United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, May 19, 2004

AVIATION SECURITY

Challenges in Using Biometric Technologies

Statement of Keith A. Rhodes, Chief Technologist
Applied Research and Methods

GAO-04-785T

May 19, 2004

AVIATION SECURITY

Challenges in Using Biometric Technologies

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-785T, a testimony before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives

Why GAO Did This Study

One of the primary functions of any security system is the control of people moving into or out of protected areas, such as physical buildings, information systems, and our national border. Technologies called biometrics can automate the identification of people by one or more of their distinct physical or behavioral characteristics. 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. Since the September 11, 2001, terrorist attacks, laws have been passed that require a more extensive use of biometric technologies in the federal government.

In 2002, GAO conducted a technology assessment on the use of biometrics for border security. GAO was asked to testify about the issues that it raised in the report, the current state of the technology, and the application of biometrics to aviation security.

www.gao.gov/cgi-bin/getrpt?GAO-04-785T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Keith Rhodes at (202) 512-6412 or rhodesk@gao.gov.

What GAO Found

Biometric technologies are available today that can be used for aviation security. Biometric technologies vary in complexity, capabilities, and performance, and can be used to verify or establish a person's identity. Leading biometric technologies include facial recognition, fingerprint recognition, hand geometry, and iris recognition. The Federal Aviation Administration (FAA), and subsequently, the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA), has been examining the use of biometrics for aviation security for several years. TSA has three current pilot projects that will study the use of biometrics to enhance aviation security: the Transportation Worker Identification Credential (TWIC), registered traveler, and an access control pilot program designed to secure sensitive areas of an airport.

It is important to bear in mind that effective security cannot be achieved by relying on technology alone. Technology and people must work together as part of an overall security process. Weaknesses in any of these areas diminish the effectiveness of the security process. The security process needs to account for limitations in biometric technology. For example, some people cannot enroll in a biometrics system because they lack the appropriate body part. Similarly, errors sometimes occur during matching operations. Exception processing that is not as good as biometric-based primary processing could be exploited as a security hole. Further, non-technological processes for enrollment are critical to the success of a biometrics-based identity management system. Before a person is granted a biometric credential, the issuing authority needs to assure itself that the person is eligible to receive such a credential.

We have found that three key considerations need to be addressed before a decision is made to design, develop, and implement biometrics into a security 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 convenience.

Security concerns need to be balanced with practical cost and operational considerations as well as political and economic interests. A risk management approach can help federal agencies identify and address security concerns. To develop security systems with biometrics, the high-level goals of these systems need to be defined, and the concept of operations that will embody the people, process, and technologies required to achieve these goals needs to be developed. With these answers, the proper role of biometric technologies in aviation security can be determined.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing on the use of biometrics for aviation security. The security of the U.S. commercial aviation system has been a long-standing concern. Following the September 11, 2001, terrorist attacks, virtually all aviation security responsibilities now reside within the Department of Homeland Security (DHS) and its Transportation Security Administration (TSA). These responsibilities include the conduct of passenger and baggage screening and overseeing security measures for airports, commercial aircraft, air cargo, and general aviation. DHS and TSA have undertaken several initiatives to improve aviation security. Some efforts, including those involving access control to secure areas of an airport and identifying travelers, include biometric technologies.

One of the primary functions of any security system is the control of people moving into or out of protected areas, such as physical buildings, information systems, and our national border. 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.

Technologies called biometrics can automate the identification of people by one or more of their distinct physical or behavioral characteristics—by something they are. The term biometrics covers a wide range of technologies that can be used to verify identity by measuring and analyzing human characteristics. Biometrics theoretically represent a more effective approach to security because each person's characteristics are thought to be distinct and, when compared with identification cards and passwords, are less easily lost, stolen, counterfeited, or otherwise compromised.

As requested, I will provide an overview of biometric technologies that are currently available, describe some of the current uses of these technologies, and discuss the issues and challenges associated with the implementation of biometrics. My testimony today is based on a body of

work we completed in 2002 that examined the use of biometrics for border control. In that report, we discussed the maturity of several biometric technologies, the possible implementation of these technologies in current border control processes, and the policy implications and key considerations for using these technologies.[1] We also researched selected prior and current TSA and DHS biometrics initiatives and summarize them in this statement. We performed our work in accordance with generally accepted government auditing standards.

