washingtonpost.com

Transit-Worker ID Program Stalled

Years of Trouble in National Effort Bodes Ill for High-Tech
Licenses, Passports

By Spencer S. Hsu

Washington Post Staff Writer

Sunday, September 17, 2006; A03

A Bush administration initiative to secure the nation's ports
is bogged down in industry opposition, technology flaws
and evidence that it fails to safeguard workers' privacy,
according to industry and government analysts.

The rocky launch of the Transportation Worker Identification Credential threatens to delay what Homeland
Security Secretary Michael Chertoff declared his highest priority after the Dubai port controversy in February:
starting by year's end to screen the backgrounds of 750,000 U.S. workers at critical sea, air and land
transportation facilities, and issuing them microchip-equipped ID cards.

More broadly, the long-overdue ID program foreshadows concerns that hundreds of millions of Americans
soon may encounter as the government starts issuing similarly equipped driver's licenses, passports,
federal-worker badges and immigrant-guest-worker cards in coming years.

"It's discouraging to see how really difficult it is to implement this sort of thing," said Doris Meissner, a
former commissioner of the U.S. Immigration and Naturalization Service who tracks identification measures
as a senior fellow at the Migration Policy Institute.

"And it's probably going to get more complicated before it gets simpler," she added.

The transportation credential, one of the first security measures initiated after the Sept. 11, 2001, terrorist
attacks, was envisioned as a model for new, "smart" ID cards. But a familiar list of hurdles has tripped up the
program, including poor administration, indifferent oversight by Congress, insufficient funding, technological
glitches and resistance from the private sector, said industry and government officials.

President Bush signed the worker-ID program into law in November 2002 as part of broader maritime
security legislation. It called for vetting workers at more than 300 ports and 3,700 cargo and passenger
terminals using technology that incorporates fingerprints, iris scans or digital photographs.

The program would streamline checks of criminal-background files, terrorist watch lists and immigration
status for truckers, stevedores, rail and airport terminal employees, and other transit workers, among others.
The new "biometric" data would make it virtually impossible for anyone other than the cardholder to use the
ID.

Department of Homeland Security officials initially told port operators that they expected to start issuing
credit-card-size ID cards to transportation workers by the end of 2003.

Then the troubles began.

Management turnover and indecision delayed prototype testing until late 2004. Instead of the 200,000 cards planned for the pilot program, only 4,000 were issued, even as the cost rose from $12 million to $23 million.

Rep. Harold Rogers (R-Ky.), chairman of the House Appropriations subcommittee that oversees the department, insisted that the TSA adopt technology currently used for U.S. "green cards," which are produced in his district. The TSA paused to complete a study concluding that its alternative to the green-card technology was superior. Prototype card production was delayed again in 2005 so it could be moved to the Kentucky plant.

It took an election-year political furor over the attempt by a Dubai company to take over operations at six U.S. seaports to jump-start the project. Faced with a reminder of how little has been done to secure facilities from infiltration by potential terrorists, lawmakers called the administration's bungling of the transportation-worker IDs the Achilles' heel of the nation's port security.

But when Homeland Security officials rushed out long-delayed rules in May, labor and the nation's port operators, truckers, barge companies and tugboat companies revolted.

Industry groups and technology providers warned that complex systems for personal identification numbers and card reading could be prone to time-consuming breakdowns in saltwater environments on boats and docks. Marine executives said requiring new workers to wait as long as 60 days to clear security checks would cripple small and seasonal operators that already face worker shortages. Unions warned that without strict limits and an appeals process, workers could be denied jobs because of mistaken identity or past offenses unrelated to terrorism.

"It just doesn't make any sense given the real-world operations of the tugboat industry," said Thomas A. Allegretti, president of American Waterways Operators, which represents 500 tug and barge firms.

In July, the Homeland Security inspector general reported that hundreds of critical security vulnerabilities in proposed cards, card readers and other parts of the system posed unacceptable risks of the theft of sensitive data. Other problems include evolving federal technology standards and a projected cost to industry and workers of $2 billion to $3 billion.

Officials said these concerns are a preview of what could happen on a much larger scale with the broader government use of "smart" cards.

"You have to have a single way of identifying people as who they are that is authentic, that maintains their confidentiality and that is secure," said David Heyman, director of the homeland security program at the Center for Strategic and International Studies.

Experts caution that Americans may not want to submit their fingerprints and eye and facial scans to the government. Privacy advocates want to know who will be in charge of keeping and discarding sensitive personal information, and how that data will be kept secure.

They are concerned about the types of government databases that would be linked to such ID records and who would see them. And even if there is consensus on the security needs, others are skeptical that the technology can be implemented without creating bottlenecks and backlogs.

"There's this idea that an ID card or ID credential is this kind of panacea," said Lee Tien, senior staff attorney for the Electronic Frontier Foundation. "But they are difficult to design and implement . . . and what we're seeing is every attempt to do so is fraught with serious, serious problems."

The questions are not hypothetical. By year's end, Homeland Security is expected to roll out national

standards for driver's licenses, which would affect 200 million Americans when the rules take effect by May 2008. The change was mandated by the Real ID Act, which was enacted to make it more difficult for criminals and potential terrorists to obtain driver's licenses.

Last month, the State Department began small-scale production of the first microchip-equipped "e-passports" that over the next 11 years will replace all 60 million U.S.-issued passports and could be upgraded to include fingerprints or other biometric data.

Up to 4 million federal workers and contractors are to be next, receiving new IDs over two years starting in October. Then will come cards allowing tens of millions of residents of the United States, Canada, Mexico and many Caribbean nations to cross each other's borders without a passport. And the White House has proposed issuing similar tamper-proof biometric cards to 2 million guest workers under its contested immigration overhaul.

Analysts cite clear lessons from the transportation-worker ID program's struggles as warnings for programs such as Real ID, which they say will have to be delayed given its far greater size, cost and complexity.

As for the Transportation Worker Identification Credential program, Homeland Security announced last month that after missing a July deadline, it will postpone the installation of card readers. Critics say that for now the department has simply created a $150-per-worker photo ID. The Senate on Thursday passed port-security legislation that would force the department to ease requirements for certain short-term workers and issue rules for card readers by Dec. 31, start more test programs and report back in 2008.

"It's clear the department seems unable to complete the task and control access to our ports, which is a fundamental aspect of security," said Sen. Susan M. Collins (R-Maine), chairman of the Senate homeland security committee and co-sponsor of the bill.

Chertoff maintained that conducting background checks and issuing conventional ID cards are progress. "The fact that we may not have the full-blown perfect system doesn't mean we can't take a big step forward," he said earlier this month.

In a Sept. 8 speech, he went further, blaming the lack of progress on unnamed critics who object to tamper-resistant IDs as too burdensome or expensive, or say they amount to a national ID card.

"That kind of backsliding runs directly contrary to the lessons of 9/11," Chertoff said, noting that nearly all the Sept. 11 hijackers had obtained IDs, in some cases through fraud. He contended that a secure ID system would have prevented the attacks. "If we'd had it five years ago, there would not have been a 9/11," Chertoff said.