

**Statement of Chairman John L. Mica**  
**Committee on Transportation & Infrastructure Committee**  
**U.S. House of Representatives**  
**to the**  
**Committee on Commerce, Science and Transportation**  
**United States Senate**  
**on**  
**the Transportation Worker Identification Credential Program**  
**March 10, 2011**

---

Mr. Chairman, Ranking Member Hutchinson, and Members of the Committee, thank you for the opportunity to testify before you today on the progress, or lack thereof, of the Transportation Worker Identification Credential – or “TWIC” – Program. It is a privilege to appear before you, and I thank you for your continued and vigilant oversight on this important issue.

As you may know, I am one of the co-requestors of the Government Accountability Office (GAO) report that I believe this Committee will release today on the weaknesses of the TWIC Program. As Chairman of the Transportation & Infrastructure Committee in the House of Representatives, I can attest that the Members of my Committee are committed to ensuring the security of the transportation workers and transportation infrastructure they oversee as part of their role on the Committee. As an original author of the legislation that created the Transportation Security Administration (TSA) after 9/11, I also feel a personal sense of obligation to ensure that this important piece of our Nation’s defense apparatus is operating as the efficient and effective security agency it was intended to be.

**Government Coordination on Transportation Security**

In the wake of 9/11, the Federal government realized how disastrous storing information in government silos could be. Information-sharing became a top priority and the Administration directed departments and agencies to work together to ensure all relevant information is on the table at all times. During this time, the TSA was transferred from the Department of Transportation (DOT) to the newly-created Department of Homeland (DHS).

Homeland Security Presidential Directive-7 directed DHS and DOT to “collaborate on all matters relating to transportation security and transportation infrastructure protection.<sup>1</sup>” In 2004, the two Departments entered into a Memorandum of Understanding and jointly expressed a desire for a “strong partnership in order to reduce the vulnerability of transportation passengers, employees, and systems to terrorism and other disruptions.<sup>2</sup>” Each department would have regulatory responsibilities in the area of transportation security, and would communicate and cooperate on funding for transportation security projects.

As evidence of this partnership, TSA officials have appeared before the Transportation and Infrastructure Committee more than a dozen times since the agency was transferred to DHS at the end of 2002. In January of 2008, former-TWIC Program Director Maurine Fanguy provided an update to the Committee on the TWIC Program.

So you will understand my surprise when TSA Administrator Pistole and TWIC Program Manager John Schwartz declined an invitation to testify before the Transportation Committee on the same issue in April of this year.

I don’t understand what has changed, but I do want to impart to Administrator Pistole, who I understand is testifying on the next panel, that it is imperative that jurisdictional issues not interfere with progress, particularly when money is being poured into flawed security programs. As evidenced by my appearance before this Committee today, Congress does indeed want to work together on these important issues and it is not the role of any government agency to interpret jurisdictional boundaries of Congressional Committees.

### **Transportation Worker Identification Credential (TWIC) Program**

With that said, I did come here today to discuss the TWIC Program. According to TSA, 1.86

---

<sup>1</sup> “Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection,” The White House. December 17, 2003.

<sup>2</sup> “Memorandum of Understanding between the Department of Homeland Security and the Department of Transportation on Roles and Responsibilities.” September 28, 2004.

million people have enrolled, 1.72 million cards have been activated<sup>3</sup>, and \$420 million has been provided to the TWIC Program. In 2007, DHS estimated that the combined cost to the Federal government and the private sector may reach \$3.2 billion over a ten-year period – not taking into account the full cost of “implementing and operating readers.”

TWIC is turning into a dangerous and expensive experiment in security. Nearly half-a-billion dollars have been spent since the Maritime Transportation Security Act of 2002 directed the Secretary of DHS to issue biometric transportation security cards to maritime workers. Yet today, ten years later, TWIC cards are no more useful than library cards. In fact, the only port that GAO investigators were NOT able to gain access to using fraudulent means was the port that still required port-specific identification for admittance to secure areas.