Biometric Technologies for Personal Identification

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. 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.

How Biometric 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

[1]U.S. General Accounting Office, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

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 start with an enrollment stage followed by a matching stage that can use either 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 and 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 is based on the system vendor's proprietary algorithms. Template size varies depending on the vendor and the technology. 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. Consequently, each time an individual's biometric data are captured, the new template is likely to be unique. 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 an identifier, 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.

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 is 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. 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.

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 computer 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 watch list system. 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 biometric may be faces captured from mug shots provided by a law enforcement agency.

Matches Are Based on Threshold Settings

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. 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. We describe seven leading biometric technologies:

- Facial Recognition
- Fingerprint Recognition
- Hand Geometry
- Iris Recognition
- Retina Recognition
- Signature Recognition
- Speaker Recognition

Facial Recognition

Facial recognition technology identifies people by analyzing features of the face that are 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.

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 at the time of our study, we found there were more than 75 fingerprint recognition technology companies. Until recently, fingerprint recognition 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. In 2002, we found that optical scanners were 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. 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 takes 96 measurements of the hand, including 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. 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. The shape and size of our hands are reasonably diverse, but are not highly distinctive. Thus, hand geometry is not suitable for performing identification matches.

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. These characteristics, which are formed during the 8th month of gestation, reportedly remain stable throughout a person's lifetime, except in cases of injury. Iris recognition can be used in both verification and identification systems.

Iris recognition systems use a small, high-quality camera to capture a black and white, high-resolution image of the iris. The systems then define the boundaries of the iris, establish a coordinate system over the iris, and define the zones for analysis within the coordinate system.

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 diseases 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.

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 name 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.

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 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.

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

Accuracy of Biometric Technology

Biometrics is a 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, unauthorized 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.

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 he or she should be denied. For example, if a person who has enrolled in a public benefits program under another identity is not correctly matched, he or she will succeed in gaining fraudulent access to benefits.

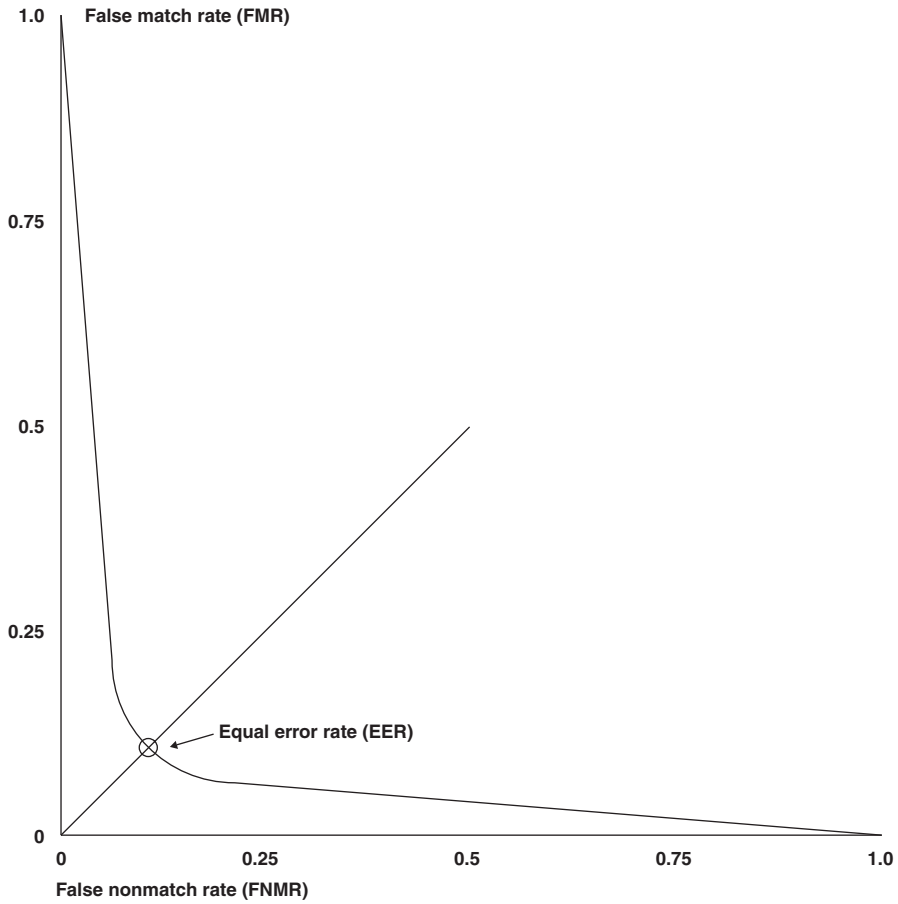
False matches may occur because there is a high degree of similarity between two individuals' characteristics. False nonmatches occur because there is not a sufficiently strong similarity between an individual's enrollment and trial templates, which could be caused by any number of conditions. For example, 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. As figure 1 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.

