

## **Abstract**

This paper will explore how GAO used the Crystal Ball software for determining uncertainty using a Monte Carlo simulation technique in conjunction with a cost estimation spreadsheet to define the uncertainty with the cost of various scenarios for border control using biometrics. The e-Gov project involved conceptualizing various scenarios to automate entry into the United States via the use of biometric data – either part of the passport or the visa. The original report – from which this material is derived – studied various biometric technologies, facial recognition, fingerprint, iris scan, etc and estimated what it would take to implement them on every port of entry into the United States. The Crystal Ball software was used to run a Monte-Carlo type simulation on the costs to give a range of values.

One facet of the US 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 US 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 a 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.

### **What the study asked GAO to assess:**

1. What biometric technologies are currently deployed, currently available but not deployed, or in development that could be deployed in the near 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?

---

## **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 of the Study**

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.

<b>Technology</b>	<b>How it works</b>	<b>Suitable for border control</b>
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

### **Cost and Uncertainty Analysis**

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.

---

## **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. The data is then 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.

---

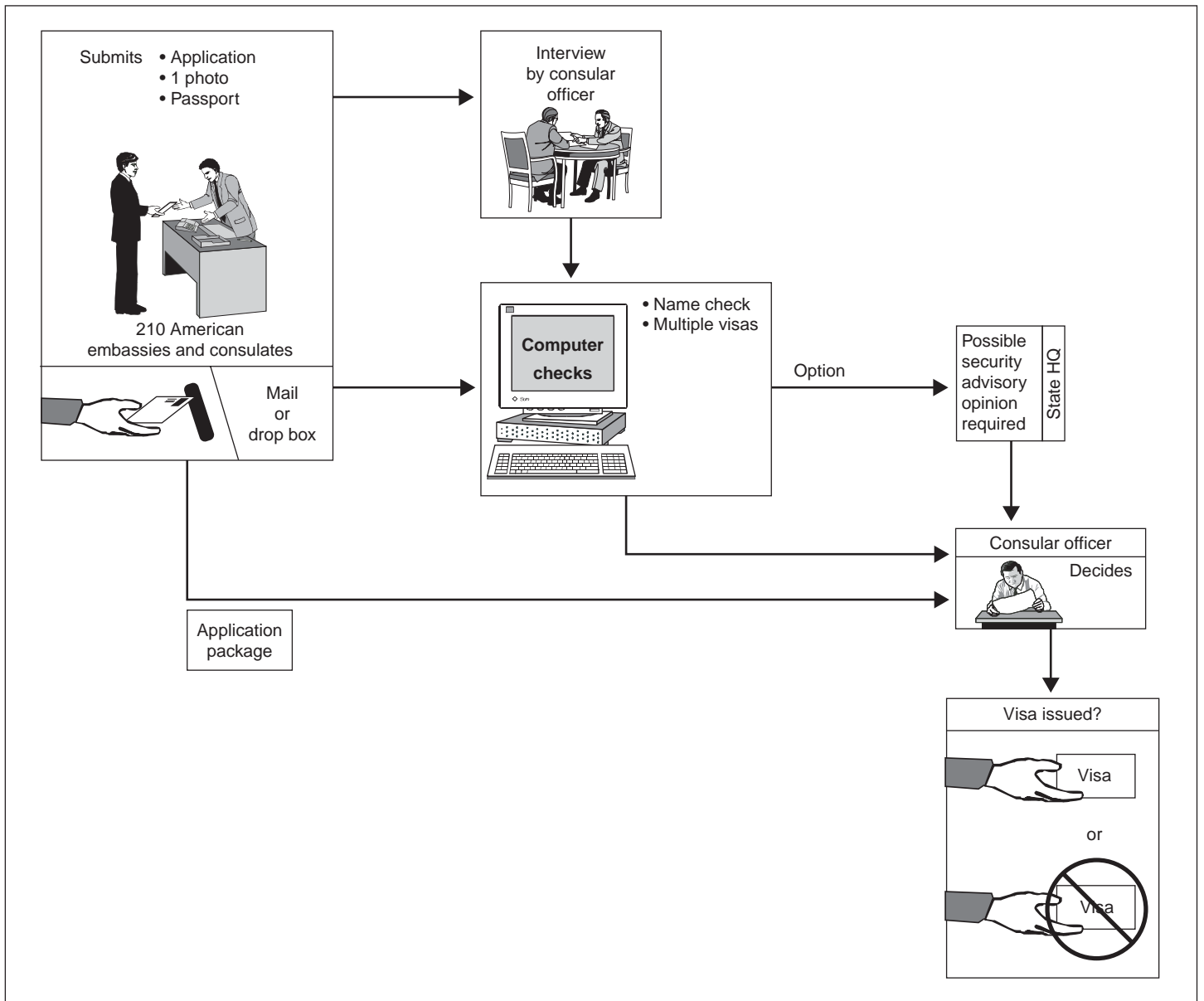
## **Port of Entry Inspections**

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.

