S. HRG. 112–164

ARE OUR NATION'S PORTS SECURE? EXAMINING THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL PROGRAM

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 10, 2011

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

71–433 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii	KAY BAILEY HUTCHISON, Texas, *Ranking*
JOHN F. KERRY, Massachusetts	OLYMPIA J. SNOWE, Maine
BARBARA BOXER, California	JIM DEMINT, South Carolina
BILL NELSON, Florida	JOHN THUNE, South Dakota
MARIA CANTWELL, Washington	ROGER F. WICKER, Mississippi
FRANK R. LAUTENBERG, New Jersey	JOHNNY ISAKSON, Georgia
MARK PRYOR, Arkansas	ROY BLUNT, Missouri
CLAIRE MCCASKILL, Missouri	JOHN BOOZMAN, Arkansas
AMY KLOBUCHAR, Minnesota	PATRICK J. TOOMEY, Pennsylvania
TOM UDALL, New Mexico	MARCO RUBIO, Florida
MARK WARNER, Virginia	KELLY AYOTTE, New Hampshire
MARK BEGICH, Alaska	

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
BRIAN M. HENDRICKS, *Republican Staff Director and General Counsel*
TODD BERTOSON, *Republican Deputy Staff Director*
REBECCA SEIDEL, *Republican Chief Counsel*

CONTENTS

WITNESSES

APPENDIX

ARE OUR NATION'S PORTS SECURE? EXAMINING THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL PROGRAM

TUESDAY, MAY 10, 2011

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The committee met, pursuant to notice, at 2:30 p.m. in room SR–253, Russell Senate Office Building, Hon. Frank R. Lautenberg, presiding.

OPENING STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. I'm pleased to open this hearing of the Committee on Commerce, Science, and Transportation. We've got important subjects at hand here.

And we are pleased to see our colleague from the House of Representatives, The Honorable John Mica, who is the Chairman of the Committee of Jurisdiction on the House side.

And, Mr. Mica, we welcome you. And we ask you to give your testimony. It's customary to have a 5-minute period for presentation, but if there is a need to extend it, please don't be unwilling to ask for it. And we'll start the clock, please, at the 5-minute level.

Thank you.

And, Mr. Mica, the table—the microphone is yours, sir.

STATEMENT OF HON. JOHN L. MICA, CHAIRMAN, COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE, U.S. HOUSE OF REPRESENTATIVES

Mr. MICA. Well, thank you. And I'm pleased to be on the Senate side this afternoon, and also to work jointly with your committee.

And actually, I'm here today because I think the subject before you is—well, the title is, "Are Our Nation's Ports Secure? Examining the Transportation Worker Identification Credential Program." And I think also you're going to focus on a GAO report that I had the opportunity to be a co-requester with members of this important Senate committee. So, I will try to talk about both the GAO report and also the issue at hand of credentialing our transportation workers.

I've submitted a full statement for the record, and I'll just give some comments here.

As you know, Mr. Chairman and other members, for nearly a decade now the federal government has struggled to produce a

transportation worker identification credential. We've tried to produce a credential for airport and transportation workers. We've attempted to produce a pilot's license. And we've also attempted to produce a frequent airline traveler identification card. After spending years and nearly half a billion dollars, we have, unfortunately, missed the mark. We've spent nearly half a billion dollars, and unfortunately, we do not have a TWIC card that provides secure identification, as you'll hear from GAO today, and also that your committee staff has revealed in their report.

I read your committee report. Being a former Senate staffer, I want to thank them. They did some excellent work. The report—the key findings are summarized very clearly—it says, "GAO investigators were able to access secure facilities"—this is using TWIC cards or fraudulent cards—they "were able to access secure facilities at U.S. ports during covert tests in which they presented either counterfeit TWIC cards, authentic TWIC cards obtained through fraudulent means, or falsified reasons for requesting access to the security." Then they also summarized and said, the—"DHS has not adequately assessed the effectiveness of the TWIC Program, nor has DHS demonstrated that the current TWIC Program enhances port and facility security better than what we've had in the past."

One other key finding is the GAO—in the GAO report, that you cite in your report, is that TSA does not have clear criteria for applying discretionary authority to applicants who have past criminal convictions.

These are just the highlights of some of the findings, not that I came up with, but that your staff recited from the GAO report.

As Chair of the House Aviation Subcommittee, I helped to launch—work with many members on this side—the Transportation Security Administration, some years ago, in 2001. Even in that first measure, Congress recognized and requested development of a secure ID for transportation workers. In 2004, I helped pass legislation to require the FAA to replace a paper pilot identification card. And we put in the law that we required a durable, biometrically-enabled license that also had a photograph of the pilot on the—this durable new identification license.

After spending billions—I'm sorry—after—I get used to billions today—but, after spending millions, FAA produced a license that was durable. However, it didn't have a biometric means. And I know there'll be a call today for having some unification of these different licenses and IDs, and what components they'd have. But, they finally produced, again, a card, at millions of dollars, that does not have a biometric measure and code—and coding capability. And the only pilots that appear on the document, on the license, are Wilbur and Orville Wright. I don't know if you've seen this, but this is—turn the—show them Wilbur and Orville Wright, there. So, there's—we spent millions of dollars, we produced this license, and it actually is not acceptable with TSA, as an ID. It doesn't have a—even a photo of the pilot on it.