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. 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.

Figure 1: The General Relationship between FMR and FNMR



Source: GAO.

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

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.

Using Multiple 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.

Standards for Biometric Technology

Identifying, exchanging, and integrating information from different and perhaps unfamiliar sources and functions are essential to an effective biometrics application. Without standards, system developers may need to define in detail the precise steps for exchanging information, a potentially complex, time-consuming, and expensive process. Progress has been made in developing biometrics standards. 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. Devices from company A do not necessarily work compatibly with devices from companies B and C.

Standards such as the National Institute of Science and Technology's (NIST) Common Biometric Exchange File Format (CBEFF) facilitate data exchange between different system components and simplify the integration of software and hardware from different vendors. The wavelet scalar quantization (WSQ) gray-scale fingerprint image compression algorithm is the standard for exchanging fingerprint images within the criminal justice system. Similarly, the Joint Photographic Experts Group (JPEG) has established an image compression standard that is designed to facilitate the transfer of images for facial recognition systems.

The American Association for Motor Vehicle Administration (AAMVA) included a format for fingerprint minutiae data in its Driver License and

Identification Standard, which provides a uniform means to identify issuers and holders of driver's licenses in the United States and Canada. However, the standard still allows for including data in a vendor-specific format. Biometric templates, which capture only the critical data needed to make a match, are small, but the template one vendor uses cannot generally be used by another for some biometric technologies, such as fingerprints. Without the creation and industry adoption of 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. Last year, the International Civil Aviation Organization (ICAO) New Technologies Working Group concluded that the only reliable globally interoperable method for exchanging face, fingerprint, or iris biometric data was the storage of the respective image. ICAO is studying the use of biometrics in machine-readable travel documents, such as passports and visas.

In November 2001, the executive board of the International Committee for Information Technology Standards (INCITS) established a technical committee for biometrics for the rapid development and approval of formal national and international generic biometric standards. Four task groups were created to conduct the work. The first task group is focused on the standardization of the content, meaning, and representation of biometric data interchange formats. This task group is working on formats for representing fingerprints, faces, irises, hand geometry, and signatures. The second task group covers the standardization of interfaces and interactions between biometric components and subsystems. CBEFF is an example of an interface standard. The third task group focuses on the development of biometric application profiles. It currently has projects in the areas of border crossings, transportation workers, and point of sale. The fourth task group handles the standardization of biometric performance metric definitions and calculations, approaches to test performance, and requirements for reporting the results of these tests.

Using Biometrics for Aviation Security

The Federal Aviation Administration (FAA), and subsequently, DHS and TSA, has been examining the use of biometrics for aviation security for several years. In 2001, the FAA and the Department of Defense Counterdrug Technology Development Program Office co-chaired the Aviation Security Biometrics Working Group (ASBWG). They examined the use of biometrics in four aviation security applications: (1) identity verification of employees and ensuring that access to secured areas within an airport is restricted to authorized personnel; (2) protection of public areas in and around airports using surveillance; (3) identity verification of

passengers boarding aircraft; and (4) identity verification of flight crews prior to and during a flight. Subsequently, in 2002, TSA contracted with the International Biometric Group to evaluate the use of biometrics for automated surveillance within airports, trusted traveler cards for passengers, and identity verification of employees for access control in airports.[2]

Since the 2001 terrorist attacks, the Congress has directed a greater use of biometrics. For example, the Aviation and Transportation Security Act (ATSA), which created TSA and mandated several actions designed to enhance aviation security, includes several provisions regarding the use of biometrics for applications, such as perimeter security or access control.[3]

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 hand geometry systems. Further, 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 using an iris recognition system to protect confidential files and working documents. Other federal agencies, including the Department of Defense, Department of Energy, and Department of Justice, as well as the intelligence community, are adopting similar technologies.

