
Fresno Yosemite International, Calif.	Ongoing	1–5	5–15	A liquid crystal display instructed each traveler when to pause in front of a fixed camera and when to resume walking.
Palm Beach International, Fla.	Completed	0.3	45	The objective was to obtain an FMR as close to 0 as possible.

Source: GAO analysis of Identix data.

Facial Recognition Vendor Test 2000

From May to June 2000, Naval Surface Warfare Center, Crane Division, evaluated an identification system in the Facial Recognition Vendor Test 2000 (FRVT 2000). The two test categories conducted during the

evaluation used the Face Recognition Technology (FERET) Database, which DOD's Counterdrug Technology Development Program Office sponsors. The evaluation report was issued on February 16, 2001.

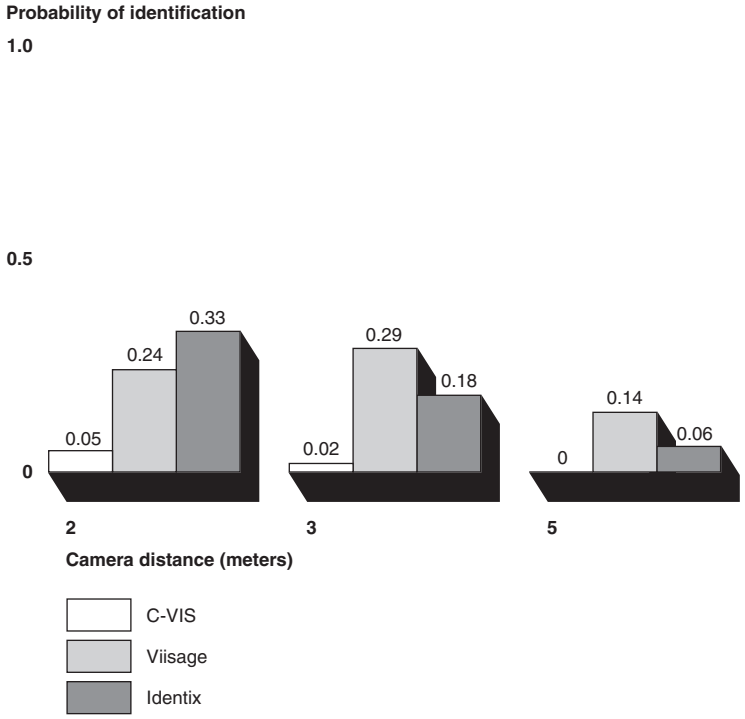
The first category, the recognition performance test, evaluated all algorithms on a standardized database collected by a universal sensor. Participating vendors were given 72 continuous hours in which to compare 13,872 images to one another, amounting to more than 192 million comparisons. Three vendors completed this portion: Identix, Viisage, and C-VIS Computer Vision and Automation GmbH. Banque Technology Systems International Ltd. (Banque-Tec) and Miros Inc. (E-True Technology), two other vendors, were able to compare only approximately 4,000 of the 13,872 images in the allotted time, and their results were not included.

Following this test, different environmental studies were conducted to show how the system responded to numerous variables such as distance, lighting, and facial expressions. We describe a sample of the results from a number of environmental studies, noting the overall lack of appreciable difference between the match accuracy of the Viisage and Identix algorithms. For the identification experiments, the charts we present show the probability that a vendor's top match correctly identified individuals. For the verification experiments, the results show the probability of correct verification while holding the FMR constant at 0.01. Each probe image was taken with a camera and matched by the vendor's system to the gallery images, which were drawn from FERET and other large databases.

Distance Experiments

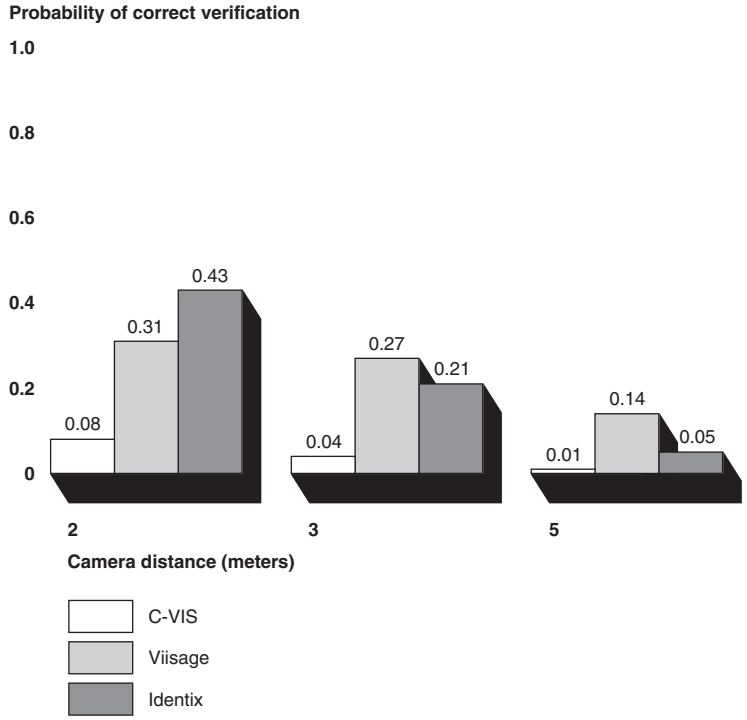
The distance experiments were designed to evaluate the performance of face-matching algorithms on images of subjects at different distances from the fixed camera. For the distance experiments, the probe images were taken at varying distances and compared, using the vendor's system, to gallery images that were taken at a distance of between 1.5 and 2 meters (see figures 40 and 41).

Figure 40: Facial Recognition Distance Identification



Source: GAO analysis of FRVT 2000 data.

Figure 41: Facial Recognition Distance Verification



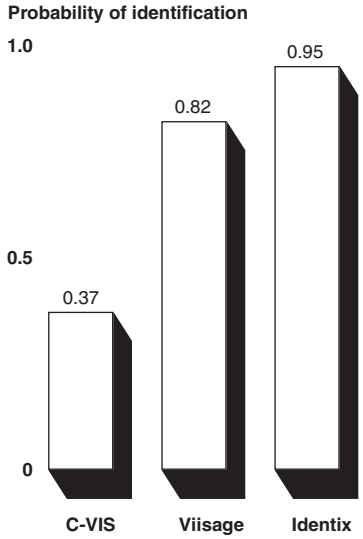
Source: GAO analysis of FRVT 2000 data.

Across all algorithms, the three sets of distance experiments indicated that performance decreases as the distance between the person and camera increases. At a distance of 5 meters, Viisage, the best vendor in this category, could correctly identify the image only about 13.7 percent of the time.

Expression Experiments

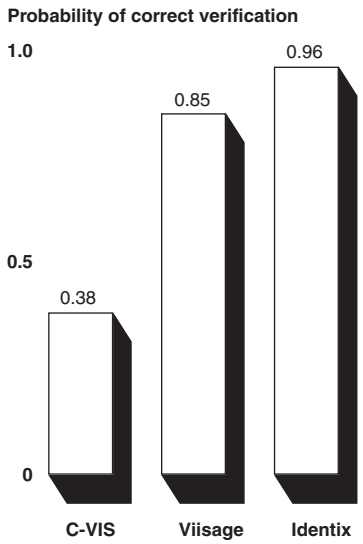
The expression tests evaluated how well identification and verification work when comparing images of the same person with different facial expressions. In this test, the gallery image was a face with a specific expression, and the probe image was the same face with an alternative expression. Identification proved more sensitive to change in expression than verification. Viisage and Identix correctly identified and verified more than 80 percent of the images (see figures 42 and 43).

Figure 42: Facial Recognition Expression Identification



Source: GAO analysis of FRVT 2000 data.

Figure 43: Facial Recognition Expression Verification

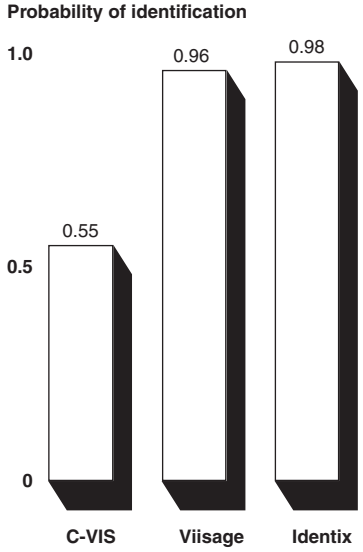


Source:GAO analysis of FRVT 2000 data.

Media Experiments

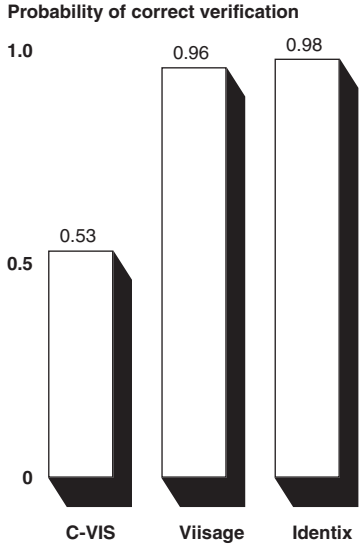
The media experiments were designed to evaluate the performance of face-matching algorithms when comparing images stored on different media. This application may be useful in comparing older mug shots to newer pictures taken with digital cameras. For Viisage and Identix, switching between 35 mm gallery images and digital probe images, and vice versa, did not significantly affect performance (see figures 44 and 45).

Figure 44: Facial Recognition Media Identification: Digital to 35 mm



Source: GAO analysis of FRVT 2000 data.

Figure 45: Facial Recognition Media Verification: Digital to 35 mm

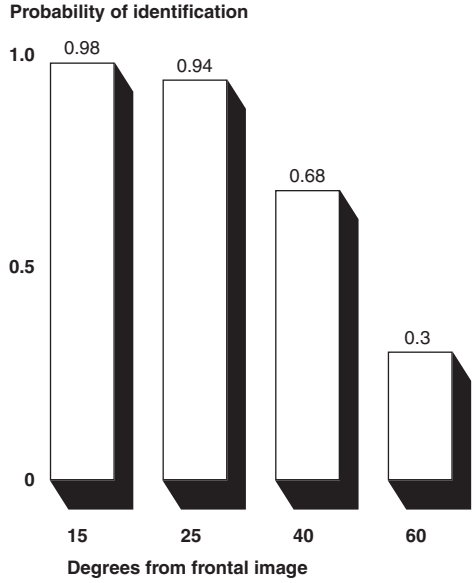


Source: GAO analysis of FRVT 2000 data.