When you talk to FAA about this, they point to Homeland Security, and then they point to TSA, for trying to get directions.

So, after spending hundreds of millions of dollars on a TWIC card, now we find, this report says, that it can easily fraudulently be used.

We still lack deployment of readers. We've issued about 1.7 million of these cards, but we don't have a reader. The TWIC card does have biometric measures for fingerprint. Iris is on its way, we're told. It has a photo. But, we don't have a reader capable of confirming the identification of the person using the card, and knowing that, in fact, is the same person that's on the ID, or carrying the ID.

With—right now, the U.S. House and also your help in the Senate—and this is a very important hearing because I'm hoping this will help prod the agencies to soon have a TWIC card with full biometric fingerprint and iris capability, and also readers capable of a reliable confirmation. However, even with that equipment and with that new capability, it will not address some of the fraudulent issues that are uncovered by GAO.

So, I'm pleased to come——

Senator LAUTENBERG. Mr. Mica, we will put your full statement into the record. I made a slight error when I invited you to go first without making my own statement. So, we listen with interest, have heard your public comments about how you saw things, in your testimony, here today. So, I am going to make my statement. And if you need a minute more, I'm happy to give it to you.

Mr. MICA. Thank you. I'd like to hear your statement. Thank you.

[The prepared statement of Mr. Mica follows:]

PREPARED STATEMENT OF HON. JOHN L. MICA, CHAIRMAN, COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE, U.S. HOUSE OF REPRESENTATIVES

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 and 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."[1] 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

[1] "Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection," The White House. December 17, 2003.

and other disruptions."[2] 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 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 million people have enrolled, 1.72 million cards have been activated,[3] 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, 10 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.

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.

---

[2] "Memorandum of Understanding between the Department of Homeland Security and the Department of Transportation on Roles and Responsibilities." September 28, 2004.

[3] "Transportation Worker Identification Credential (TWIC) Program Briefing" to the House Committee on Oversight and Government Reform, Transportation Security Administration. May 2, 2011.

TSA's Screening People by Observation Techniques—or "SPOT"—program, will require $1.2 billion over the next 5 years, but TSA has yet to validate the underlying methodology of the program or to conduct a cost-benefit analysis.[4]

Likewise, GAO found in April of last year that TSA has not conducted comprehensive risk assessments across the surface transportation sector.[5] 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.

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 (NISI), 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.

Senator LAUTENBERG. Thanks very much. And again, welcome.

And I'm pleased to have a chance to have this committee hearing. We have serious concerns about the government's record, and efforts to make America's ports more secure. Our maritime facilities are global gateways, and they provide American businesses and consumers access to the world marketplace. The ports are a vital part of our economy, but they've also been identified as special targets for terrorist attacks.

Now, my state is home to—as said by the FBI—to the country's most at-risk areas for a terrorist attack, a stretch that includes major hubs like the Port of New York and New Jersey, which handled more than $140 million in cargo last year.

Now, to improve security at our ports, 9 years ago the government created a worker identification program, known as TWIC, to try to make sure that access to the nation's ports is limited to people who belong there, such as dock workers and cargo handlers and other professionals. Now, after several delays, the program is now, as you said, up and running, and the government has issued almost 2 million TWIC cards.

---

[4] "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.

[5] "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.

But, a recent Government Accountability Office investigation raises a disturbing question. Are America's ports actually safer now than they were a decade ago? The GAO has identified serious problems with TWIC, including startling evidence that this program might actually diminish the safety of our ports.

At this committee's request, the GAO conducted covert testing. Investigators were able to fraudulently obtain TWIC cards and use the cards to access secure locations. Not only were they able to access the port facilities, but they were able to drive a vehicle with a simulated explosive into a secure area. Fraudulent and counterfeit cards, like the ones used by investigators, could also be used as identification at airports or military facilities.

The problems don't stop with fraudulent cards. There are also issues with criminal background checks, immigration checks, and the lack of safeguards to determine if an applicant even needs a TWIC card. So, despite these alarming findings, the Transportation Security Administration has, so far, been unable to close the gaping holes that plague this program.

Additionally, the Department of Homeland Security, which heads the TSA, has not yet conducted a review to determine if the card program helps or hinders security at our nation's ports. And given the critical importance of our ports, it's unacceptable that we're spending hundreds of millions of tax dollars on a program that might actually be making the ports less safe. So, according to estimates, it could cost as much as $3 billion to deploy the cards over a 10-year period. And this doesn't include the cost of the sophisticated biometric equipment that's needed to read the card. So, we've got to thoroughly examine and correct the TWIC Program, and make sure we're focusing our resources where they're needed most, the areas that present the highest risk.

So, I look forward, Mr. Mica, to hearing from you and our other witnesses about how you see the status of the program and how we can best implement changes to make sure our port security programs are effective and the money we spent—spend is improving at our ports.