We have previously reported on the critical need to limit access to secure airport areas. In 2000, we reported on the ability of our special agents to use fictitious law enforcement badges and credentials to gain access to secure areas of two commercial airports.[4] The agents, who had been issued tickets and boarding passes, were not screened through magnetometers at the security checkpoints nor was their baggage inspected. This vulnerability could have allowed our agents to carry weapons, explosives, or other dangerous objects onto an aircraft.

[2]International Biometric Group, "Framework for Evaluating and Deploying Biometrics in Air Travel Applications: Surveillance, Trusted Travel, Access Control" (Apr. 3, 2002).

[3]Aviation and Transportation Security Act (Public Law 107-71, Nov. 19, 2001).

[4]U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports*, GAO/T-OSI-00-10 (Washington, D.C.: May 25, 2000).

Since 1991, San Francisco International Airport has used hand geometry devices in conjunction with identification cards to protect secure areas of the airport, such as the tarmac and loading gates. Last year, Toledo (Ohio) Express Airport also installed hand geometry devices to ensure that only authorized personnel can gain access to critical areas of the airport.

FAA has conducted several tests and pilots of biometrics for access control to secure areas of airports. In 1998, FAA funded an operational test at Chicago's O'Hare International Airport involving smart cards and fingerprint recognition to identify employees of motor carrier and air cargo companies at access control points to cargo areas. Further, in 2001, FAA conducted tests of hand geometry and fingerprint and facial recognition technologies for employee access control at airports.

TSA has two current efforts examining the use of biometrics for access control. The Transportation Worker Identification Credential (TWIC) is designed to be a common credential for all transportation workers requiring unescorted physical access to secure areas of the national transportation system, such as airports, seaports, and railroad terminals. It will also be used to help secure logical access to computers, networks, and applications. The program was developed in response to ATSA and the Maritime Transportation Security Act of 2002 and will include the use of biometrics to provide a positive match of a credential for up to 6 million transportation workers across the United States.[5] The TWIC program is designed as an identity authentication tool for individual facilities and to provide assurance that individuals with a TWIC card have undergone a threat assessment to ensure that they are not known terrorists. Individual facilities will be able to use the TWIC cards to control access to secure areas to only authorized individuals.

Last week, TSA issued a request for proposal for a TWIC prototype to determine the performance of TWIC as an access control tool. For the prototype, TSA will be examining the use of at least fingerprint and iris recognition. During a technology evaluation last year, TSA evaluated six card technologies and determined that an integrated circuit chip smart card was the most appropriate for the TWIC card. As part of the prototype, TSA will also examine the use of cards with 2-dimensional bar codes and optical stripes. The prototype phase is expected to last 7 months and will

[5]Aviation and Transportation Security Act, §106(c) and §136, and Maritime Transportation Security Act of 2002 (Public Law 107-295, Nov. 25, 2002), §102.

be conducted in Philadelphia, PA; Wilmington, DE; the ports of Long Beach and Los Angeles, CA; and the 14 major port facilities in the state of Florida. TSA anticipates that up to 200,000 workers will be enrolled in the program. Following the prototype, TSA will make a decision on whether to proceed with implementation of the program.

Earlier this month, TSA announced an access control pilot program that will test various technologies, including biometrics, that are designed to ensure that only authorized personnel have access to non-passenger controlled areas. Developed in response to a section in ATSA that directed the establishment of pilot programs to test and evaluate technologies for providing access control to closed or secure areas of airports, the program will test fingerprint recognition at four airports and iris recognition at one airport.[6] Boise Air Terminal/Gowen Field Airport, Southwest Florida International Airport, and Tampa International Airport will test fingerprint recognition to control vehicle access. Newark International Airport will test fingerprint recognition to allow only authorized persons into secure areas of the airport. T.F. Green State Airport (Providence, RI) will test iris recognition to control access to secure areas of the airport.