Pose Experiments

The pose experiments measured the effect of different viewpoints on identification. They attempted to match a frontal gallery image with probe images that were rotated various degrees away from the front. The results reflected the best score of all vendors at each degree. As the degrees from the frontal image increased, the probability of identification fell rapidly. At 60 degrees away from the frontal image, identification was correct only 30 percent of the time (see figure 46).

Figure 46: Facial Recognition Pose Identification



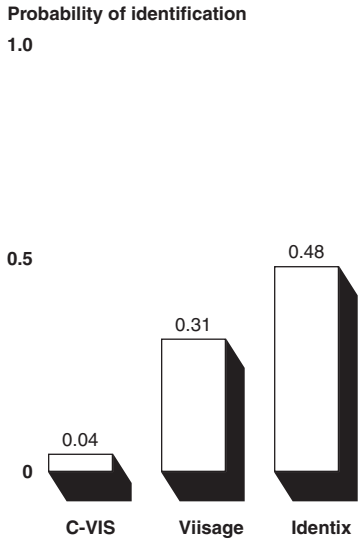
Note: These results reflect the best scores of all vendors at each degree.

Source: FRVT 2000.

Temporal Experiments

Temporal experiments addressed the effect of time delay between a first and subsequent capture of facial images. The test attempted to match each probe image with a gallery image of the same person taken approximately 1 year earlier. These experiments showed that a vendor's ability to correctly identify and verify images decreases significantly with time. After 1 year, Viisage and Identix identified 31 percent and 48 percent of faces, respectively. Viisage correctly verified 41 percent of images, Identix 56 percent (see figures 47 and 48).

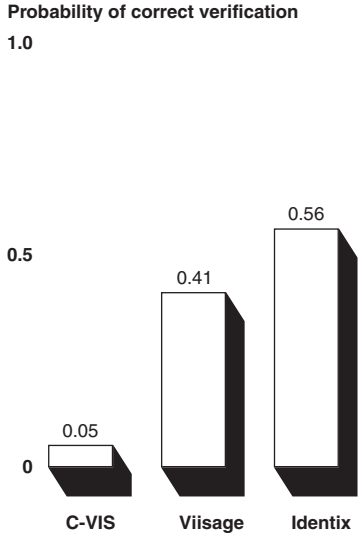
Figure 47: Facial Recognition Temporal Identification



Note: The time period measured was 1 year.

Source: GAO analysis of FRVT 2000 data.

Figure 48: Facial Recognition Temporal Verification



Note: The time period measured was 1 year.

Source: GAO analysis of FRVT 2000 data.

The second test category, product usability, evaluated the complete facial recognition system rather than just the facial recognition algorithm. An access control scenario with live subjects was chosen. Five vendors reported results, including the three vendors that completed the recognition performance test and the two that did not. When discussing the results, however, it is important to note that some systems tested were not intended for access control applications.

The two product usability tests were the enrollment timed test (ETT) and the old image database timed test (OIDTT). The tests had two main differences: (1) the subjects were stationary for the ETT and walked toward the camera in the OIDTT and (2) all vendors performed substantially better on the ETT, in which they enrolled the images under their own systems, than on the OIDTT, in which the images were provided to them before the test. Also, the facial recognition systems were quicker and more accurate in the verification experiments than in the identification experiments. See table 25 for the results.

Table 25: Facial Recognition Product Usability Test

	Old image database timed		Enrollment timed	
Vender	Percent verified	Percent identified	Percent verified	Percent identified
Banque-Tec	7%	0	22%	22%
C-VIS	0	0	69	83
Identix	64	31%	78	52
Miros (E-True)	36	0	78	71
Viisage	0	0	84	84

Note: Percentages are correct matches. Matching that took longer than 10 seconds counted as failure.

Source: GAO analysis of FRVT 2000 data.

Facial Recognition Vendor Test 2002

Facial Recognition Vendor Test 2002 (FRVT 2002), a follow-up to FRVT 2000, does not use the FERET database and is not a live facial recognition test.[2] Since the variables involved with a live capture do not allow for an equal test bed among all the participants, databases of photograph images will be used. Also, this test will include video data to determine whether multiple images of a person increase matching accuracy.

[2]Fifteen different agencies are sponsors of FRVT 2002, including the Defense Advanced Research Projects Agency, the National Institute of Justice, and the Transportation Security Administration. NIST is selecting images and computing test scores.

Twenty-seven organizations are participating in FRVT 2002, each testing for a minimum of 4 days and a maximum of 11 days with its own hardware and software (i.e., its own algorithms). The tests will perform a 100 kilobyte by 100 kilobyte comparison (comparing each face to every other face in the database) and return the results in the form of similarity matrixes. In preliminary tests of facial recognition, NIST has seen a 75 percent probability of verification with a 1 percent probability of false acceptance, compared with fingerprint recognition's 95 percent probability of verification and 1 percent probability of false acceptance.

Biometric Product Testing

NPL conducted a performance evaluation of seven biometric systems from May through December 2000, producing a final biometric product testing report on March 19, 2001. The facial recognition portion of the test used an Identix FaceIt Verification demonstration as well as alternative enrollment and matching algorithms.

The 0 percent FTER included persons unable to present the required biometric feature, those unable to produce an image of sufficient quality at enrollment, and those unable to reproduce their biometric feature consistently. At an FMR of about 1 percent, the facial recognition system with the alternate matching algorithm had an FNMR of approximately 3.3 percent. Additional experimental results were

- The facial recognition system collected a sequence of images over a 10-second period, saving the best match. This resulted in a mean transaction time of 15 seconds, a median of 14 seconds, and a minimum of 10 seconds.
- The matching algorithm could make 800 matches per minute with a Pentium processor, a Windows interface, and a Windows 2000 operating system. These diagnostic programs had significant overhead, so the matching algorithm may be significantly faster than the results showed, perhaps by a factor exceeding 100.
- Tests also found that males had a lower FNMR than females, and the FNMR for attempts made immediately following enrollment were significantly lower than those made at a volunteer's second or third visit.

U.S. Army Research Laboratory Test

For a personnel identification application, the Army Research Laboratory tested an identification system from July through October 2001, using Identix facial recognition technology. With 270 participants, approximately 42,000 face identification attempts were made. Despite the vendor's claims

of a 75 percent rate of correct identification, the testing showed that only 51 percent were correctly identified. Further, the correct identification was in the system's top 10 possible matches only 81 percent of the time, instead of the 99.3 percent that the vendor claimed. Inadequate lighting was a primary performance issue.

FAA Facial Recognition Test

In 2001, FAA and Safe Skies tested a facial recognition technology system for access control of airport employees. Following the test, the biometric system was removed. Twenty-eight people successfully enrolled in an average of 3 minutes and 2 seconds. The test included operational testing in a normal environment as well as testing under a controlled environment. The FNMR for the operational test was approximately 26 percent. Before device installation, the time required to pass through the door was approximately 2 seconds; after installation, 11.5 seconds. The FNMR for the controlled test was approximately 3 percent. Under normal test conditions, the rate of passage through the door was about six people per minute.

Test results for abnormal conditions were as follows:

- FNMR was nearly 100 percent when test subjects enrolled without sunglasses but passed through the device with sunglasses. The opposite—enrolling with sunglasses and presenting with sunglasses—also yielded an FNMR of nearly 100 percent.
- When test subjects enrolled without reading glasses but passed through the device with reading glasses, FNMR was nearly 60 percent; when they enrolled with and presented without reading glasses, FNMR was nearly 20 percent.
- FNMR increased notably for one test subject of three with a 5-day beard growth. No effect was noted for the two other subjects. The effect was little or none for enrolling with 5-day beard growth and then attempting access while clean-shaven.
- A horizontal ¾-inch adhesive bandage on the chin produced an overall FNMR of 40 percent, but the results were highly dependent on the test subject—three had a rate of 0 percent and two had a rate of 100 percent. A round bandage on the cheek produced an overall FNMR of 6 percent.
- No effect was noted from high backlighting directly; however, one test subject with glasses was falsely rejected 10 of 10 times. Further

investigation showed a reflection on the glasses from the backlighting from the door window.

State Department Consular Affairs Tests

The Department of State Bureau of Consular Affairs evaluated facial recognition technology for identifying ineligible visa applicants. Viisage and Identix provided facial recognition software. The final evaluation report was issued on January 30, 2001.

Laboratory testing involving data sets of 10,000 to 100,000 images revealed that less than 30 percent of intentionally seeded duplicate images were correctly matched. This translates into an FNMR of around 70 percent. The processing speed for facial recognition enrollment was more than adequate. Images were aligned and enrolled at a rate of approximately two per second for both tested products. Processing speed for search ranged from excellent for one vendor's product to marginal for the other vendor's product. In the latter case, an improved version of the software, submitted after formal testing was completed, was faster by a factor of two in performing searches of large data sets. The search speed might limit its usefulness in processing a large data set but is acceptable for daily operations.

The National Visa Center tested the technology with the diversity visa program in the field. This trial showed that a facial recognition system can be successful in identifying matches involving duplicate applications. More than 500 matches were found while examining more than 5,000 of 35,000 possible duplicate images. Of these 500 and more, 146 represented cases that had not been discovered by other means. This success was obtained despite the obviously poor quality of the pictures submitted, the poor capture characteristics of the Quickcam cameras used, and the less than optimal scanning technique the data entry personnel used. It was observed that Identix's product was more forgiving of the image quality problems and generally reported more matches.

Despite the vendors' cooperative, responsive, and interactive approach in supplying testable products and engineering support, the facial recognition software packages, even in their "final" versions, following numerous developmental versions, exhibited significantly troublesome behavior—such as corrupt databases, poorly implemented capabilities, and the need for workaround solutions—that impeded testing.