Now, I've got Senators here that are waiting at a chance to make their statements. And if you want to add a ex post facto thing for just a couple of minutes, Mr. Mica, I'd be——

Mr. MICA. Sure, I'm here, waiting. Love to hear the other Senators, too. Thank you, sir.

Senator LAUTENBERG. Thank you. In the order of their appearance, Senator Ayotte is here. And we're pleased to see you, and invite you to give your statement, please.

STATEMENT OF HON. KELLY AYOTTE,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator AYOTTE. Thank you, Mr. Chairman.

Thank you, Representative Mica. Thank you so much for coming over to testify from the House.

Security at our nation's ports is critically important to our safety and to our economy. Not only would an attack on our nation's ports be devastating, in terms of the loss of human life, but would also severely impact our national economy.

It is deeply troubling that the GAO investigators were able to access secure facilities at U.S. ports during covert tests by presenting counterfeit or fraudulent TWIC cards. This represents a significant hole in our national security that must be addressed. And we certainly don't want a security program in place that gives the appearance of making us more secure, but in reality does not, because that can cause people to actually act less vigilantly than they should, given the situation.

I look forward to discussing the reasons behind why this was able to happen, ways we can prevent this from happening in the future, and how this program can be corrected to ensure the security of our ports. I also wanted to raise the issue that transportation workers who are getting these IDs—they also are pretty inconvenienced, in terms of having to make two trips to a TWIC enrollment center to obtain their TWIC card, which can be time-consuming and expensive for, particularly, workers in rural areas that don't live close to an enrollment center, which can place an additional financial burden, particularly on a program which we have questions about the efficacy of it. I'm also interested in discussing ways that this burden could be alleviated so that workers don't have to make multiple, costly trips in order to receive the TWIC card, while, at the same time, ensuring the integrity of the card, which is very important.

As millions of TWICs are going to be coming up for renewal in 2012, now is the time for this committee to address this issue. And it's critical that we solve these problems right away.

And I look forward to your testimony today.

Thank you.

Senator LAUTENBERG. Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. I'm looking forward to hearing from the witnesses. Thank you, Mr. Chairman.

Senator LAUTENBERG. Senator Boozman.

STATEMENT OF HON. JOHN BOOZMAN,
U.S. SENATOR FROM ARKANSAS

Senator BOOZMAN. I think, in the interest of time, Mr. Chairman, I will put my statement in the record, with your permission.

[The prepared statement of Senator Boozman follows:]

PREPARED STATEMENT OF HON. JOHN BOOZMAN, U.S. SENATOR FROM ARKANSAS

Senator Lautenberg, thank you for presiding over this hearing today. The results of this GAO study are troubling, including the multiple breaches at facilities by investigators using fraudulent and/or counterfeit TWIC cards. Perhaps the only thing that is positive to see is that the Department of Homeland Security agrees with the recommendations.

I look forward to listening to your testimony today, and working with both DHS and the Coast Guard in the future to improve the TWIC program.

Senator LAUTENBERG. We're making haste here, Mr. Mica. We've got, if you want, a couple of minutes.

Mr. MICA. Thank you. I'll just conclude. And again, I associate myself with your remarks, and Senators that are here.

You're looking at TWIC, you're looking at problems we've uncovered. The last Senator who spoke indicated that, 2012, we'll be renewing these cards. I think it's incumbent on both the House and the Senate that we get our act together on these IDs. If we've spent a half a billion dollars. We don't have a reader. We're on the cusp of getting a second biometric measure. And we have transportation workers in other fields—aviation, for example—where I showed you a card that we have for a license, that can't be used for an ID, that doesn't meet the criteria that Congress intended. We can, and we must, do a better job of getting our whole act together.

Now, this, folks, too, is not rocket science. There are other agencies that already have identification cards. They have them with biometrics, both iris and thumb. They have them with readers that can confirm that that person is the person that has the ID and can be identified. So, we go on spending more and more money, and we don't have security at our ports, our airports, or other transportation facilities.

So, I'll work with you. I know you're going to hear from Mr. Pistole. He's fairly new at the gate. A lot of this didn't happen under his watch. But, we do need to work with him, with the administration, and others, to somehow call a halt to spending hundreds of millions of dollars and still, 10 years later, not having a secure ID.

Thank you. And I'm pleased to be here.

Senator LAUTENBERG. We appreciate your presence here.

Senator Begich, you've just come in. Can we proceed with the witnesses, or——

Senator BEGICH. Let me think about it, if you could, Mr. Chairman. I have lots of thoughts on my mind.

Senator LAUTENBERG. OK.

Senator BEGICH. No, go ahead.

[Laughter.]

Senator LAUTENBERG. All right. And I would call the second panel to the table: Mr. John Pistole, the Administrator of the Transportation Security Administration. You're not so new. And we're glad that you've brought your experience and leadership to the task. We'll hear from you on the administration's efforts to implement the card program. Rear Admiral Kevin Cook, Director of Prevention Policy for the United States Coast Guard, to testify on the Coast Guard's role in the TWIC Program. And Mr. Steve Lord, Director of Homeland Security and Justice for the GAO, the Government Accountability Office. And your testimony, I understand is going to be on the GAO's oversight and investigation of this program.

