COMMITTEE ON APPROPRIATIONS

David Price (D-NC), Chairman, Subcommittee on Homeland Security

FOR RELEASE UPON DELIVERY
Thursday, March 19, 2009

Media Contact: Phil Feagan
202-225-1784

OPENING STATEMENT OF CHAIRMAN DAVID PRICE

Biometrics and Identity Management
March 19, 2009 / 10:00 am

Recognizing and authenticating a person's identity is part of daily life in business and in government. Recording a person's physical features to authenticate their identity has been done for millennia, beginning with use of fingerprints in ancient Assyria. This recording has evolved in modern times to the high technology of biometrics – automating collection, management, and authentication of data about personal physical characteristics – and storing that information in databases that can be used to identify people. Supporters of these practices see them as a solution to identity security challenges; critics view them as a threat to individual privacy.

Our governments use identity databases in several ways. US-VISIT relies on IDENT, one of the largest identity databases in the world, to track foreign individuals as they deal with our immigration services. We have watchlists that identify people for special screening at airports, or bar people from flying altogether. Several of these databases are outside of DHS, including the Consolidated Consular Database system at the State Department and the interstate data-sharing network we have required states to establish for their drivers' license files under REAL ID. Effective use of these databases to confirm or discover personal identities is critical

in maintaining our national security, but there are many signs that we are not where we need to be.

For example, on March 16th GAO released a report that showed fundamental vulnerabilities in the way our government issues passports. A single investigator obtained four U.S. passports using fraudulent identity documents and was able to travel on those identities. While weaknesses identified in the report are in the State Department and Postal Service, not DHS, it proves we need to build vigilance into our system to catch bogus documents, and that watch lists and databases must be constantly scrubbed for accuracy. Inclusion of biometrics can be a part of this solution, but just bolting it to our current system and practices will no more solve this problem than re-roofing a house will solve a termite problem.

Since the 9/11 attacks, the federal government has intensified the use of biometrics in databases to identify terrorists or other individuals of concern. We have also used this practice to confirm the rights and privileges of those who pose no security risk or who may be entitled to special credentials. The Department of Homeland Security has a principal role in collecting and managing biometric and biographic information on millions of foreign nationals, residents, and citizens in programs used for border and travel security, counterterrorism, immigration control, law enforcement, and infrastructure protection.

DHS incorporates biometrics in a variety of identification documents, particularly for immigration. DHS has at least nine other systems or databases that collect and maintain biometric and biographic records, and links to at least five others in other Departments. Identification data is collected for “trusted traveler” and “safe shipper” programs, to credential transportation workers, and for critical infrastructure protection.

Such broadened use of biometrics may seem justified in the post-9/11 world, but that begs the questions we expect to discuss today. How is the Department using biometric technology today, and how can we best use it to secure the homeland while protecting individual privacy rights? Under this theme, how is DHS working with other agencies to develop standards for biometric and contextual data and to coordinate the collection, management, sharing and control of such records? Why are there so many different databases? What is DHS doing to ensure the use of biometric technology improves security, law enforcement, or program effectiveness, with a minimum duplication of effort? Lastly, how does DHS protect personal information in its custody, and keep this powerful tool from being abused?

The most prominent DHS biometric program is US-VISIT, which collects and verifies fingerprint and facial images for almost all non-US travelers entering this country, and in theory, will someday do the same for their departure. US-VISIT has evolved into a provider of "identity management services" for U.S. Immigration and Customs Enforcement, Coast Guard, and U.S. Citizenship and Immigration Services, as well as other U.S. government agencies. In that role, it is working to link its records to those of the Departments of Justice and State, and is developing information sharing agreements with the Department of Defense. We expect to hear today how US-VISIT is undertaking its mission as custodian for one of the world's largest databases of biometric information. We also expect to hear about plans for the air traveler exit tracking pilots mandated in the fiscal 2009 appropriations, as well as any plans for a comprehensive exit strategy.

Clearly, widespread use of biometric technologies to confirm or discover people's identities is here to stay. It is critical, then, that we understand the full range of policy implications, management challenges, and funding issues such programs entail.

We welcome today for the first time before this Subcommittee Kathleen Kraninger, the Deputy Assistant Secretary for Screening, and welcome back Mr. Robert Mocny, the Director of US-VISIT. Your written statements will be entered in the record, and I ask that you provide brief oral statements. Before you begin, let me turn to my distinguished Ranking Member, Mr. Rogers, for his comments.

# # #