Border Control Applications Piloted and Deployed

INS SENTRI

INS conducted a facial verification test for the Secure Electronic Network for Travelers Rapid Inspection (SENTRI) from November 1997 through July 1998 at California's Otay Mesa port of entry. The facial verification test involved taking video images of drivers at an inspection booth. The video clips were compared to the SENTRI enrollment database of photographs for all drivers in the SENTRI lane. An Identix system was used for the tests.

The experiment found that pictures taken in a full frontal enrollment pose showed a significantly higher recognition rate than pictures taken when the head was rotated slightly. It also found a principal identification problem when the image was obtained during validation. Obscured faces that were hidden by part of the vehicle and those with excessive glare or extreme shadows were essentially unusable. In testing, the proportion of video clips exhibiting these properties was initially very high. Adding cameras increased the chance of getting an unobstructed video clip. A new camera system using fuzzy logic helped reduce glare and shadows.

With these changes, the system was able to get usable images for approximately 90 percent of the vehicles in a lane. With such images, the system had an FNMR of 1.6 percent and a low EER of 2.1 percent. The report concluded that the facial verification system performed admirably in a challenging environment.

State Department Posts

The State Department is conducting pilots using facial recognition technology from Identix and Viisage to compare images from 23 of its posts. The facial recognition software is used primarily to compare digital pictures in one-to-many matching to identify people who apply more than once for nonimmigrant visas or diversity visas.[3] A secondary one-to-many matching of photographs from both previously issued visas and new visa

[3]The annual Diversity Visa Lottery Program makes 50,000 immigrant visas available through a lottery to people who wish to come to the United States from countries with low immigration rates. Winners are chosen randomly from all qualified entries by the State Department's National Visa Center.

applications is performed against a watch list database. The photographs from all visa applications are scanned into the system, regardless of whether visas are issued or applications are rejected. All scanned images (not just the templates) are retained in case future versions of the facial recognition software use a different template format.

The primary performance factor for the State Department pilots has been the quality of the photographs submitted with applications. The better the quality of the photographs is, the more likely it is that match results will be good. It was found that many of the images in the databases are poor in quality—either too dark or too light for facial recognition, poorly focused, or distorted in some other way. Consequently, the State Department is working to develop standards for photograph quality. Age was found to be a performance factor. For example, both Identix and Viisage have found it difficult to match children because their faces change rapidly. However, State Department officials have not noticed any appreciable differentiation in the quality between the Identix and Viisage match algorithms.

Of approximately 197,000 images (applicants' photographs) for diversity visas processed in the 2002 program year, 75 percent were successfully enrolled in the diversity visa facial recognition database. The images from the 74,348 successful applications were matched against the enrollment database. About 6,000 candidate matches were made; 85 percent were determined to be actual matches. The facial recognition technology identified 60 individuals who submitted multiple applications that were not detected by the manual process.

In October 2001, 23 posts processed approximately 26,000 nonimmigrant visa images, of which 78 percent were successfully enrolled in the nonimmigrant visa facial recognition database. For all 23 posts, around 4,000 candidate matches were made. The percentage of actual matches varied by post, as one post's matching had an FMR of 1 percent, and another post's matching resulted in an FMR of 65 percent.

Iceland

One of the first major installations of facial recognition technology at an airport was at Iceland's Keflavik International Airport in June 2001. As a result of Iceland's participation in Europe's Schengen agreement, border controls between that country and others participating in the agreement

have been eliminated.[4] The facial recognition system was implemented to identify known criminals and false asylum seekers while maintaining a level of convenience for citizen travelers.

Israel

The Basel Project is a pending implementation of facial recognition and hand geometry for day workers entering and exiting Israel by way of the Gaza Strip. Fingerprint technology was rejected, since the primary users are laborers whose fingerprints are unreliable as a biometric for matching.

Individuals enrolling at the Israeli-Palestinian land border will receive a contactless smart card with a high-resolution picture and a hand geometry biometric. As they enter and leave Israel, they will be processed through 42 routing passages to unattended checkpoints at verification terminals inside a building. An estimated 60,000 verifications will be processed daily, performing a one-to-one match against a stored template in a central server, with a backup stored on the smart card.

Australia

Australia's Sydney Airport is conducting a facial recognition pilot to determine cost effectiveness and efficiency in an operational environment. The technology is being used for both verification and identification. One-to-one verification is performed to identify false passports as travelers present their passports, and one-to-many identification is used to identify terrorists among the crowds.

Dominican Republic

The Dominican Republic is implementing Identix's facial recognition technology for scanning passports at 120 entry points. The system will capture a face biometric, which will be used in a search against a central criminal watch list database. If another biometric is needed in the future, the passport reader will also be capable of reading a fingerprint.

Processing Issues

Processing speed for facial recognition enrollment is approximately two images per second. The raw search speed is one million searches per second on a single computer, but other factors are involved, such as the

[4]The Schengen agreement, begun in 1985, is designed to facilitate travel within the European Union. Passengers flying between member countries now leave from domestic rather than international airport terminals, eliminating the need to present travel documents when entering and exiting. The Schengen agreement went into effect in Iceland on March 25, 2001.

size of the database. For an identification application, search speed can be dramatically improved by storing some templates on a disc during alignment for use during later searches. A facial recognition system can be designed to achieve a desired response time by increasing the number of processors, but the trade-off to increased speed is greater cost.

Because facial recognition biometrics can be used in various applications, different requirements affect performance time differently. The requirements for performing a background check and a duplicate face check at enrollment would differ from those for performing verifications at borders. Verifications at a border would be practically instantaneous if performing a one-to-one match against a template stored on a travel document or a smart card, but an additional one-to-many watch list search would add time, depending on the size of the database. Facial recognition results in a faster response time than fingerprint recognition in a one-to-many search. The implication of a heavily queried database is that a priority level must be assigned to determine when the various transactions are to be handled.

Device Durability and Environmental Constraints

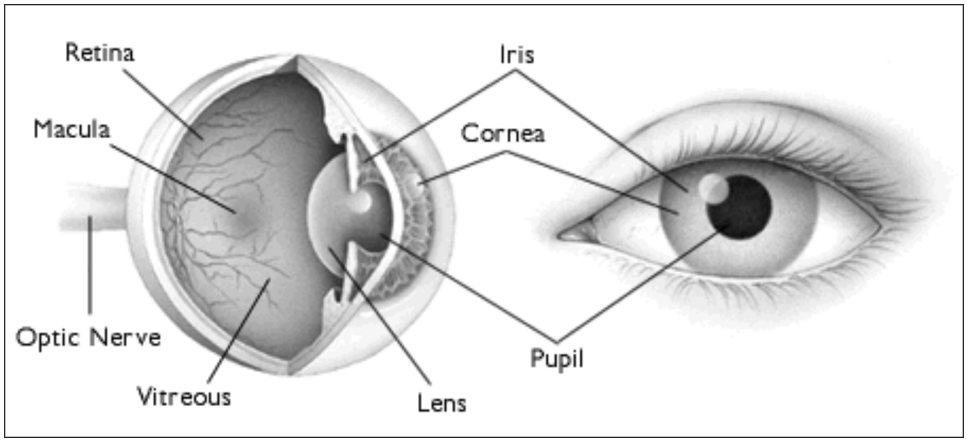
In surveillance applications, travelers would not interact physically with the cameras and computers that run the facial recognition technology. The durability of this equipment would depend on the manufacturer's specifications.

Because lighting is such a major performance factor, the use of awnings or shades with outdoor installations of facial recognition technology could be required to block direct light. Without awnings or shade, glare or shadows might present a problem that could be compounded by reflections from nearby buildings or vehicles.

Appendix V: Iris Recognition Technology

Iris recognition technology was developed in 1992 and is therefore one of the newest of the commercially available biometric technologies. It is based on the distinct, visible characteristics of the eye's iris, the colored ring that surrounds the pupil (see figure 49). Built from elastic connective tissue, the iris is a very rich source of biometric data. The characteristics of the iris are formed during the eighth month of gestation and do not change except through actions such as refractive surgery, cataract surgery, and cornea transplants. Iris recognition can even be used to verify the identity of blind people as long as one of their sightless eyes has an iris.

Figure 49: The Iris and Other Parts of the Eye



Source: Copyright, the American Academy of Ophthalmology.

The iris has more numerous and dense forms of variability than other biometrics. Whereas traditional biometrics have only 13 to 60 distinct characteristics, the iris can be said to have 266 unique spots, and iris recognition technology uses some 173 of these features. The primary visible characteristic of the iris is the trabecular meshwork, tissue that gives the appearance of dividing the iris radially. Other features include striations, rings, furrows, a corona, and freckles.

Besides the iris' many distinctive characteristics, its patterns also differ substantially from person to person. A person's left and right eyes have different iris patterns, and the irises of identical twins have almost no statistical similarity. It has been postulated that the probability of two persons having the same iris pattern is 1 in 7 billion.

How the Technology Works

An iris recognition system uses a small high-quality camera to capture a black-and-white, high-resolution picture of the iris. The technology relies on infrared imaging, using wavelengths from 700 to 900 nanometers, a range the American Academy of Ophthalmology has stated is safe.

How close the person should be to the camera and her level of participation depend on the type of system. Physical access control applications require a person to stand within 3 to 10 inches of the camera and center the iris in a mirror within an area 1 inch square directly in front of the camera (see figure 50). The system may prompt the person to move slightly forward or backward to allow a proper image capture. Systems using desktop cameras to control logical access to computers and networks require a distance of about 18 inches to capture the iris image (see figure 51). Users must center their eyes on the camera with a guidance light or hologram. Personal identification systems, such as those at airport kiosks in trusted traveler applications, allow users to stand as far away as 3 feet. However, users must remain still as the camera locates the eye and captures the image.

Figure 50: Iris Recognition Physical Access Control System



Source: Panasonic Digital Communications & Security Co.