So, I thank all of you for coming today.

And, Mr. Pistole, please begin. We have 5 minutes for your testimony.

STATEMENT OF HON. JOHN S. PISTOLE, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. PISTOLE. Thank you, Chairman Lautenberg. And good afternoon, distinguished members of the Committee.

I appreciate the opportunity to testify today about Transportation Security Administration's work with the United States Coast

Guard on the Transportation Worker Identification Credential Program, or TWIC.

TWIC Program, of course, authorized by the Maritime Transportation Security Act of 2002, MTSA, and the SAFE Port Act, strengthens the security of our nation's port while facilitating trade through the provision of a tamper-resistant biometric credential to all port workers requiring unescorted access to secure areas of these MTSA-regulated port facilities and vessels.

The purpose of the TWIC Program is to provide a means of positively verifying the identify of those seeking access to secure areas, and to conduct Security Threat Assessments, or STAs, to determine their eligibility, and to deny access to unauthorized individuals.

Like all security procedures, use of TWIC cards help reduce or mitigate risk, but do not eliminate risk, as detailed in the GAO report. Not only do I agree with the findings and conclusions of the GAO report, and have taken initial steps to address the first two recommendations—the first three apply to TSA, particularly—but, I've asked GAO to follow up with a rigorous cost-benefit analysis of the entire TWIC Program, in conjunction with DHS, Coast Guard, and TSA. I believe this type of comprehensive assessment will help us all make judgments on how well we, the U.S. Government and industry, are buying down risk, and the best way forward with this program. In other words, what's our return on investment?

To date, TSA has vetted and ruled more than 1.8 million TWIC applicants. The majority of transportation workers who have no criminal history receive their TWIC within 5 to 10 calendar days of submitting an application. Applicants with criminal histories require a more stringent review, of course, and generally receive either their TWIC or notification of a potentially disqualifying offense within 30 calendar days of submitting an application.

Now, in accordance with the SAFE Port Act of 2006, a TWIC pilot is currently being conducted to evaluate the feasibility, as well as technical and operational impact, of implementing a transportation security card reader. Formal data collection from the pilots is expected to be completed in 3 weeks—the end of May. Thereafter, an independent test agent will develop individual participant reports for review by TSA and Coast Guard. And we also continue to analyze data already collected in the pilot. And we'll analyze new data as it is required. We have drafted a report required by section 104 of the SAFE Port Act, and will continue to make further updates to this report until its anticipated delivery to Congress this summer. These reports, along with direct feedback from the participants, will inform decisions regarding Coast Guard's rulemaking that will establish TWIC-reader use requirements.

I don't believe this testimony would be complete without mention of TSA's efforts to harmonize the Security Threat Assessments across all modes of transportation. We share the goal of Congress and stakeholders that STA programs be harmonized to alleviate the burden and inconvenience placed on individuals by the need to obtain multiple STAs. To this end, we are working on a rulemaking that may further—may propose further harmonization of the security threat assessments. To achieve the optimal benefit of this rule, new legislation must be enacted that would harmonize different

statutorily required procedures that prevent harmonization and cannot be changed through rulemaking. TSA looks forward—I look forward to working with this committee, and other committees, to develop the needed legislation.

Mr. Chairman, members of the Committee, I thank you for the opportunity to appear before you. I look forward to your questions. Thank you.

[The prepared statement of Mr. Pistole follows:]

PREPARED STATEMENT OF HON. JOHN S. PISTOLE, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Good morning, Chairman Lautenberg, Ranking Member Hutchison, and distinguished members of the Committee. Thank you for the opportunity to testify today about the Transportation Security Administration's (TSA) work with the United States Coast Guard (USCG) on the Transportation Worker Identification Credential (TWIC) program.

The TWIC program, authorized by the Maritime Transportation Security Act of 2002 (MTSA) and the SAFE Port Act, strengthens the security of our nation's ports while facilitating trade through the provision of a tamper-resistant biometric credential to all port workers requiring unescorted access to secure areas of MTSA-regulated port facilities and vessels. The mission of the TWIC program is to provide a means of positively verifying the identity of those seeking access to secure areas, to conduct Security Threat Assessments (STA) to determine their eligibility, and to deny access to unauthorized individuals.

TSA began the national deployment of the TWIC program on October 16, 2007, with the enrollment of maritime workers at the Port of Wilmington, DE. A nationwide requirement for individuals to hold a TWIC in order to access MTSA-regulated facilities went into effect in April 2009, and TSA continues to operate approximately 134 enrollment centers located in ports and concentrations of maritime activity throughout the United States and its territories. These centers serve the diverse population of maritime workers, including truckers, suppliers, maintenance personnel and others who require a TWIC to allow them unescorted access to secure areas of MTSA-regulated facilities and vessels.