Registered Traveler

The concept of a registered traveler program is to provide an expedited security screening for passengers who meet the eligibility criteria and who voluntarily provide personal information and clear a background check. ATSA permits TSA to "establish requirements to implement trusted passenger programs and use available technologies to expedite the security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening."[7]

In 2002, we reviewed the policy and implementation issues associated with a registered traveler program.[8] We identified four key questions that need to be addressed by the federal government before proceeding with such a program: (1) What criteria should be established to determine eligibility to apply for the program? (2) What kinds of background checks should be

[6]Aviation and Transportation Security Act, §106(d).

[7]Aviation and Transportation Security Act, §109(a)(3).

[8]U.S. General Accounting Office, *Aviation Security: Registered Traveler Program Policy and Implementation Issues*, GAO-03-253 (Washington D.C.: Nov. 22, 2002).

used to certify that applicants are eligible to enroll in the program, and who should perform these? (3) Which security-screening procedures should registered travelers undergo, and how should these differ from those used for unregistered travelers? and (4) To what extent do equity, privacy, and liability issues have to be resolved prior to program implementation?

In April 2004, TSA issued a combined solicitation synopsis for a registered traveler pilot program. TSA has evaluated the capabilities statements from about 40 proposals. TSA expects to award contracts for the pilot program in early June 2004. The pilot program will run for about 90 days at up to five airports. TSA expects to enroll up to 10,000 travelers in the program using fingerprint and/or iris recognition. To enroll, travelers will submit biographic and biometric data at the selected airports. A security assessment will be conducted on the applicants to verify their eligibility for the program. TSA may use a TSA-issued card or an airline frequent flier card as an identifier to conduct biometric verification matches of registered travelers at airport security checkpoints. TSA is also considering the use of identification (1-to-many) matching to ascertain the identity of the registered traveler. Once registered travelers are identified, they will undergo an adjusted screening process, designed to expedite throughput for low-risk travelers.

Similar programs have been used for expediting border control processes. For example, the Immigration and Naturalization Service (INS) Passenger Accelerated Service System (INSPASS), a pilot program in place since 1993, has more than 45,000 frequent fliers enrolled at nine airports, and has admitted more than 300,000 travelers. 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.[9] To participate, users provide a passport or travel document and submit two fingerprints and a hand geometry biometric. Once travelers successfully undergo a background screening and are enrolled, they can circumvent immigration procedures and lines. An INSPASS participant presents their hand geometry biometric at an airport kiosk for comparison against the reference template stored in a central database for that traveler. INSPASS has reduced the inspection time for participants to less than 15 seconds.

[9]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.

Airport Surveillance

It has been suggested that facial recognition could be used in airports as a surveillance tool that could identify persons of interest without the subject's cooperation or knowledge. Key to such an effort is the availability of a database of biometric information of persons of interest (i.e., a watch list). Surveillance activities are often conducted by humans who are looking for persons of interest using closed-circuit televisions. However, because it is well understood that humans are limited in their ability to recognize individuals they are not familiar with, and that there are limits of human attention when conducting surveillance activities, facial recognition has been cited as a potential surveillance tool.

In 2001, the ASBWG found that facial recognition technology was not sufficiently mature to be relied upon for wide-area surveillance. Further, as we reported in 2002, one vendor conducted pilots using facial recognition technology to conduct surveillance at U.S. airports. For these pilots, video cameras were installed at the security checkpoints, near the magnetometers. From the pilots, it was learned that lighting was the primary factor in determining the performance of facial recognition.

Other Federal Biometric Applications

There are two other primary uses of biometrics in the federal government: criminal identification and border security.

Criminal Identification

Fingerprint identification has been used in law enforcement over the past 100 years and has become the de facto international standard for positively identifying individuals. The Federal Bureau of Investigation (FBI) has been using fingerprint identification since 1928. The first fingerprint recognition systems were used in law enforcement about 4 decades ago.

The FBI's Integrated Automated Fingerprint Identification System (IAFIS) is an automated 10-fingerprint matching system that stores 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. In 2002, we found that IAFIS 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.