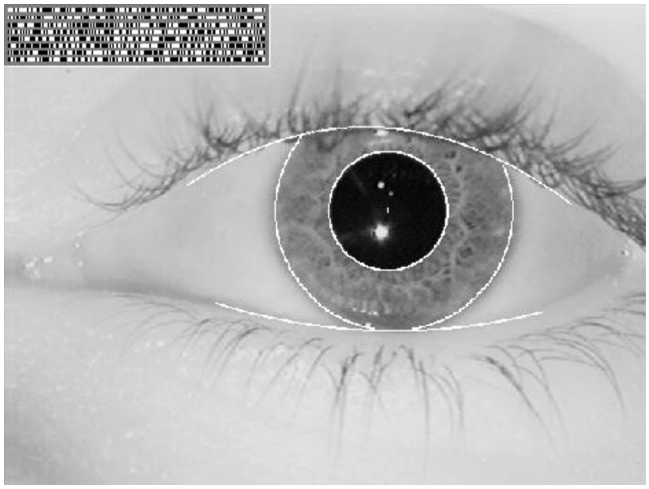
Figure 51: Iris Recognition System with Desktop Camera



Source: Panasonic Digital Communications & Security Co.

An iris recognition system first defines the boundaries of the iris, establishes a coordinate system over the iris, and defines the zones for analysis within the coordinate system. Feature extraction algorithms map the segments of the iris into hundreds of independent vectors that define the orientation and spatial frequency of the distinctive features, along with the position of the features. However, the entire iris is not used: A portion of the top as well as 45 degrees of the bottom remain unused, to account for pupil dilation, occlusion from eyelids, and reflection from the camera (see figure 52).

Figure 52: Mapping the Eye for Iris Recognition Systems



Source: Dr. John Daugman, Cambridge University, Cambridge, U.K.

Algorithms also check for the presence of a pattern on the sphere of the eye instead of on an internal plane and use measurements at different wavelengths to determine that the eye is living. The visible characteristics within the zones are then converted into a 512 byte template that is used to identify or verify the identity of an individual; 256 of these bytes contain control information.

The Leading Vendors

Iridian Technologies Inc. is the sole owner and developer of iris recognition technology. Iridian markets applications through hardware manufacturers and systems integrators, including Argus Solutions, EyeTicket Corp., IBM, Joh. Enschede Security Solutions, LG Electronics, NEC Singapore, Oki Electric Industry Co., Panasonic, SAFLINK Corp., Siemens AG, Titan Corp., and Unisys.

The Cost of Devices

Iris recognition systems cost approximately $2,000 for physical access units. The camera itself costs $200.

Performance Issues

Some users are unable to provide adequate enrollment images because they find the iris image capture process too difficult. Poor eyesight may also hinder the ability of some people to line up their eyes with the camera. Colored and bifocal contact lenses can affect system performance, and so can exceptionally strong glasses. People with

glaucoma may not be reliably identified. Also, glare and reflections, along with user settling and distraction, can cause interference.

User Acceptance

Some people resist technologies that scan the eye, but unlike biometric identification and verification technologies such as fingerprint recognition or hand geometry, iris recognition technology requires no body contact. Iris recognition technology is more user friendly than retina recognition systems in that no light source is shone into the eye and close proximity to the scanner is not required. However, iris recognition does use active infrared illumination in the 700 to 900 nanometer wavelength range. It has none of the inherent risks associated with lasers. Some people assume that the imaging of their irises will reveal their medical data, such as heart disease, diabetes, and high blood pressure, but images of the iris acquired for iris recognition reveal no information about a person's health.

The Technology's Maturity

Operational Uses

Iris recognition is being used operationally for physical access control, logical access control, and personal identification applications. An EyeTicket access control system was installed at Douglas International Airport in Charlotte, North Carolina, in July 2000 to control airline and airport employee access to restricted areas. The company has also installed the access control system at Germany's Frankfurt Airport. Iridian has installed IrisAccess™ at Baltimore Technologies' data hosting center in Sydney, Australia. Access to the highly secure facility requires that anyone requesting entry verify her identity with both a proximity card and the iris recognition technology.

The Office of Legislative Counsel for the U.S. House of Representatives has recently installed an iris recognition system to protect confidential computer files and working documents. Iris recognition systems have been deployed in several prison systems in the United States to prevent inmates from swapping identities with visitors as well as to verify the identity of prisoners before they are released.

Tests

Biometric Product Testing

NPL conducted a performance evaluation of seven biometric systems from May through December 2000. The iris portion used Iridian's IriScan System 2200. The FTER was 0.5 percent. The FMR was 0 percent and the iris recognition system had an FNMR of 1.9 percent. Additional experimental results were that

- the iris system had a mean transaction time of 12 seconds, a median of 10 seconds, and a minimum of 4 seconds;
- the matching algorithm could make 1.5 million matches per minute when using a SunUltra5 with a SunOS 5.8 operating system, 270 MHz processor, and 128 Mb of memory; and
- people without glasses had a lower FNMR than those with glasses.

U.S. Army Research Laboratory

The U.S. Army Research Laboratory recently tested an Iridian verification system. There were 186,918 eye identification attempts on 93,459 registrations. The FMR was well below 1 percent. Despite the vendor's claims of greater than 99.5 percent correct identification, the testing showed a 6 percent FNMR; glare and reflections appeared to be primary culprits in this discrepancy. User settling and distraction also contributed to the problem.

Sandia National Laboratories

In April 1996, Sandia National Laboratories evaluated a prototype biometric recognition system provided by IriScan. Average enrollment time was 2 minutes and 15 seconds. During the first phase of the test, there was a raw FNMR of 11.8 percent. After removing the errors that could be attributed to extreme environmental conditions or deliberate misuse, the FNMR became 10.2 percent. The average transaction time of a sampling of transactions was 14 seconds. The minimum transaction time recorded was 6 seconds, the maximum 23 seconds. Users attempted 96 false match transactions with no actual false matches. Overall, the researchers concluded that the system performed extremely well in difficult conditions.

c't Magazine

Researchers at *c't Magazine* in Germany set out to see whether they could fool Panasonic's Authenticam BM-ET100, a desktop iris recognition system. The investigators' first attempts to spoof the system by using iris images projected on monitors failed because of the too intense reflection of light. However, they succeeded in beating the system by holding up to

the camera a high-resolution picture of an iris with a tiny hole cut out to allow the pupil of a live eye shine through. They also found it possible to enroll with the aid of this artificial eye. From that point on, anyone in possession of the eye pattern was able to log on to the system. Moreover, the system also matched the iris of the person whose picture had been used to create the artificial eye with the enrolled reference template.

Border Control Applications Piloted and Deployed

United Kingdom

Iris recognition has been used in some border control environments. For example, beginning in July 2001, frequent travelers on transatlantic Virgin Atlantic Airways and British Airways flights have been able to bypass passport control at London's Heathrow Airport, without waiting in line for an immigration agent. In trial runs, 2,000 American and Canadian passengers have undergone identity checks by British immigration officers before being enrolled. Once registered and enrolled, they can proceed, as arriving passengers, directly to specific lanes to verify their identity against a biometric template stored in a central database (see figures 53 and 54). If the verification is successful, they are issued a ticket admitting them directly to the United Kingdom. The trial is being operated by the airlines and involves no changes to passports.

Figure 53: Iris Recognition Device for Border Control at London's Heathrow Airport



Source: EyeTicket Corporation.

Figure 54: Border Control Lane with Iris Recognition Device at London's Heathrow Airport



Source: EyeTicket Corporation.

Canada

The Canada Customs and Revenue Agency has initiated the Expedited Passenger Processing System, which will include iris recognition technology. The system will allow frequent travelers to expedite inspection. It is planned to be operational at Lester B. Pearson International Airport in Toronto and Vancouver International Airport at the beginning of 2003. An enrollment of about 200,000 spread out over 5 years is expected. The plan is to use a central database for storing the iris templates. Initially, it was not clear whether computer performance would allow for a central database, so provision was made for a token to store the biometric. However, testing has shown that doing the checks centrally does not significantly affect performance time. Either one-to-one matches (with an identifying token) will be made or one-to-many, with the system identifying applicants by the iris match.

Netherlands

In October 2001, an iris recognition system was installed at Amsterdam's Schiphol Airport. The system expedites the way for travelers from 18 European countries into the Netherlands and includes about 2,000 frequent travelers. Users must go through a two-phase process. First, passengers undergo a background check, a passport review, and an iris scan. The template is encrypted and embedded on a smart card. This phase takes about 15 minutes. The second phase identifies and verifies each registered traveler at the immigration checkpoint. The traveler's reference template is compared with a real-time scan of the iris. This process typically takes about 10 to 15 seconds and allows the passenger to bypass long immigration lines. The Schiphol program charges each enrolled traveler a yearly fee of $89 to use the system. The FNMR is less than 1 percent; the FMR is less than 0.001 percent.

Singapore

Iris recognition is used to admit workers who travel into Singapore from Malaysia each day by motorcycle. The workers' irises are scanned by a camera installed in kiosks in designated lanes, instead of their having to present their paperwork to an official. About 50,000 workers cross the border each day.

Saudi Arabia

In February 2002, at the King Abdul Aziz Airport in Jeddah, Saudi Arabia, iris recognition tracked and identified visitors who were on pilgrimage for the Hajj season of worship. The process included a random check at passport control, enrollment into a database, and subsequent identification on departure. The systems were in place to ensure that visitors did not overstay their visas and also to identify potential security threats. It is estimated that images of 20,000 to 30,000 irises were collected.

Processing Issues

Although iris recognition systems can perform both one-to-many identification and one-to-one verification, they are deployed primarily for identification. In some processors, iris recognition technology can search hundreds of thousands of records per second. Very few biometrics have the capability of iris recognition for a high-speed exhaustive search of a database.

Device Durability and Environmental Constraints

Because iris recognition systems use infrared illumination, they can be used in the dark. Their durability depends greatly on the specifications of the system's individual components.

Appendix VI: Cost Estimates for Using Biometrics for Border Security

For each of the four scenarios, we created cost models to estimate the cost of developing, implementing, and maintaining various biometric systems. Besides including the cost of purchasing the biometric hardware, we estimated costs for additional hardware, software, maintenance, personnel, training, and effects on other procedures in order to derive life-cycle cost estimates. We followed the cost element structure that DOD uses at acquisition program milestone and decision reviews to assess major automated information systems costs. Tailoring this structure to reflect our four scenarios, we used it to standardize costs so that they could be compared at a high level. We present the costs in two parts. Initial costs represent the costs required to plan, design, develop, and field the system. Recurring costs represent the annual costs required to operate and continually maintain the system to keep it in operation.