The process to obtain a TWIC requires two visits to an enrollment center: an initial visit to provide biographic and biometric data, and a subsequent visit to activate the credential upon successful completion of the STA. While TSA understands that this process can pose a burden on transportation workers who do not live within close proximity of an enrollment center, the process is critical to verify the identity of the individual to whom the credential is to be issued, and TSA has made efforts to mitigate this potential burden by operating 135 enrollment centers nationwide centered around maritime populations. In addition, TSA allows more remote area authorities or organizations to conduct enrollment and activation operations on their own for their defined population. TSA continues to actively engage all stakeholders to address issues concerning proximity to enrollment centers as well as other challenges faced by the maritime population relating to the TWIC program.

To date, TSA has vetted more than 1.8 million TWIC applicants. The majority of transportation workers who have no criminal history receive their TWIC within 5 to 10 calendar days of submitting an application. Applicants with criminal histories require a more stringent review and generally receive either their TWIC or notification of a potentially disqualifying offense within 30 calendar days of submitting an application. Initially, transportation workers who requested redress following an initial determination of ineligibility experienced delays in the process necessary to reach a decision. TSA took this issue very seriously and, through increased staff and adjudicative process improvements, we have been able to significantly reduce the wait time for individuals in these scenarios.

The national implementation of the TWIC as the common credential verifying the identity and background suitability significantly enhances national maritime security, which previously relied on a patchwork of private and public identity verification and threat assessment architectures to allow access to secure and restricted areas.

The STA and associated TWIC must be renewed every 5 years and preparations are being made in advance of the impending initial five-year renewal cycle. TSA is in the process of developing policies and procedures that will ensure a smooth renewal phase for the transportation workers who rely on this card to do their jobs. These procedures will both minimize the operational impact at TWIC enrollment

centers and ensure that individuals who have completed the redress process are not required to repeat the process when no new criminal information is found. This will help prevent adjudication backlogs that the expected surge in renewal enrollments might otherwise cause. Throughout this process, TSA will continue to engage the stakeholder community in order to minimize the impact of the renewal cycle on affected workers.

In addition to renewing the STA and TWIC every 5 years, TSA conducts recurrent checks of TWIC holders against terrorist watchlists and has the authority to revoke TWICs based on the results of this recurrent vetting.

In accordance with the SAFE Port Act of 2006, a TWIC pilot is currently being conducted to evaluate the feasibility as well as technical and operational impact of implementing a transportation security card reader system. Biometric identity verification would require workers to present their card to a TWIC card reader and place their finger on a biometric sensor. The reader would then verify the worker's identity by matching the fingerprint presented to the fingerprint templates on the TWIC. Based on stakeholder feedback to the TWIC Notice of Proposed Rulemaking (NPRM)[1] as well as its own analysis, DHS determined that the maritime commercial environment would benefit from an easy, rapid entrance process, not one that included entering a Personal Identification Number (PIN) as is required with the Federal Personal Identity Verification (PIV) smart card-based standard for Federal employees and contractors.[2] TSA and the Coast Guard engaged maritime stakeholders, smart card industry experts, and appropriate Federal agency representatives to develop TWIC specifications that would meet maritime industry requirements for biometric identity verification.

Formal data collection from the pilots is expected to be completed at the end of this month. Thereafter, an independent test agent will develop individual participant reports for review by TSA and the Coast Guard. TSA also continues to analyze data already collected in the pilot and will analyze new data as it is acquired. TSA has drafted the report required by Section 104 of the SAFE Port Act and will continue to make further updates to this report until its anticipated delivery to Congress this summer. These reports, along with the direct feedback from the participants, will inform decisions regarding the Coast Guard's rulemaking that will establish TWIC reader use requirements.

Notwithstanding several factors that contributed to a delay in commencing the TWIC Pilot—including the fact that participation in the pilot was voluntary, limiting DHS's ability to influence the overall pace of the pilot—the pilot officially began with the start of the first reader tests during the Initial Technical Testing (ITT) phase on August 20, 2008. The Early Operational Assessment (EOA) phase began in April 2009 with the installation of readers in the Port of Brownsville, TX, and the System Test and Evaluation (ST&E) phase began in November 2009. Over the course of the pilot, approximately 156 portable and fixed readers were in use at participating ports and facilities.

This testimony would not be complete without mention of TSA's effort to harmonize STAs across all modes of transportation. We share the goal of Congress and stakeholders that STA programs be harmonized to alleviate the burden and inconvenience placed on individuals by the need to obtain multiple STAs. To this end, TSA is working on a rulemaking that may propose further harmonization of STAs. To achieve the optimal benefit of this rule, new legislation must be enacted that would harmonize differing statutorily required procedures that prevent harmonization and cannot be changed through rulemaking. TSA will work with Congress to develop the needed legislation.

Mr. Chairman, Ranking Member Hutchison, I thank you for the opportunity to appear before you today and I look forward to answering your questions about progress in the TWIC program.

Senator LAUTENBERG. Thanks very much.

Admiral your turn. And we look forward to your testimony.