Border Security

There are several uses of biometrics for border security in the United States and worldwide.[10] Two notable examples are the INS Automated Biometric Fingerprint Identification System (IDENT) and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system.

INS began developing 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. In 2002, IDENT had over 4.5 million entries. A fingerprint query of IDENT normally takes about 2 minutes.

Laws passed since the September 11, 2001, terrorist attacks require a more extensive use of biometrics for border control.[11] The Attorney General and the Secretary of State jointly, through NIST are to develop a technology standard, including biometric identifier standards.[12] When developed, this standard is to be used to verify the identity of persons applying for a U.S. visa for the purpose of conducting a background check, confirming identity, and ensuring that a person has not received a visa under a different name. Further, aliens are to be issued machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers. Similarly, equipment and software are to be installed at all ports of entry that can allow the biometric comparison and authentication of all U.S. visas and other travel and entry documents issued to aliens and machine-readable passports.

[10]We describe several of these uses in *Technology Assessment: Biometrics for Border Security*, GAO-03-174.

[11]See the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Public Law 107-56, Oct. 26, 2001), §403(c) and §414, and the Enhanced Border Security and Visa Entry Reform Act of 2002 (Public Law 107-173, May 14, 2002), §202(a)(4) and §303.

[12]In January 2003, in response to this requirement, NIST submitted its technical standards for biometric identifiers and tamper-resistance for travel documents as a part of a joint report to the Congress from the Attorney General, the Secretary of State, and NIST. NIST recommended that 10 fingerprints be used for background identification checks and that a dual biometric system using 2 fingerprint images and a face image may be needed to meet projected system requirements for verification.

DHS is developing the US-VISIT system to address these requirements. The US-VISIT system currently uses IDENT technology to collect a photograph and two index fingerprints from travelers holding non-immigrant visas. Travelers are initially enrolled either at a port of entry using US-VISIT entry procedures or at a U.S. consulate or embassy when they apply for their visa. US-VISIT entry procedures are currently in place at 115 airports and 14 seaports. By December 31, 2004, US-VISIT is planned to be in place at the 50 busiest land ports of entry. By December 31, 2005, US-VISIT is planned to be in place at all 165 land ports of entry. As of March 4, 2004, biometric data collection was in place at more than 80 visa-adjudicating posts. By October 2004, biometric data collection is expected to be in use at all 211 visa-issuing embassies and consulates. By September 30, 2004, US-VISIT procedures will be expanded to include visitors traveling to the United States under the visa waiver program arriving at air and sea ports of entry.

Each time a visitor enters the United States at a port of entry employing US-VISIT entry procedures, the visitor's fingerprints will be matched against the reference fingerprints captured during enrollment. During enrollment and each subsequent visit, the biographic and biometric data of the visitor is compared to watch lists to assist the inspectors in making admissibility decisions. At one airport and one seaport, visitors are also expected to record their departure from the United States using an automated self-service kiosk that can scan the visitor's travel documents and capture the visitor's fingerprints.[13]

Challenges and Issues in Using Biometrics

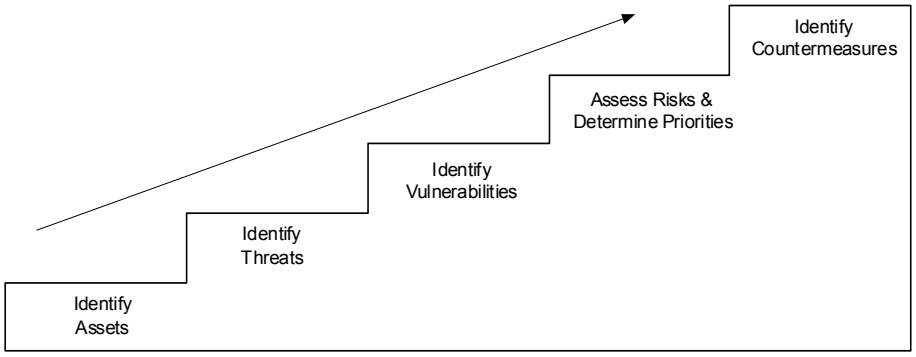
While biometric technology is currently available and used in a variety of applications, questions remain regarding the technical and operational effectiveness of biometric technologies in large-scale applications. We have found that a risk management approach can help define the need and use for biometrics for security. In addition, a decision to use biometrics should consider the costs and benefits of such a system and its potential effect on convenience and privacy.