Initial Cost Elements

We estimated seven sets of initial cost elements: costs for systems engineering and program management; development, installation, and training; biometric hardware; biometric software; network infrastructure; renovating consular facilities; and hardware infrastructure upgrades.

Systems engineering and program management costs included both program management activities and government in-house engineering efforts to design, develop, and test the biometric system. For the watch list scenarios, we used an engineering build-up of personnel and their respective costs. For issuing visas and passports with biometrics, we used an overall factor of the total initial cost to estimate this effort.

Development, installation, and training costs included all resources required to design, develop, test, and implement a biometric system. For the watch list scenarios, we used an analogy to the Consular Lookout and Support System (CLASS) to estimate the cost of developing and implementing a watch list database. For issuing visas and passports with biometrics, we used an analogy to IAFIS and applied an engineering scaling factor to account for additional biometric storage space.

Biometric hardware costs included costs for biometric scanners, token card readers, and token cards for storing biometric data as well as costs for the personal computers to make these devices function properly. To estimate costs, we used average vendor costs where available and, in other cases, we relied on expert opinion.

Biometric software costs included the licensing cost for biometric scanners, card readers, and database software. For the watch list

scenarios, we used cost estimates provided by the State Department, based on analogy to CLASS. For issuing visas and passports with biometrics, we assumed this cost was already included in the development cost for IAFIS.

Network infrastructure included costs associated with purchasing and installing the local area networks needed to establish the connectivity required by the biometric systems. For the watch list scenarios, we used cost estimates provided by the State Department, based on an analogy to CLASS. For issuing visas and passports with biometrics, we used an analogy to a trusted traveler cost estimate developed by IBG.

To issue visas with biometrics, additional space at the consulates and embassies will be required to accommodate the new process of capturing applicants' biometrics. For the watch list scenarios, the consular facility cost is for the renovation of primary and contingency space for the new computer systems. We used square foot data provided by the State Department to estimate this cost. We did not include costs for the collection of biometrics at passport acceptance offices because most of these are not State Department facilities, and we had no basis on which to estimate the appropriate amount of space for these offices.

Hardware infrastructure upgrades included the cost to refresh hardware every 3 years. To estimate this element, we calculated the cost to replace one-third of the hardware annually, an accepted industry standard and the practice for the State Department's visa and passport sites.

Recurring Cost Elements

We estimated 10 sets of recurring cost elements: program management, biometric hardware maintenance, software and system maintenance, network infrastructure maintenance, consular operating personnel, port of entry operating personnel, communications, training, consular facility maintenance, and annual supplies.

Program management included the cost of providing continuing program management over the system's useful life. To estimate this cost for the watch list scenarios, we used an engineering build-up of personnel and their respective costs. For issuing visas and passports with biometrics, we estimated this cost to be 20 percent of the initial systems engineering and program management cost.

Biometric hardware maintenance included the cost of providing maintenance and repair for the biometric and system hardware. We used

an average factor of 12.5 percent, based on a 10 percent to 15 percent range IBG provided in its trusted traveler cost estimate.

Software and system maintenance costs included annual software licensing for databases plus costs for personnel to upgrade and maintain them. For the watch list scenarios, we used an engineering build-up of personnel and their respective costs. For issuing visas and passports with biometrics, we used an analogy to IAFIS annual system costs, applying the engineering scaling factor to account for additional database storage of the various biometrics.

Network infrastructure maintenance included the cost of providing hardware and software maintenance for the network. For the watch list scenarios, we used data from the State Department, based on its experience from CLASS. For issuing visas and passports with biometrics, we used the same factor of 12.5 percent that was used for estimating hardware maintenance.

The costs for consular operating personnel are for visa operating personnel at embassies and consulates around the world or for passport operating personnel at passport acceptance offices. For the checking of a biometric watch list before issuing visa, we estimated that one additional staff member per embassy or consulate would be required to resolve watch list hits. We did not include additional staff for checking a biometric watch list before issuing a passport. For the issuance of visas with biometrics, we first estimated the number of personnel needed at the consulates, using time to capture the biometrics as a variable. We then estimated the cost for the foreign service nationals who would perform the capturing, the foreign service officers who would oversee them, and auxiliary consulate staff to assist during peak load times. The annual costs for all visa operating personnel and the one-time moving costs for new foreign service nationals and officers were provided to us by the State Department. For the issuance of passports with biometrics, we assumed one staff member per passport acceptance office to troubleshoot problems with the biometric equipment.

Port of entry operating personnel include staff to troubleshoot biometrics at ports of entry. To estimate costs for these personnel, we made the assumption that there would be three staff per port of entry who would be trained and able to troubleshoot problems arising from biometric capturing or the inability to match biometric data.

The costs of communications included the cost of maintaining a wide area network able to provide secure electronic connectivity from the consular and port of entry sites to a headquarters location for comparing biometrics. To estimate this element, we used an analogy to IAFIS communication costs with a cost-per-location methodology.

Training included the costs to train personnel in using biometrics, including the cost of travel. We used an average of $5,000 per staff annually to estimate this cost.

The cost of maintaining consular facilities included maintaining newly acquired space. We used data on cost per square foot provided by the State Department.

In estimating the cost of annual supplies, we included the cost to purchase biometric token cards for the storage of biometrics collected for issuing passports and visas. This cost also includes the amortized cost of the infrastructure required to produce the cards, including elements such as centralized certificate issuance servers, key management components, and the card management infrastructure. We used data provided by the State Department for the Mexican border crossing card.

Assumptions

We prepared the life-cycle cost estimates using fiscal year 2002 constant dollars—that is, inflation was not considered for the multiple years over which funds would be required for acquisition—and they represent rough order of magnitude costs. Following are the assumptions that frame the boundary of our cost estimates.

- Scenario life-cycle cost estimates represent development and installation time plus 10 years' operational life.
- Phasing of costs over time is simplified, and actual schedules to both develop and install equipment and infrastructure will most likely differ.
- Biometric technologies—fingerprint, facial, and iris recognition—represent standardization to a single vendor's protocols. Biometric technology costs represent the average costs of vendors' products. Four flat fingerprints will be collected for fingerprint recognition.
- There are 210 visa-issuing embassies and consulates worldwide. There are 4,500 passport acceptance offices. There are 3,950 primary and secondary inspection stations at 400 ports of entry.

- Personnel costs reflect both direct costs and indirect costs. Three personnel will be needed to troubleshoot equipment at ports of entry, or 1,200 additional staff.

No costs were estimated for

- additional inspectors at ports of entry,
- additional facility space for passport acceptance offices or at ports of entry for primary and secondary inspections,
- biometric equipment for exiting the United States, and
- biometric security technology (e.g., encryption of biometric data).

Estimated Costs for Conducting Watch List Checks with Biometrics

We used the following assumptions to create the cost estimates for the two biometric watch list scenarios:

- The watch list database will include 10 million records.
- Matches will be performed using facial recognition technology.
- To conduct watch list checks before issuing travel documents, facial images will be generated by capturing the physical photographs applicants present when they apply for a visa or passport.
- The images will be collected and scanned at consulates and embassies for visas and at passport acceptance offices and transmitted through telecommunications resources to a central facility in metropolitan Washington, D.C.

The estimated costs for conducting biometric watch list checks before travelers are issued travel documents and before they enter the country are shown in table 26.

Table 26: Estimated Costs for Watch List Checks before Issuing Travel Documents and before Entering the United States

	Watch list check before issuing travel documents		Watch list check before entering the United States[a]	
Cost element	**Initial cost**	**Annual recurring cost**	**Initial cost**	**Annual recurring cost**
Investment				
Systems engineering and program management	$540		$540	
Development; installation; training	7,900		207,900	
Initial biometric hardware	6,045		16,488	
Initial biometric software	4,600		4,600	
Network infrastructure	100		100,000	
Consular facility renovation	570		570	
Hardware infrastructure upgrade		$2,523		$38,969
Operations and support				
Program management		540		540
Biometric hardware maintenance		926		14,761
Software and system maintenance		6,400		38,560
Network infrastructure maintenance		100		12,513
Visa operating personnel	33,075	50,715		
Port of entry operating personnel				94,679
Communications		10,540		10,038
Recurring training		1,000		26,750
Consular facility maintenance		152		152
Total	**$52,830**	**$72,896**	**$330,197**	**$236,960**

Note: In thousands of fiscal year 2002 constant dollars.

[a]Numbers do not sum because of rounding.

Source: GAO analysis.

Estimated Costs for Issuing Visas with Biometrics

We developed cost estimates for six different combinations of biometric technologies under two different possibilities for issuing visas. The State Department receives about 10.3 million visa applications each year. In fiscal year 2000, INS estimated that approximately 14 million individuals traveled under the visa waiver program. If these travelers must obtain a visa to travel to the United States, we assume that this same number would also be required to have their biometric sample collected. We used the following assumptions to estimate the costs of adding biometrics to visas:

- The number of visa applicants will remain constant at 10.3 million annually. The number of travelers in the visa waiver program will remain constant at 14 million annually.

- Enrolling travelers using a single biometric (whether for fingerprint, facial, or iris recognition) is estimated at 6 minutes (10 applicants enrolled per hour).

- Enrolling travelers using multiple biometrics (for example, fingerprint and facial combined, fingerprint and iris combined, or fingerprint, facial, and iris combined) is estimated at 10 minutes (6 applicants enrolled per hour).

- All current visa-issuing embassies and consulates will be equipped to collect biometrics from visa applicants.

Costs were not included for additional inspectors or facility space at ports of entry. Tables 27–32 show the cost of issuing visas with biometrics using fingerprint recognition, iris recognition, facial recognition, fingerprint and iris recognition, fingerprint and facial recognition, and fingerprint, iris, and facial recognition.