STATEMENT OF REAR ADMIRAL KEVIN S. COOK, DIRECTOR, OF PREVENTION POLICY, U.S. COAST GUARD

Admiral COOK. Well, good afternoon, Mr. Chairman and distinguished members of the Committee.

---

[1] 71 FR 29396, May 22, 2006.

[2] Federal Information Processing Standards Publication 201–1 March 2006.

With your permission, Mr. Chairman, I'd like to have my written testimony entered into the record.

Senator LAUTENBERG. So it'll be done.

Admiral COOK. Thank you for the opportunity to speak with you today about the progress the Coast Guard, working together with the Transportation Security Administration, has made in implementation of the TWIC Program, the ongoing TWIC compliance efforts for facilities and vessels regulated under the Maritime Transportation Security Act, or MTSA, and future plans for card readers.

The Coast Guard remains cognizant of how implementation and enforcement of TWIC impacts individuals and their livelihoods while balancing security needs with the economic vitality of port operations. The TWIC Program, as envisioned under MTSA and strengthened by the subsequent requirements of the SAFE Port Act, provides an additional layer of security. This is accomplished by ensuring all transportation workers and credentialed merchant mariners who seek unescorted access to secure areas in approximately 2,700 regulated facilities, 12,000 regulated vessels, and 50 regulated Outer Continental Shelf facilities have been vetted and do not pose a security risk to our marine transportation system.

As of April 15, 2009, applicable Coast Guard-credentialed mariners, MTSA-regulated facilities and vessels were required to be in compliance with the TWIC Program. The Coast Guard, through the captain of the port and the area maritime security committees, continue to monitor and enforce TWIC regulations by working closely with owners and operators.

Internal guidance documents for training, compliance, and enforcement for Coast Guard personnel have been developed and shared with our DHS partners, including TSA and CBP, and state and local agencies to promote a unified approach to enforcement protocols.

The SAFE Port Act mandates that the Coast Guard conduct two security inspections annually at all MTSA-regulated facilities, with one inspection being unannounced. During each of these, TWICs are checked by Coast Guard personnel either visually or using biometric hand-held readers.

As originally planned with the TWIC rule in 2006, the final step of implementation of the TWIC Program is to utilize the full security benefits of the card through the use of readers. Although the implementation and reader requirements were originally combined in one rulemaking, the Coast Guard and TSA heard loud and clear from the industry that further research and a different approach for readers was necessary, especially as it applies to incorporating contactless reader technology. Our stakeholders spoke, and we listened, and agreed to split the rule so that the first phase of the TWIC Program, that we're using now, is based on visual verification. Based on industry recommendations, a working specification for the use of contactless readers was developed. It is subsequently being tested through the reader pilot test that Administrator Pistole just mentioned.

In parallel with the pilot testing, the Coast Guard has been working on a proposed rulemaking that will address potential requirements for MTSA vessels and facilities to utilize electronic card readers. A key component in this will be informing with the oper-

ational, environmental, and technical data from—the TWIC reader pilot program brings to our rulemaking. Based on the current status of the pilot program, we hope to be able to publish a notice of proposed rulemaking toward the end of calendar year 2011 or early in 2012.

In the meantime, to maximize the security benefits of the TWIC, the Coast Guard procured and deployed over 200 hand-held readers for use during routine and unscheduled inspections. The Coast Guard and TSA developed several supplementary documents to help those who are required to comply with the TWIC regulations. The latest Policy Advisory Council decision, 01–11, on the voluntary use of TWIC readers was published in the *Federal Register* on the 15th of March, 2011, to assist the marine industry with consistency in the voluntary use of TWIC readers.

Also, we recently directed that our captains of the port place a higher priority on review and validation of TWIC verification procedures that are conducted during MTSA inspections. This is being done through a direct engagement with facility security officers to highlight the importance of properly trained guards, and remind them of the training aids that are available on the Coast Guard's Homeport website.

In conclusion, Mr. Chairman, the TWIC implementation marked a major milestone in the MTSA to protect our maritime transportation system. Card readers are a key step in maximizing the security benefit. And the Coast Guard is anxiously awaiting the pilot test results to help us draft effective regulations, minimizing the potential adverse impacts of the reader. While we have accomplished a great deal thus far, we acknowledge that the process has not been free from challenges. We will continue to keep the public interest in mind and also keep you informed on our progress.

Thank you for the opportunity to speak with you today. And I would be pleased to take any of your questions.

[The prepared statement of Admiral Cook follows:]

PREPARED STATEMENT OF REAR ADMIRAL KEVIN S. COOK, DIRECTOR OF PREVENTION POLICY, U.S. COAST GUARD

Good morning, Chairman Rockefeller, Ranking Member Hutchison and distinguished members of the Committee. I am Rear Admiral Kevin Cook, U.S. Coast Guard Director of Prevention Policy. It is a pleasure to be here today to update you on how the Coast Guard, in partnership with the Transportation Security Administration (TSA), continues to implement the Transportation Worker Identification Credential (TWIC) program, which strengthens the security of our nation's ports while facilitating trade by adding a layer of security which allows vetted employees with a biometric credential to have unescorted access to secure areas.