[13]GAO has conducted reviews of annual expenditure plans of the US-VISIT program. The review of the fiscal year 2004 expenditure plan can be found in U.S. General Accounting Office, *Homeland Security: First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed*, GAO-04-586 (Washington, D.C.: May 11, 2004).

Risk Management Is the Foundation of Effective Strategy

The approach to good security is fundamentally similar regardless of the assets being protected. As we have previously reported, these principles can be reduced to five basic steps that help to determine responses to five essential questions (see figure 2).[14]

Figure 2: Five Steps in the Risk Management Process



Source: GAO.

What Am I Protecting?

The first step in risk management is to identify assets that must be protected and the impact of their potential loss.

Who Are My Adversaries?

The second step is to identify and characterize the threat to these assets. The intent and capability of an adversary are the principal criteria for establishing the degree of threat to these assets.

How Am I Vulnerable?

The third step involves identifying and characterizing vulnerabilities that would allow identified threats to be realized. In other words, what weaknesses can allow a security breach?

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

What Are My Priorities?

In the fourth step, risk must be assessed and priorities determined for protecting assets. Risk assessment examines the potential for the loss or damage to an asset. Risk levels are established by assessing the impact of the loss or damage, threats to the asset, and vulnerabilities.

What Can I Do?

The final step is to identify countermeasures to reduce or eliminate risks. In doing so, the advantages and benefits of these countermeasures must also be weighed against their disadvantages and costs.

Protection, Detection, and Reaction Are Integral Security Concepts

Countermeasures identified through the risk management process support the three integral concepts of a holistic security program: protection, detection, and reaction. Protection provides countermeasures such as policies, procedures, and technical controls to defend against attacks on the assets being protected. Detection monitors for potential breakdowns in protective mechanisms that could result in security breaches. Reaction, which requires human involvement, responds to detected breaches to thwart attacks before damage can be done. Because absolute protection is impossible to achieve, a security program that does not incorporate detection and reaction is incomplete.

Biometrics can support the protection component of a security program. It is important to realize that deploying them will not automatically eliminate all security risks. Technology is not a solution in isolation. Effective security also entails having a well-trained staff to follow and enforce policies and procedures. Weaknesses in the security process or failures by people to operate the technology or implement the security process can diminish the effectiveness of technology.

Accordingly, there is a need for the security process to account for limitations in technology. For example, procedures for exception processing would also need to be carefully planned. As we described, not all people can enroll in a biometrics system. Similarly, false matches and false nonmatches will also sometimes occur. Procedures need to be developed to handle these situations. Exception processing that is not as good as biometric-based primary processing could be exploited as a security hole. The effect on the process is directly related to the performance of the technology. In our study of biometrics for border security, we found that fingerprint recognition appears to be the most

mature of the biometric technologies. Fingerprint recognition has been used the longest and has been used with databases containing up to 40 million entries. Iris recognition is a young technology and has not been used with large populations. While facial recognition has also been used with large databases, its accuracy results in testing have lagged behind those of iris and fingerprint recognition.

As with any credentialing or identity management system, it is critical to consider the process used to issue the credential. Biometrics can help ensure that people can only enroll into a security system once and to ensure that a person presenting himself before the security system is the same person that enrolled into the system. However, biometrics cannot necessarily link a person to his or her true identity. While biometrics would make it more difficult for people to establish multiple identities, 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. The use of biometrics does not relieve the credential-issuing authority of the responsibility of ensuring the identity of the person requesting the credential or of conducting a security check, commensurate with the level of access being granted, to assure itself that the person is entitled to receive the credential. The quality of the identifier presented during the enrollment process is key to the integrity of a biometrics system.

Even if the biometric is checked against a biometrics-based watch list, the effectiveness of such a list is also dependent on nontechnological processes. The policies and procedures governing the population of the watch list as well as the effectiveness of the law enforcement and intelligence communities to identify individuals to place on the watch list are critical to the success of the program. People who are not on the watch list cannot be flagged as someone who is not eligible to receive a credential.

