Stateline.org
Politics & policy news, state by state

Monday, December 20, 2004

Drivers' licenses now a tool for homeland security

By Kathleen Hunter, Stateline.org

Look closely at Massachusetts' new driver's license and you'll notice an outline of the state. Hold it at a slightly different angle, and instead you'll see the word "Massachusetts."

The changing image, known as a Kinegram, is one of several security features the Bay State recently added to its drivers' licenses. It acted shortly before Congress called for the first federal standards on drivers' licenses and other state-issued identification cards.

State officials hope Massachusetts and other states ahead of the curve in making their drivers' licenses more secure will serve as models for a new federal rule-making committee on drivers' licenses mandated by Congress. The drive to beef up security of drivers' licenses nationwide was signed into law Dec. 17 by President Bush as part of a massive overhaul of U.S. intelligence processes to try to prevent a repeat of the Sept. 11, 2001, terrorist attacks .

The new federal law has some state officials upset because, up to now, it has been strictly a state's business how it issues and designs the drivers' cards commonly used as identification nationwide.

"Our concern is that federal standards will stifle innovation because states are doing things differently from each other," said Cheye Calvo, who handles federal-state issues for the National Conference of State Legislatures. "But all states are advancing the ball in terms of security.... To try and impose a one-size-fits-all approach, I think, is short-sighted."

The Kinegram on Massachusetts' new cards features several additional layers of images and code designed to make tampering obvious and to make the cards nearly impossible to replicate.

"Bar none, this is the most tamper-resistant license in America," Massachusetts Transportation Secretary Daniel Grabauskas bragged in a press release.

Massachusetts is the first to use the state-of-the-art technology on drivers' licenses but isn't alone in revamping its licensing procedures. Since the 2001 terrorist attacks, in which four of the 19 hijackers used valid state-issued drivers' licenses to board the airplanes they later crashed, drivers' licenses have been viewed as a homeland-security tool and not just a way to regulate who's allowed on the nation's roadways.

A number of states have been adopting innovations – both in the physical appearance of the licenses and in how they're issued – and could provide ideas for the federal rule-making panel.

In Colorado, state officials are employing facial recognition technology that uses a digital photograph to take measurements of an applicant's facial features. The data is fed into a computer and compared to photographs already on file to determine whether the applicant already has a Colorado license under another name. The process has netted an average of 20 duplicate applicants a month.

Colorado also is among a small but growing number of states that have outfitted their licenses with digital watermarks, coded data invisible to the naked eye that can be read by an electronic scanner to determine whether the license is valid.

In Florida, Department of Motor Vehicles officials use new auditing processes to ensure that licensing data and materials are secure from the time an applicant steps into a Department of Motor Vehicles office until a finished license is placed in his hands.

At least 13 states now use some form of biometric – or body measurement – technology to verify the identity of those renewing or replacing drivers' licenses, according to NCSL.

Biometrics software takes photographs or scans facial features, retinas or fingerprints and quantifies that information into mathematical algorithms. Facial biometrics quantify the distances between major points such as the eyes, nose or temples, and fingerprint biometrics quantify the distances between points on the hand. Scans of the thumb or other physical features can be crosschecked with existing databases to verify identity.

California, Colorado, Connecticut, Georgia, Hawaii, Illinois, Oklahoma, Nebraska, New Jersey, Oklahoma, Nebraska, New Jersey, South Carolina, Texas, West Virginia and Washington now use biometric technology.

Technological improvements, including biometrics, Kinegrams and digital watermarks, already have made drivers' licenses much more difficult to counterfeit, said Reed Stager, a vice president for Digimarc Corp., an Oregon-based company that supplies licenses to 32 states.

"It isn't as simple as switching out a photograph anymore," Stager said.

Virginia recently formed a legislative panel to consider whether to embed computer chips in drivers' licenses with information such as height, weight, age and Social Security number that normally appears on the license. Starting in 2005, all U.S. passports will contain similar computer chips.

Besides focusing on the physical appearance of drivers' licenses, many states also have sought to improve the processes by which they issue licenses and other identification documents. A number of states have enacted stricter requirements for documents such as birth certificates and Social Security cards that are used to obtain, renew or replace a driver's license.

The new federal intelligence law also creates national standards for state-issued birth certificates.

The Coalition for a Secure Driver's License, a nonprofit organization formed in the wake of the terrorist attacks, recently analyzed states' licensing requirements. It found the most secure licensing processes in 17 states (Arizona, Florida, Iowa, Kentucky, Maryland, Minnesota, Mississippi, Nevada, New Jersey, New York, Ohio, Pennsylvania, South Carolina, South Dakota, Virginia, West Virginia and Wyoming).

The study considered whether a state requires applicants to prove legal presence, whether drivers' licenses automatically expire with an applicant's visa and whether the state accepts "insecure" documents, such as birth certificates from other countries.

New York, for example, uses the Internet to verify applicants' information and denies licenses to those who submit false information.

Hawaii, Illinois, Michigan, Montana, New Mexico, North Carolina, Oregon, Tennessee, Utah, Vermont, Washington and Wisconsin were listed as having the most lax requirements.

The new intelligence law specifies that each driver's license include a digital photograph, full name, date of birth, gender, and drivers' license or personal identification number, but leaves other issues to the committee. States also will be required to meet stiffer standards for the documents they can accept as proof of identity, for verification of those documents and for processes of issuing licenses.

If a state's license does not meet the standards in two years, federal agencies will not be allowed accept it as valid identification.

Send your comments on this story to letters@stateline.org. Selected reader feedback will be posted in our Letters to the editor section.

Contact Kathleen Hunter at khunter@stateline.org.