TWIC enrollment began in 2007 and today, maritime vessels and facilities within all 42 Coast Guard Captain of the Port (COTP) Zones are in compliance with the TWIC program. In April of this year, we reached more than 1.8 million enrollments for TWIC with no significant impact to commerce and the maritime transportation system. Since the Coast Guard and TSA published the TWIC requirements on January 25, 2007 in a Final Rule, we have been developing regulations, policies, systems and capabilities to serve as a solid foundation for enrollment and compliance. The deliberate process and careful steps taken to lay this foundation ensure that we gain the full security benefit from TWIC.

Background

The TWIC program builds on the security framework established by Congress in the Maritime Transportation Security Act (MTSA) of 2002. Coast Guard regulations stemming from MTSA established security requirements for maritime vessels and facilities posing a high risk of being involved in a transportation security incident.

The MTSA also required the Secretary of Homeland Security to issue a biometric transportation security card to all licensed and documented U.S. mariners, as well as those individuals granted unescorted access to secure areas of MTSA-regulated vessels and facilities. TSA was assigned this requirement, and because of our overlapping responsibilities, the Coast Guard and TSA formally joined efforts to carry out the TWIC program in November 2004. In this partnership, TSA is responsible for TWIC enrollment, security threat assessment and adjudication, card production, technology, TWIC issuance, conduct of the TWIC appeal and waiver process as it pertains to credential issuance, and management of government support systems. The Coast Guard is responsible for establishing and enforcing TWIC access control requirements for MTSA-regulated vessels and facilities.

TSA and the Coast Guard published a joint TWIC Notice of Proposed Rulemaking (NPRM) on May 22, 2006. Following the publication of the NPRM and the subsequent comment period, Congress enacted the Security and Accountability for Every Port Act of 2006 (the SAFE Port Act). The SAFE Port Act created new statutory requirements for the TWIC Program, including: the commencement of a pilot program to test the viability of TWIC cards and readers in the maritime environment; deployment of the program in priority ports by set deadlines; inclusion of a provision to allow newly hired employees to work while their TWIC application is being processed; and concurrent processing of the TWIC and merchant mariner applications.

TSA and the Coast Guard published the TWIC Final Rule on January 25, 2007, in which the Coast Guard's MTSA regulations and TSA's Hazardous Material Endorsement regulations were amended to incorporate the TWIC requirements. After receiving many comments regarding technology issues of the reader requirements as proposed in the NPRM, we removed from the final rule the requirement to install TWIC readers at vessels and facilities. This requirement is currently being addressed in a second rulemaking, which I will discuss later.

Policy

The Coast Guard and TSA developed several supplementary documents to help those who are required to comply with the TWIC regulation. To explain in detail how the Coast Guard intends to apply TWIC regulations, we established policy guidance in the form of a Navigation and Vessel Inspection Circular (NVIC) and provided answers in 16 Policy Advisory Council documents that have been published since November 21, 2007.

The Policy Advisory Council was established during the original implementation of the MTSA regulations. It is made up of Coast Guard representatives from headquarters and field level commands that are charged with considering questions from stakeholders and/or field offices to ensure consistent interpretation of regulation. The latest Policy Advisory Council Decision 01–11 on the voluntary use of TWIC readers was published in the *Federal Register* on March 15, 2011. This guidance document will assist the maritime industry and general public with TWIC reader requirements and is designed to ensure consistent installation for the voluntary use of TWIC readers for electronic identity verification across MTSA-regulated facilities and vessels.

Stakeholder Engagement and Outreach

Engagement with affected stakeholders continues to be crucial to successful implementation, and the regulatory process is one of the most important vehicles for the public to voice concerns and provide comment on the TWIC program. For example, responses received during the TWIC NPRM comment period provided valuable insight into the unique operational issues facing labor, maritime facilities and vessels required to comply with TWIC requirements. Comments regarding the technological and economic feasibility of employing the TWIC cards and card readers in the maritime environment led to splitting the rule, with the card reader requirements forming a separate, pending rulemaking. The Coast Guard published the TWIC Reader Requirements Advanced Notice of Proposed Rulemaking (ANPRM) on March 27, 2009, which again afforded the public and maritime community an opportunity to shape future TWIC requirements.

Since publication of the TWIC Final Rule and TWIC Reader Requirements ANPRM, the Coast Guard and TSA have conducted numerous outreach events at national venues such as: the American Trucking Association; Association of American Railroads; American Short Line and Regional Railroad Association; Passenger Vessel Association; American Waterways Operators; National Association of Charter Boat Operators; National Association of Waterfront Employers; National Petrochemical Refiners Association meetings; smart card and biometric industry conferences; maritime union meetings; American Association of Port Authorities conferences; and many others. In addition, quarterly TWIC Stakeholder Communica-

tion Committee meetings are being held and remain an important avenue for keeping the public informed and creating the opportunity for open dialogue.

The Coast Guard, through COTP and Area Maritime Security Committees, continues to closely monitor and encourage enrollment for TWIC and work collaboratively with owners and operators of regulated facilities and vessels to ensure compliance and enforcement of the TWIC program.