Table 27: Estimated Costs for Issuing Visas with Biometrics Using Fingerprint Recognition

	Annual visa applicants			
	10.3 million with visa waiver program		24.3 million without visa waiver program	
Cost element	Initial cost	Annual recurring cost	Initial cost	Annual recurring cost
Investment costs				
Systems engineering and program management	$111,147		$145,645	
Development; installation; training	527,655		558,936	
Initial biometric hardware	219,033		443,241	
Initial biometric software				
Network infrastructure	152,500		152,500	
Consular facility renovation	335,781		463,606	
Hardware infrastructure upgrade		$79,114		$93,986
Operations and support				
Program management		22,229		29,129
Biometric hardware maintenance		10,905		16,538
Software and system maintenance		73,123		125,292
Network infrastructure maintenance		19,063		19,063
Visa operating personnel	75,926	111,626	114,903	150,603
Port of entry operating personnel		94,679		94,679
Communications		20,577		20,577
Recurring training		32,472		38,040
Consular facility maintenance		89,541		123,628
Annual supplies (cards)		154,809		365,229
Total	**$1,422,042**	**$708,138**	**$1,878,832**	**$1,076,765**

Note: In thousands of fiscal year 2002 constant dollars. Numbers do not sum because of rounding.

Source: GAO analysis.

Table 28: Estimated Costs for Issuing Visas with Biometrics Using Iris Recognition

	Annual visa applicants			
	10.3 million with visa waiver program		24.3 million without visa waiver program	
Cost element	Initial cost	Annual recurring cost	Initial cost	Annual recurring cost
Investment				
Systems engineering and program management	$110,925		$145,375	
Development; installation; training	527,655		558,936	
Initial biometric hardware	216,563		440,240	
Initial biometric software				
Network infrastructure	152,500		152,500	
Consular facility renovation	335,781		463,606	
Hardware infrastructure upgrade		$78,298		$92,996
Operations and support				
Program management		22,185		29,075
Biometric hardware maintenance		10,596		16,163
Software and system maintenance		73,123		125,292
Network infrastructure maintenance		19,063		19,063
Visa operating personnel	75,926	111,626	114,903	150,603
Port of entry operating personnel		94,679		94,679
Communications		20,577		20,577
Recurring training		32,472		38,040
Consular facility maintenance		89,541		123,628
Annual supplies (cards)		154,809		365,229
Total	**$1,419,349**	**$706,970**	**$1,875,562**	**$1,075,346**

Note: In thousands of fiscal year 2002 constant dollars. Numbers do not sum because of rounding.

Source: GAO analysis.

Table 29: Estimated Costs for Issuing Visas with Biometrics Using Facial Recognition

	Annual visa applicants			
	10.3 million with visa waiver program		24.3 million without visa waiver program	
Cost element	Initial cost	Annual recurring cost	Initial cost	Annual recurring cost
Investment				
Systems engineering and program management	$109,258		$143,350	
Development; installation; training	527,655		558,936	
Initial biometric hardware	198,037		417,737	
Initial biometric software				
Network infrastructure	152,500		152,500	
Consular facility renovation	335,781		463,606	
Hardware infrastructure upgrade		$72,185		$85,570
Operations and support				
Program management		21,852		28,670
Biometric hardware maintenance		8,280		13,350
Software and system maintenance		73,123		125,292
Network infrastructure maintenance		19,063		19,063
Visa operating personnel	75,926	111,626	114,903	150,603
Port of entry operating personnel		94,679		94,679
Communications		20,577		20,577
Recurring training		32,472		38,040
Consular facility maintenance		89,541		123,628
Annual supplies (cards)		154,809		365,229
Total	**$1,399,156**	**$698,207**	**$1,851,033**	**$1,064,702**

Note: In thousands of fiscal year 2002 constant dollars. Numbers do not sum because of rounding.

Source: GAO analysis.

Table 30: Estimated Costs for Issuing Visas with Biometrics Using Fingerprint and Iris Recognition

	Annual visa applicants			
	10.3 million with visa waiver program		24.3 million without visa waiver program	
Cost element	Initial cost	Annual recurring cost	Initial cost	Annual recurring cost
Investment				
Systems engineering and program management	$151,218		$193,935	
Development; installation; training	820,165		867,087	
Initial biometric hardware	253,098		495,336	
Initial biometric software				
Network infrastructure	228,750		228,750	
Consular facility renovation	378,188		563,655	
Hardware infrastructure upgrade		$119,315		$145,299
Operations and support				
Program management		30,244		38,787
Biometric hardware maintenance		16,601		26,444
Software and system maintenance		96,591		176,331
Network infrastructure maintenance		28,594		28,594
Visa operating personnel	95,044	130,744	160,006	195,706
Port of entry operating personnel		94,679		94,679
Communications		20,577		20,577
Recurring training		70,405		88,966
Consular facility maintenance		100,850		150,308
Annual supplies (cards)		154,809		365,229
Total	**$1,926,463**	**$863,409**	**$2,508,769**	**$1,330,920**

Note: In thousands of fiscal year 2002 constant dollars.

Source: GAO analysis.

Table 31: Estimated Costs for Issuing Visas with Biometrics Using Fingerprint and Facial Recognition

	Annual visa applicants			
	10.3 million with visa waiver program		24.3 million without visa waiver program	
Cost element	Initial cost	Annual recurring cost	Initial cost	Annual recurring cost
Investment				
Systems engineering and program management	$149,375		$191,495	
Development; installation; training	820,165		867,087	
Initial biometric hardware	232,621		468,231	
Initial biometric software				
Network infrastructure	228,750		228,750	
Consular facility renovation	378,188		563,655	
Hardware infrastructure upgrade		$112,557		$136,354
Operations and support				
Program management		29,875		38,299
Biometric hardware maintenance		14,042		23,056
Software and system maintenance		96,591		176,331
Network infrastructure maintenance		28,594		28,594
Visa operating personnel	95,044	130,744	160,006	195,706
Port of entry operating personnel		94,679		94,679
Communications		20,577		20,577
Recurring training		70,405		88,966
Consular facility maintenance		100,850		150,308
Annual supplies (cards)		154,809		365,229
Total	**$1,904,143**	**$853,723**	**$2,479,223**	**$1,318,099**

Note: In thousands of fiscal year 2002 constant dollars. Numbers do not sum because of rounding.

Source: GAO analysis.

Table 32: Estimated Costs for Issuing Visas with Biometrics Using Fingerprint, Iris, and Facial Recognition

	Annual visa applicants			
	10.3 million with visa waiver program		24.3 million without visa waiver program	
Cost element	Initial cost	Annual recurring cost	Initial cost	Annual recurring cost
Investment				
Systems engineering and program mnagement	$177,371		$221,694	
Development; installation; training	1,027,676		1,090,238	
Initial biometric hardware	259,924		504,372	
Initial biometric software				
Network infrastructure	305,000		305,000	
Consular facility renovation	378,188		563,655	
Hardware infrastructure upgrade		$150,527		$182,402
Operations and support				
Program management		35,474		44,339
Biometric hardware maintenance		18,893		30,967
Software and system maintenance		119,661		226,432
Network infrastructure maintenance		38,125		38,125
Visa operating personnel	95,044	130,744	160,006	195,706
Port of entry operating personnel		94,679		94,679
Communications		20,577		20,577
Recurring training		105,608		133,449
Consular facility maintenance		100,850		150,308
Annual supplies (cards)		154,809		365,229
Total	**$2,243,202**	**$969,947**	**$2,844,964**	**$1,482,212**

Note: In thousands of fiscal year 2002 constant dollars. Numbers do not sum because of rounding.

Source: GAO analysis.

Estimated Costs for Issuing Passports with Biometrics

We used the following assumptions to estimate the costs of adding biometrics to passports:

- The number of passport applicants will remain constant at 7 million annually.
- Enrolling travelers using a single biometric (whether for fingerprint, facial, or iris recognition) is estimated at 6 minutes (10 applicants enrolled per hour).
- Enrolling travelers using multiple biometrics (for example, fingerprint and facial combined, fingerprint and iris combined, or fingerprint,

facial, and iris combined) is estimated at 10 minutes (6 applicants enrolled per hour).

- All current passport acceptance offices will be equipped to collect biometrics passport applicants.

Costs were not included for additional inspectors or facility space at ports of entry. Costs are also not included for additional facility space at passport acceptance offices.

Tables 33–38 show the cost of issuing passports with biometrics using fingerprint recognition, iris recognition, facial recognition, fingerprint and iris recognition, fingerprint and facial recognition, and fingerprint, iris, and facial recognition.

Table 33: Estimated Costs for Issuing Passports with Biometrics Using Fingerprint Recognition

Cost element	Initial cost	Annual recurring cost
Investment		
Systems engineering and program management	$370,797	
Development; installation; training	2,665,282	
Initial biometric hardware	229,685	
Initial biometric software		
Network infrastructure	1,225,000	
Consular facility renovation		
Hardware infrastructure upgrade		$450,488
Operations and support		
Program management		74,159
Biometric hardware maintenance		17,514
Software and system maintenance		58,146
Network infrastructure maintenance		153,125
Passport operating personnel		443,805
Port of entry operating personnel		94,679
Communications		122,962
Recurring training		53,875
Consular facility maintenance		
Annual supplies (cards)		105,210
Total	**$4,490,764**	**$1,573,965**

Note: In thousands of fiscal year 2002 constant dollars. Numbers do not sum because of rounding.

Source: GAO analysis.

Table 34: Estimated Costs for Issuing Passports with Biometrics Using Iris Recognition

Cost element	Initial cost	Annual recurring cost
Investment		
Systems engineering and program management	$370,366	
Development; installation training	2,665,282	
Initial biometric hardware	224,898	
Initial biometric software		
Network infrastructure	1,225,000	
Consular facility renovation		
Hardware infrastructure upgrade		$448,908
Operations and support		
Program management		74,073
Biometric hardware maintenance		16,916
Software and system maintenance		58,146
Network infrastructure maintenance		153,125
Passport operating personnel		443,805
Port of entry operating personnel		94,679
Communications		122,962
Recurring training		53,875
Consular facility maintenance		
Annual supplies (cards)		105,210
Total	**$4,485,545**	**$1,571,700**

Note: In thousands of fiscal year 2002 constant dollars**.** Numbers do not sum because of rounding.

Source: GAO analysis.