We have also learned from GAO that:

1. Individuals can obtain authentic TWICs using fraudulent identification documentation;
2. Individuals can gain access to ports using counterfeit TWICs; and that, among other things,
3. TSA is unable to confirm that TWIC holders maintain their eligibility throughout the life of their TWIC.

This is a troubling scenario and counterintuitive to the purpose of the program. GAO determined that an individual does not have to prove who they say they are when enrolling in the program. In other words, an individual can present a fraudulent identification document with somebody else’s name, but provide their own fingerprints to obtain an authentic TWIC card. In this instance, the TWIC card transforms into a biometric key that unlocks our Nation’s ports and facilities for any individual with the intent and desire to do us harm.

GAO tells us that DHS has not assessed whether or not the TWIC program enhances security or not. In fact, DHS cannot demonstrate that TWIC – as implemented and planned – is more effective than the approach used to secure ports and facilities before 9/11.

---

<sup>3</sup> “Transportation Worker Identification Credential (TWIC) Program Briefing” to the House Committee on Oversight and Government Reform, Transportation Security Administration. May 2, 2011.

I believe we must begin to ask if these vulnerabilities in fact make our nation less secure.

### **TSA Needs to Conduct Cost-Benefit and Risk Analyses of Programs Prior to Funding**

The root of this problem is evidenced in many other TSA programs as well— this fledgling agency still does not conduct risk assessments and cost-benefit analyses of its security programs as required by law.

TSA’s Screening People by Observation Techniques – or “SPOT” – program, will require \$1.2 billion over the next five years, but TSA has yet to validate the underlying methodology of the program or to conduct a cost-benefit analysis.<sup>4</sup>

Likewise, GAO found in April of last year that TSA has not conducted comprehensive risk assessments across the surface transportation sector.<sup>5</sup> This lack of analysis results in ill-informed resource allocations and more importantly calls into question whether the highest risk targets are being secured. In light of the plot against the U.S. rail sector uncovered in the Bin Laden raid, it is alarming that TSA still has not addressed recommendations to close these gaps.

### **Biometric Pilot Licenses**

TSA is not the only agency that has struggled to develop a biometric credential for transportation workers. In April the Federal Aviation Administration (FAA) testified before my Committee on the long delayed development of biometric pilot license. Although Congress mandated that pilot licenses include biometric identifiers in the Intelligence Reform and Terrorism Prevention Act of 2004, FAA has yet to produce them. FAA recently spent \$2.7 million to issue 700,000 pilot licenses that complied with one requirement of the 2004 legislation – they are now plastic instead of paper and therefore tamper-resistant. Unfortunately, the requirements to include a photograph and biometric identifiers were not taken into consideration.

---

<sup>4</sup> “Efforts to Validate TSA’s Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges.” U.S. Government Accountability Office, May 2010.

<sup>5</sup> “Surface Transportation Security: TSA Has Taken Actions to Manage Risk, Improve Coordination, and Measure Performance, but Additional Actions Would Enhance It’s Efforts.” U.S. Government Accountability Office, April 2010.

In closed door sessions with my Committee, FAA informed Members that they believed TSA was going to produce a biometric standard for them, perhaps in the form of a TWIC card.

Given the testimony that you will hear today, and the results of this GAO report, I think it is safe to say that roping additional transportation workers into the TWIC Program is an idea destined for disaster. While the biometric standard for the TWIC Program, developed by the National Institute of Standard and Technology (NIST), works well and fulfilled a much-needed mandate, the program itself is poorly managed.

NIST's Director of Information Technology recently informed me that the agency is in the process of updating the current biometric standard to include iris scanning, an effort which I applaud. I understand that this standard will be complete by the end of this year and look forward to its inclusion in future personal identify verification cards for the Federal workforce.

I want to thank the Committee again for the opportunity to testify before you today, and for your important work on the issue of secure credentials for transportation workers.