

COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL
RELATIONS AND THE CENSUS
CONGRESSMAN ADAM PUTNAM, CHAIRMAN



OVERSIGHT HEARING
STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic: “*Advancements in Smart Card and Biometric Technology.*”

Tuesday, September 9, 2003
10:00 a.m.
Room 2154 Rayburn House Office Building

OPENING STATEMENT

Securing government buildings and computer systems is a task which has grown in both importance and challenge over the past number of years. Recognizing this, Federal agencies, working with the General Services Administration, have begun testing advanced identification technology that will better authenticate the identity of those requiring access to and interaction with the Federal government.

Specifically, agencies are examining the use of smart cards, which offer a number of benefits to Federal agencies including identity authentication of cardholders, increased security over buildings, safeguarding computers and data, and conducting financial and non-financial transactions more accurately and efficiently. In fact, some agencies, such as the Department of Defense, have already issued smart cards. The DoD’s Common Access Card, CAC, enables physical access to buildings, installations, and controlled spaces. It also permits access into DoD’s computer networks. The CAC provides DoD the information security and assurance necessary to protect vital information resources.

A number of other agencies across the Federal government are still exploring the possibilities of smart card use. And while some progress has been made, a recent report released by GAO outlines some areas of concern that need to be addressed in order for agencies to move forward in implementing the use of smart cards. As is too often the case, agencies have been unable to sustain an executive level commitment to this project, according to findings by GAO. If these kinds of initiatives fail to be a priority with the leadership of an agency, it is difficult to imagine that adequate resources will be allocated for their implementation.

Some additional noted challenges to progress include: recognizing and understanding resource requirements, integrating physical and IT security practices, focusing on achieving interoperability among smart

card systems, maintaining the ongoing security of smart card systems, and protecting the privacy of personal information. These are just a few of the issues agencies will need to address as they move forward.

There are other advanced and emerging technologies that have the potential to offer additional assurance to the identity authentication process. Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometry is being explored, developed and even utilized by some agencies today, including the FBI, at our borders and by state government's in detecting fraud and abuse of government benefits through identity verification. Biometric authentication may also be used with smart card technology. For instance, some smart cards have the capability of holding a biometric identifier, such as a fingerprint. This holds the potential to increase the accuracy of the identity authentication process. These possibilities, as well as the limitations and challenges presented by this technology, should be explored further.

As agencies proceed to explore the use of these advanced identity authentication technologies, government cannot neglect the importance people and process will continue to play in providing a secure environment. Regardless of how well these technologies work on behalf of the Federal government in authentication and identity management, technology has its limitations. Without the people and process in place to make it work we will have wasted a lot of money as well as provided a false sense of security.

I am hopeful that as the Office of Management and Budget, working with GSA and the National Institute of Standards and Technology go forward in setting some guidance for agencies, concrete progress in the actual implementation of smart card technology across Federal agencies will be demonstrated in the near future.