Table 35: Estimated Costs for Issuing Passports with Biometrics Using Facial Recognition

Cost element	Initial cost	Annual recurring cost
Investment		
Systems engineering and program management	$367,135	
Development; installation; training	2,665,282	
Initial biometric hardware	188,991	
Initial biometric software		
Network infrastructure	1,225,000	
Consular facility renovation		
Hardware infrastructure upgrade		$437,059
Operations and support		
Program management		73,427
Biometric hardware maintenance		12,428
Software and system maintenance		58,146
Network infrastructure maintenance		153,125
Passport operating personnel		443,805
Port of entry operating personnel		94,679
Communications		122,962
Recurring training		53,875
Consular facility maintenance		
Annual supplies (cards)		105,210
Total	**$4,446,407**	**$1,554,716**

Note: In thousands of fiscal year 2002 constant dollars. Numbers do not sum because of rounding.

Source: GAO analysis.

Table 36: Estimated Costs for Issuing Passports with Biometrics Using Fingerprint and Iris Recognition

Cost element	Initial cost	Annual recurring cost
Investment		
Systems engineering and program management	$552,750	
Development; installation; training	4,026,605	
Initial biometric hardware	277,560	
Initial biometric software		
Network infrastructure	1,837,500	
Consular facility renovation		
Hardware infrastructure upgrade		$670,993
Operations and support		
Program management		110,550
Biometric hardware maintenance		24,476
Software and system maintenance		67,777
Network infrastructure maintenance		229,688
Passport operating personnel		443,805
Port of entry operating personnel		94,679
Communications		122,962
Recurring training		107,750
Consular facility maintenance		
Annual supplies (cards)		105,210
Total	**$6,694,415**	**$1,977,890**

Note: In thousands of fiscal year 2002 constant dollars.

Source: GAO analysis.

Table 37: Estimated Costs for Issuing Passports with Biometrics Using Fingerprint and Facial Recognition

Cost element	Initial cost	Annual recurring cost
Investment		
Systems engineering and program management	$549,518	
Development; installation; training	4,026,605	
Initial biometric hardware	241,654	
Initial biometric software		
Network infrastructure	1,837,500	
Consular facility renovation		
Hardware infrastructure upgrade		$659,144
Operations and support		
Program management		109,904
Biometric hardware maintenance		19,988
Software and system maintenance		67,777
Network infrastructure maintenance		229,688
Passport operating personnel		443,805
Port of entry operating personnel		94,679
Communications		122,962
Recurring training		107,750
Consular facility maintenance		
Annual supplies (cards)		105,210
Total	**$6,655,277**	**$1,960,906**

Note: In thousands of fiscal year 2002 constant dollars. Numbers do not sum because of rounding.

Source: GAO analysis.

Table 38: Estimated Costs for Issuing Passports with Biometrics Using Fingerprint, Iris, and Facial Recognition

Cost element	Initial cost	Annual recurring cost
Investment		
Systems engineering and program management	$723,821	
Development; installation; training	5,302,929	
Initial biometric hardware	289,529	
Initial biometric software		
Network infrastructure	2,450,000	
Consular facility renovation		
Hardware infrastructure upgrade		$879,648
Operations and support		
Program management		144,764
Biometric hardware maintenance		26,950
Software and system maintenance		77,407
Network infrastructure maintenance		306,250
Passport operating personnel		443,807
Port of entry operating personnel		94,679
Communications		122,962
Recurring training		161,625
Consular facility maintenance		
Annual supplies (cards)		105,210
Total	**$8,766,279**	**$2,363,302**

Note: In thousands of fiscal year 2002 constant dollars.

Source: GAO analysis.

Appendix VII: Comments from the U.S. Department of State

United States Department of State

Washington, D.C. 20520

Dear Ms. Westin:

We appreciate the opportunity to review your draft report, "TECHNOLOGY ASSESSMENT: Using Biometrics for Border Security," GAO-02-952, GAO Job Code 460525.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report, as well as technical comments.

If you have any questions concerning this response, please contact Columbia Barrosse, Office of Executive Director, Bureau of Consular Affairs, at (202) 663-2504.

Sincerely,

Christopher B. Burnham
Assistant Secretary and
Chief Financial Officer

Enclosure:

As stated.

cc: GAO/IAT - Mr. Richard Hung
State/OIG - Mr. Berman
State/CA - Mr. Frank Moss

Ms. Susan S. Westin,
Managing Director,
International Affairs and Trade,
U.S. General Accounting Office.

Department of State Comments on GAO Draft Report

TECHNOLOGY ASSESSMENT: Using Biometrics for Border Security (GAO-02-952, Job Code 460525)

The Department appreciates the thorough and balanced approach taken by GAO in its assessment of the use of biometrics for Border Security. We find the overall thrust of the report to be in keeping with our own considerations of how a biometrics component could be used in the admission of individuals into the United States and how it could be integrated into the existing process for visa and passport applications. We are particularly gratified to see the GAO report stress the need for high-level policy decisions to be made prior to execution of a biometrics program. Foremost among these are: a decision regarding the specific uses to be made of the biometrics data (identification of individuals, exclusion of dangerous or otherwise inadmissible individuals, etc.); and a cost benefit analysis that weighs effectiveness and security benefits of the program versus resource costs and probable implications or consequences of implementation (including economic, civil liberty and foreign policy). These policy decisions must be made before a selection of the options laid out in this study can be made, a final estimated cost reached, and execution and successful implementation of the program by all involved agencies take place.

It should be noted that the State Department has some additional options for implementation of a biometrics program that will be laid out in our own study. They do not necessarily generally conflict with the options set forth in the GAO report, though final estimated costs might differ.

Appendix VIII: Comments from the U.S. Department of Justice

U.S. Department of Justice

Washington, D.C. 20530

OCT - 3 2002

Ms. Nancy Kingsbury
Managing Director
Applied Research and Methods Issues
U.S. General Accounting Office
441 G Street, NW
Washington, D.C. 20548

Dear Ms. Kingsbury:

On August 30, 2002, the General Accounting Office (GAO) provided the Department of Justice (DOJ) copies of its draft report entitled "TECHNOLOGY ASSESSMENT: Using Biometrics for Border Security." The DOJ is concerned that the report fails to adequately address some of the serious difficulties associated with such programs. The DOJ believes the report does not 1) properly consider an overall border security strategy; 2) adequately recognize the draft National Institute of Standards and Technology (NIST) certified standards recommendations for biometrics, tamper-resistant travel documents, or interoperability; or 3) fully explore the advantages of some biometrics over others. In addition, the report contains a number of serious analytical weaknesses related to a misunderstanding of the false match rate metric and to performance data and levels. A proper understanding and use of biometrics is a critical component of increasing both security and efficiency at our border crossings. The GAO can play an important role in educating the government and the public as to the possibilities and limitations of such systems. We urge the GAO to reconsider major portions of this report, which currently rely on questionable information and interpretation, and to very carefully critique the report to ensure the accuracy of all the information presented.

An Overall Border Security Strategy.
Earlier this year the DOJ prepared an overall border security strategy to significantly improve border security and meet legislative intent and it has shared its strategy with the Office of Homeland Security, the Department of State and others. The U.S. Government is continuing to consider this strategy. The eventual direction selected will require a major investment in border systems and will need to be a foundation for future improvements. Since the existing border security processes, systems, and databases are fragmented and can be readily compromised, any substantial investment in the current state could be a throwaway and thus, it would not yield improvements commensurate with the huge investment required.

In addition, if the requirement to provide a biometric-based enrollment is limited to visa applicants (about 3 percent of the visits to the United States), the impact on preventing potential terrorists entry into the country would be marginalized. Unless enrolling visa applicants is just the first step in a larger process of using biometric-based enrollments, making a huge investment that improves borders security controls for only one of many border entry paths (e.g. visa holders, immigrants, Mexicans with border crossing cards; certain residents of visa-waiver countries; entrants through the Canadian border; U.S. citizens) should be challenged. Without strengthening the controls of the other paths, it would be easy for terrorists to enter via one of those paths.

NIST Standards.
The NIST study, required in the PATRIOT Act, is reaching its final recommendations based on empirical data and scientific methods. The Attorney General and the Secretary of State will rely on the NIST report with regard to the adoption of a technical standard for the design and development of a system to establish and verify unique identities. However, the GAO draft report appears to present information about biometrics inconsistent with the direction of NIST. The GAO team should examine the NIST direction to ensure that its report accurately reflects how various biometrics would fit in the overall context of the intended application. The intended application must: 1) employ a biometric that is able to establish and verify a unique identity in a hundreds of millions population, 2) be used to run a check against criminal records, and 3) operate with a very low risk of either false positive reads or the verification process being ineffective in different border, lighting, and weather conditions. To the extent possible, empirical evidence should support these requirements thereby mitigating the risk of making such a major investment only to discover that the biometric cannot meet the core requirements.

Advantages of Selected Biometrics
In reviewing the use of biometrics, there are certain advantages to the use of fingerprints. Section 221(b) of the Immigration and Nationality Act (INA) requires each alien applying for a visa to be registered by the Department of State unless waived at the discretion of the Secretary of State. Section 262 of the INA further clarifies this registration process to include the collection of fingerprints by stating that every alien in the United States not registered and fingerprinted under section 221(b) who remains in the United States 30 days or longer must apply for registration and be fingerprinted before the expiration of the 30 day period. We believe this constitutes a statutory mandate to register and collect fingerprints for all aliens applying for visas. When considering the variety of biometrics technologies amenable to support border control processes, the GAO should recognize this existing statutory requirement for the pre-arrival collection of fingerprint biometrics for all aliens with visas seeking to travel to the United States.

Fingerprints also are the most effective biometric for computer identification on a large scale. In addition, unlike other biometric data, fingerprints are left at crime scenes. The ability to run latent (unidentified) fingerprints collected at the scene of criminal or terrorist incidents against the database of aliens present in the United States has immense law enforcement value. The National Security Entry-Exit Registration System (NSEERS) is already making use of this capacity in its fingerprint

checks at the border. Further, the report does not consider that the use of fingerprints would allow a search of the incoming visa applicants against the 43 million ten prints sets in Integrated Automated Fingerprint Identification System (IAFIS) to check for prior criminal history. Extrapolating data from the GAO study, approximately 900 persons with prior criminal activity would be screened out per year. While this number is statistically small compared to the total applicant pool, it is significant when one considers the type of person we are trying to prevent from entering the United States. In fact, the ability of fingerprints to provide quick, reliable matches at the border has been well demonstrated by the IDENT/IAFIS integration project. Running prints from aliens in secondary inspection and apprehended by the Border Patrol against this database led to 2,511 arrests between January 1, 2002 and September 18, 2002. This project has been yielding approximately 70 "hits" per week.