Deciding to Use Biometric Technology

A decision to use biometrics in a security solution should also consider the benefits and costs of the system and the potential effects on convenience and privacy.

Weighing Costs and Benefits

Best practices for information technology investment dictate that prior to making any significant project investment, the benefit and cost information of the system should be analyzed and assessed in detail. A business case should be developed that identifies the organizational needs for the project and a clear statement of high-level system goals should be developed. The high-level goals should address the system's expected

outcomes such as the binding of a biometric feature to an identity or the identification of undesirable individuals on a watch list. Certain performance parameters should also be specified such as the time required to verify a person's identity or the maximum population that the system must handle.

Once the system parameters are developed, a cost estimate can be developed. Not only must the costs of the technology be considered, but also the costs of the effects on people and processes. Both initial costs and recurring costs need to be estimated. Initial costs need to account for the engineering efforts to design, develop, test, and implement the system; training of personnel; hardware and software costs; network infrastructure improvements; and additional facilities required to enroll people into the biometric system. Recurring cost elements include program management costs, hardware and software maintenance, hardware replacement costs, training of personnel, additional personnel to enroll or verify the identities of people in the biometric system, and possibly the issuance of token cards for the storage of biometrics.

Weighed against these costs are the security benefits that accrue from the system. Analyzing this cost-benefit trade-off is crucial when choosing specific biometrics-based solutions. The consequences of performance issues—for example, accuracy problems, and their effect on processes and people—are also important in selecting a biometrics solution.

Effects on Privacy and Convenience

The Privacy Act of 1974 limits federal agencies' collection, use, and disclosure of personal information, such as fingerprints and photographs.[15] Accordingly, the Privacy Act generally covers federal agency use of personal biometric information. However, 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 of biometric data and (2) secondary uses and "function creep." These concerns relate to the adequacy of protections under current law for 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.

[15] 5 U.S.C. §552a.

Because there is no general agreement on the appropriate balance of security and privacy to build into a system using biometrics, further policy decisions are required. 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.

Finally, consideration must be given to the convenience and ease of using biometrics and their effect on the ability of the agency to complete its mission. For example, some people find biometric technologies difficult, if not impossible, to use. Still others resist biometrics because they believe them to be intrusive, inherently offensive, or just uncomfortable to use. Lack of cooperation or even resistance to using biometrics can affect a system's performance and widespread adoption.

Furthermore, if the processes to use biometrics are lengthy or erroneous, they could negatively affect the ability of the assets being protected to operate and fulfill its mission. For example, in 2002, we found that there are significant challenges in using biometrics for border security. The use of biometric technologies could potentially impact the length of the inspection process. Any lengthening in the process of obtaining travel documents or entering the United States could affect travelers significantly. Delays inconvenience travelers and could result in fewer visits to the United States or lost business to the nation. Further studies could help determine whether the increased security from biometrics could result in fewer visits to the United States or lost business to the nation, potentially adversely affecting the American economy and, in particular, the border communities. These communities depend on trade with Canada and Mexico, which totaled $653 billion in 2000.

In conclusion, biometric technologies are available today that can be used for aviation security. However, it is important to bear in mind that effective security cannot be achieved by relying on technology alone. Technology and people must work together as part of an overall security process. As we have pointed out, weaknesses in any of these areas diminishes the effectiveness of the security process. We have found that three key considerations need to be addressed before a decision is made to design, develop, and implement biometrics into a security 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 convenience.

Security concerns need to be balanced with practical cost and operational considerations as well as political and economic interests. A risk management approach can help federal agencies identify and address security concerns. To develop security systems with biometrics, the high-level goals of these systems need to be defined, and the concept of operations that will embody the people, process, and technologies required to achieve these goals needs to be developed. With these answers, the proper role of biometric technologies in aviation security can be determined. If these details are not resolved, the estimated cost and performance of the resulting system will be at risk.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or members of the subcommittee may have.

Contacts

For further information, please contact Keith Rhodes at (202)-512-6412 or Richard Hung at (202)-512-8073.

GAO's Mission

The General Accounting Office, the audit, evaluation and 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 e-mail alerts" under the "Order GAO Products" 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