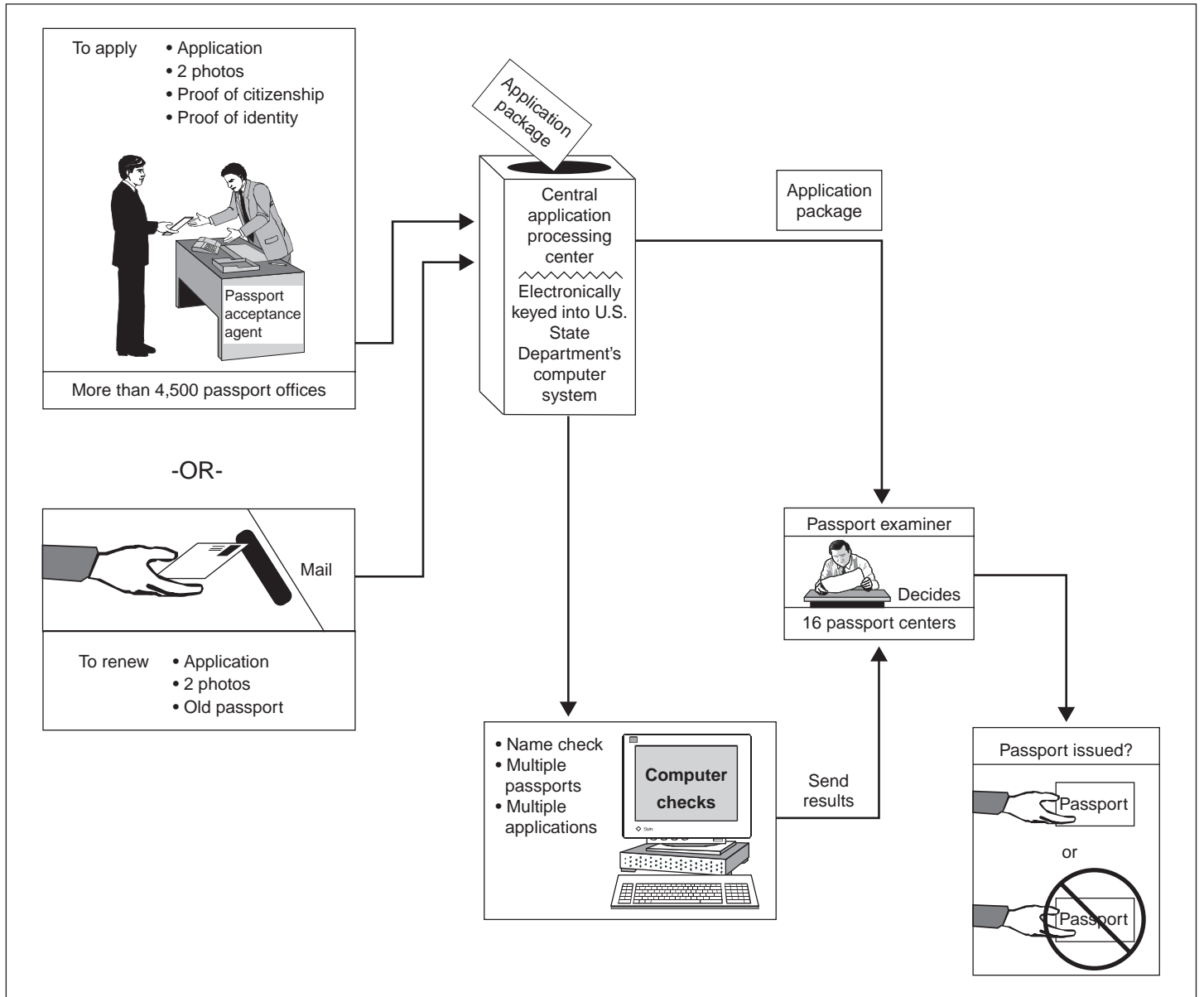
### **Number of Inspections at U.S. Ports of Entry, Fiscal Year 2001**

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

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.



Visa Application Process



Passport Application Process

# Scenarios, Cost Elements, and Uncertainty

---

## 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.

<b>Scenario</b>	<b>Initial cost</b>	<b>Annual recurring cost</b>
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 millions.

For items 3 and 4, we estimated costs for various biometrics such as fingerprint, iris, facial, and combination of the three. Only one such model for each is discussed in this paper.

---

## 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 assumed 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).

### 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.

Scenario	Initial		Recurring			
	Cost	% certainty	Cost at 90% certainty	Cost	% certainty	Cost at 90% certainty
1. Watch list check before issuing document	\$52.80	50%	\$53.30	\$72.90	50%	\$74.20
2. Watch list check and facial recognition	330.2	50	347.9	237	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

Cost Estimation Models

Scenario 1 Watch list check before issuing travel documents

Scenario 2 Watch list check before entering the United States

Cost element	Watch list check before Issuing travel documents		Watch list check before Entering the United States	
	Initial cost	Annual recurring cost	Initial cost	Annual recurring cost
<b>Investment</b>				
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		100,100	
Consular facility renovation	570		570	
Hardware infrastructure upgrade		\$2,523		\$38,969
<b>Operations and support</b>				
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
<b>Total</b>	<b>\$52,830</b>	<b>\$72,896</b>	<b>\$330,197</b>	<b>\$236,960</b>

## Cost Estimation Model

### Scenario 3 Issuing Visas with Biometrics Using Fingerprint Recognition

Cost element	Annual visa applicants			
	10.3 million		24.3 million	
	with visa waiver program		without visa waiver program	
	Initial cost	Annual recurring cost	Initial cost	Annual recurring cost
<b>Investment costs</b>				
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
<b>Operations and support</b>				
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
<b>Total</b>	<b>\$1,422,042</b>	<b>\$708,138</b>	<b>\$1,878,832</b>	<b>\$1,076,765</b>

## Cost Estimation Model

### Scenario 4 Issuing passports with biometrics – fingerprints and iris

<b>Cost element</b>	<b>Initial Cost</b>	<b>Annual Recurring Cost</b>
<b>Investment</b>		
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
<b>Operations and support</b>		
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
<b>Total</b>	<b>\$6,694,415</b>	<b>\$1,977,890</b>

## Uncertainty Analysis Demo

During this session, GAO will present a demonstration of the Crystal Ball Uncertainty Tool.