Analytical Issues.
While the report provides an overview of biometric products that are typically used for data and facility access control for relatively small systems, it does not provide sufficient analysis of large systems such as those that will be required for effective Border Control. To prevent duplicate identification documents, the subjects enrolled in the Border Control system will have to be searched against each other. This capability will require that the system be of the same order of magnitude as that of IAFIS. It therefore follows that the biometrics used for such a system must have performance numbers that are of the same order of magnitude as IAFIS. We question the reported performance of the facial recognition based Mexican Federal Elections Institute system with respect to false alarms since all available biometric data points to the impossibility of conducting effective facial recognition on that scale. It is suspected that the system does not compare all new search facial records against the database of 60,000,000It probably performs verification only and the database is likely to contain many duplicate records.

Although the report addresses performance issues, it fails to tie the performance requirements with realistic operational impact analysis due in large part to a misuse and misunderstanding the false match rate (FMR) metric. The FMRs and the False Non Matching Rates (FNMR) are dependent on the number of fingerprints captured, the type of image captured (rolled or plain), and the skill and experience of the individual capturing the fingerprint. To assess the impact of the FMR in a given operational setting it would be necessary to consider the size of each operational database and the workload. This relationship is not clearly explained in this report.

Failure to Properly Define and Use the FMR Metric. The report's entire analysis flows as if the size of the required biometric database is irrelevant. It is critical to differentiate between matching errors (FMR and FNMR) and decision errors (false accept rate and false reject rate.) The former are based on one-to-one comparisons and should be independent of the database size, while the later are based on transactions and depend on database size. The FMR is the probability of a false match when one search biometric is compared against one file biometric. It is a metric that is independent of the size of the database. It corresponds to the FNMR which is the probability of a non match when a search biometric is compared against its mated file biometric. An equal rate metric is a popular method for

quickly comparing relative performance metrics for different biometric systems. However, it only makes sense if the two metrics are applied consistently. The improper use of the FMR is in part due to the lack of consistent standards within the industry in reporting their performance levels.

The FMR usually must be resolved by manual means. This has a serious impact on the operational staffing and facility requirements. To assess the impact of the FMR in a given operational setting it is necessary to consider the size of the operational database and the workload. The total number of false matches during operations that must be resolved by the operators during a typical day will be the FMR multiplied by the size of the file database multiplied by the daily workload. This relationship is not clearly explained in the report, worse the FMR is sometimes cited as a system metric that does not rationalize the number by the database size. The significance of this error is exponential.

Systems Performance Data and Levels. The report also provides incorrect performance data for the IAFIS and provides no performance data for other large biometric systems. These two errors lead the report to incorrect conclusions with respect to the viability of various biometric devices. IAFIS was tested rigorously during development and acceptance testing. The system also has been periodically retested to ensure that the performance levels are maintained and improved. In addition, daily statistics are collected for the FMR and failure to enroll rate. The IAFIS performance levels indicate that only a multiple finger based system is capable of supporting the Border Control identification (enrollment) functionality.

The report does not address the fact that some biometrics are by nature multiple biometric. Most subjects have ten fingers, two eyes, and two hands. Nor does the report address the variations in fingerprint technology and the impact of these technologies on system performance. The more data that is captured the better the potential for achieving high performance levels. For IAFIS the primary biometric is ten rolled fingers. In effect it is like fusing ten different biometrics. This is what allows IAFIS to achieve its outstanding performance levels. Tests are currently being conducted to determine the impact on IAFIS of using flat fingerprint data and possibly fewer fingers. All of these factors will play an important role in the design of the Border Control systems.

There also is the issue of the amount of data that is captured. Performance levels can be improved by the simple process of storing and matching against multiple file data. That is, instead of keeping one facial image or one set of fingerprints on file, keep multiple copies on file. By having more copies on file the FNMR can be increased with corresponding trade-offs on the FMR. This clearly has implications on the size of the central matching system. Further, to evaluate the efficacy of the biometrics it is recommended that target performance levels be specified for all of pertinent metrics for identification and verification. In all likelihood different combinations of biometrics will be used for the two functions. Establishing goals also will provide the necessary signals for industry to improve their products or to make more effective use of the biometric information that may be available.

In conclusion, we note that the GAO draft report infers that any move toward biometrics be made slowly and cautiously. While we agree that it is important to proceed judiciously, we must also instill the sense of congressional urgency, both implied and expressed, in the PATRIOT Act and the Enhanced Border Security Act. The DOJ believes that the current border security processes are not effectively preventing terrorists and other criminals from entry into the United States. Most of the processes and systems were designed for a different set of problems decades ago. Adopting biometrics-based unique identification method is a key element in changing what exists today to meet these new challenges to our border security.

As noted by the above comments, we believe that the report falls short by not adequately addressing these significant issues. The DOJ urges you to consider its concerns in preparing the final GAO report on this important subject. If you have any questions regarding the Department's comments, you may contact Vickie L. Sloan, Director, Audit Liaison Office, on (202) 514-0469.

Sincerely,

Robert F. Diegelman
Acting Assistant Attorney General
for Administration

Appendix IX: GAO Contacts and Acknowledgments

GAO Contacts

Nancy R. Kingsbury (202) 512-2700; kingsburyn@gao.gov.
Naba Barkakati (202) 512-4499; barkakatin@gao.gov.

Acknowledgments

Additional staff who made major contributions to this report were Venkareddy Chennareddy, Barbara Hills, Ashfaq Huda, Richard Hung, Elizabeth Johnston, John C. Martin, Eric Ow, Madhav Panwar, Penny Pickett, Tracy Pierson, David Plocher, and Karen Richey.

We gratefully acknowledge the time and assistance of the following people who reviewed a draft of this report: Dennis Carlton, International Biometric Group; Paul Collier, The Biometric Foundation; Larry Hornak, West Virginia University; Anil Jain, Michigan State University; Rick Lazarick, Transportation Security Administration; Peter Neumann, SRI International; Lee Tien, Electronic Frontier Foundation; Jim Wayman, San Jose State University; Charles Wilson, National Institute of Standards and Technology; and John Woodward, RAND Corporation.

We also appreciate the contributions provided by the following organizations during our meetings on biometrics and border security: Airports Council International; American Civil Liberties Union; American Immigration Lawyers Association; Biometric Technology Inc.; Border Trade Alliance; Cameron County Bridge Systems; Cogent Systems Inc.; Electronic Data Systems Corp.; Electronic Privacy Information Center; EyeTicket Corp.; Graphco Technologies Inc.; Identix Inc.; International Biometric Industry Association; International Organization of Masters, Mates, and Pilots; Iridian Technologies Inc.; Mitretek Systems Inc.; National Council La Raza; Recognition Systems Inc.; Sagem Morpho Inc.; and Viisage Technology Inc.

Bibliography

American Association of Motor Vehicle Administrators. *AAMVA National Standard for the Driver License/Identification Card*. AAMVA DL/ID-2000. June 30, 2000. http://www.aamva.org/standards/

American National Standards Institute. *Biometric Information and Security*. ANSI X9.84-2001, 2001. http://www.ansi.org/default.asp

BioAPI Consortium. *BioAPI Specification Version 1.1*, March 16, 2001. http://www.bioapi.org/

Blackburn, Duane M., Mike Bone, and P. Jonathon Phillips. *Facial Recognition Vendor Test 2000: Evaluation Report*. Sponsored by DOD Counterdrug Technology Development Program Office, Defense Advanced Research Projects Agency, and National Institute of Justice, February 16, 2001. http://www.frvt.org/FRVT2000/documents.htm

International Civil Aviation Organization. *Machine Readable Travel Documents Technical Report: Selection of a Globally Interoperable Biometric for Machine-Assisted Identity Confirmation with MRTDS*, 1st ed., 2001. http://www.icao.int/index.cfm

Jain, Anil, Ruud Bolle, and Sharath Pankanti, eds. *Biometrics: Personal Identification in Networked Society*. Boston: Kluwer Academic Publishers, 1999.

Maio, Dario, and others. "FVC 2000: Fingerprint Verification Competition," technical report, University of Bologna, Department of Electronics, Computer Science, and Systems, September 2000.

Mansfield, Tony, and others. *Biometric Product Testing Final Report*. Middlesex, Eng.: National Physical Laboratory, March 19, 2001.

Nanavati, Samir, Michael Thieme, and Raj Nanavati. *Biometrics: Identity Verification in a Networked World*. New York: John Wiley & Sons, 2002.

National Institute of Standards and Technology. *Common Biometric Exchange File Format (CBEFF)*, NISTIR 6529. Gaithersburg, Md.: January 3, 2001.

Phillips, P. Jonathon, and others. "An Introduction to Evaluating Biometric Systems." *IEEE Computer* 33:2 (February 2000): 56–63.

U.S. General Accounting Office. *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*. GAO-02-231T. Washington, D.C.: November 9, 2001.

U.S. General Accounting Office. *Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program*. GAO/OSI-95-20. Washington, D.C.: September 29, 1995.

U.S. General Accounting Office. *Federal Funding for Selected Surveillance Technologies*. GAO-02-438R. Washington, D.C.: March 14, 2002.

U.S. General Accounting. *Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs*. GAO-02-160T. Washington, D.C.: November 7, 2001.

U.S. General Accounting Office. *Identity Fraud: Prevalence and Links to Alien Illegal Activities*. GAO-02-830T. Washington, D.C.: June 25, 2002.

U.S. General Accounting Office. *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*. GAO-01-277. Washington, D.C.: February 26, 2001.

U.S. General Accounting Office. *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*. GAO/AIMD-96-110. Washington, D.C.: September 24, 1996.

U.S. General Accounting Office. *National Preparedness: Technologies to Secure Federal Buildings*. GAO-02-687T. Washington, D.C.: April 25, 2002.

U.S. General Accounting Office. *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*. GAO-02-352. Washington, D.C.: May 31, 2002.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER