September 9, 2003

INFORMATION SECURITY

Challenges in Using Biometrics

Highlights of GAO-03-1137T, a testimony for the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives

Why GAO Did This Study

One of the primary functions of any security system is the control of people 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. In the last 2 years, laws have been passed that will require a more extensive use of biometric technologies in the federal government.

Last year, 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 use of biometrics in the federal government, and the current state of the technology.

What GAO Found

Biometric technologies are available today that can be used in security systems to help protect assets. 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, iris recognition, retina recognition, signature recognition, and speaker recognition. Biometric technologies have been used in federal applications such as access control, criminal identification, and border 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. Weaknesses in any of these areas diminishes 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. Similarly, errors sometimes occur during matching operations. Procedures need to be developed to handle these situations. Exception processing that is not as good as biometric-based primary processing could also be exploited as a security hole.

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. As federal agencies consider the development of security systems with biometrics, they need to define what the high-level goals of this system will be and develop the concept of operations that will embody the people, process, and technologies required to achieve these goals. With these answers, the proper role of biometric technologies in security can be determined. If these details are not resolved, the estimated cost and performance of the resulting system will be at risk.

www.gao.gov/cgi-bin/getrpt?GAO-03-1137T.

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.