Reader Pilot Testing

In accordance with the SAFE Port Act of 2006, a TWIC pilot is currently being conducted to evaluate the feasibility as well as technical and operational impact of implementing a transportation security card reader system. TSA and the Coast Guard have begun operational testing of the TWIC card readers at geographically and operationally diverse port and vessel locations and formal data collection should be completed on May 31, 2011. Thereafter, individual participant reports will be developed by an independent test agent and then reviewed by TSA and the Coast Guard. These individual participant-level reports, along with the direct feedback from the participants, will be the primary data source for the Coast Guard to move forward in the next phase of the TWIC reader rulemaking.

Reader Requirements

Per the SAFE Port Act, the Coast Guard is required to use the pilot report to inform a final reader rulemaking. The Coast Guard, with the support of TSA, is developing a second TWIC reader requirements rule that will serve to meet the requirement for electronic TWIC readers in the maritime environment. This rulemaking will apply requirements in a risk-based fashion to leverage security benefits and capabilities. The Coast Guard solicited and received valuable input and recommendations from the Towing Safety Advisory Committee, Merchant Marine Personnel Advisory Committee, and the National Maritime Security Advisory Committee on specific aspects of potential applications of readers for vessels and facilities. As in all aspects of the TWIC program, our goal is to enhance maritime security while balancing impacts on the stakeholders, who are at the forefront of providing that security. As we evaluate the economic and operational impact on the maritime industry we will continue to seek input and recommendations to develop and issue regulations requiring industry compliance.

Compliance

The Coast Guard has the primary responsibility for ensuring compliance with the TWIC regulations. We continue to work extensively with our DHS partners, including TSA and U.S. Customs and Border Protection, as well as state and local agencies to enhance partnerships and develop enforcement assistance protocols.

All of the approximately 2,700 maritime facilities impacted by the TWIC regulations are—and have been—in compliance as of the April 15, 2009 implementation date. The Coast Guard continues to conduct both announced and unannounced spot checks to ensure compliance with the TWIC regulations.

To fully leverage the security benefits of the TWIC and other credentials, the Coast Guard has deployed 218 multi-use biometric handheld readers nationwide. The use of these readers serves as the primary means of TWIC verification during Coast Guard compliance activities. Over the past 2 years since the national compliance date, the Coast Guard has verified more than 150,000 TWICs through a combination of visual and electronic verification methods.

The use of readers by the Coast Guard and industry alike reduces the risk of successful counterfeit attempts and further adds to the ability to identify authentic credentials that have been revoked at some point after activation and delivery.

The Way Ahead

The Coast Guard continues to focus on the enforcement of the TWIC regulations and deployment of handheld readers will continue to enhance these efforts. Approximately 130 additional readers are scheduled for deployment in 2011.

We recently directed our COTPs to place higher priority on review and validation of TWIC verification procedures during required MTSA inspections. This review and validation is being done through direct engagement with Facility Security Officers to highlight the importance of properly trained guards and remind them of the training aids available.

Our ongoing compliance efforts in combination with the future reader requirements on commercial vessels and facilities through rulemaking are critical in ensuring the security of America's maritime transportation system.

Conclusion

We continue to work closely with TSA to facilitate outreach to the maritime industry in an effort to enhance the overall TWIC experience for workers and maritime operators—from improving the enrollment and activation processes to ensuring the necessary guidance and support is in place for maritime operator enforcement. We have accomplished important milestones, strengthened working relationships with public and industry stakeholders, and held a steadfast commitment to securing the maritime transportation system while facilitating commerce. As we continue to make improvements regarding compliance, enforcement, and continued industry engagement, we will ensure Congress remains informed of our progress.

Thank you for the opportunity to testify today. I look forward to your questions.

Senator LAUTENBERG. Thank you, Admiral Cook.

And Mr. Steve Lord, we invite you to give your testimony.

STATEMENT OF STEPHEN M. LORD, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. LORD. Thank you, Mr. Chairman and distinguished members of the Committee.

I'm really pleased to be here today to discuss the findings of our TWIC report, which is being publicly released today. As you know, TSA and the Coast Guard jointly manage the TWIC Program, which requires maritime workers to obtain a biometric ID card to access secure areas of MTSA-regulated facilities and vessels.

Today, I would like to discuss two issues: the internal controls governing TWIC enrollment, background checking, and use, as well as DHS assessments of the effectiveness of this program.

The main point that I'd like to convey today is that internal control weaknesses in the TWIC Program's enrollment and background checking process do not provide what we deem as reasonable assurance in meeting key security goals; in other words, that only qualified individuals are acquiring TWICs. And second, once issued a TWIC, TWIC holders maintain their eligibility for holding the card. For example, we found that the flags raised by enrollment personnel or electronic document scanners were not being systematically used during the background checking process to verify an applicant's identification. This helps explain why our special investigators were not detected when using counterfeit or fraudulent application documents to acquire TWICs. TSA also does not verify that applicants need a TWIC for employment-related reasons. In other words, there's not employee sponsorship, unlike other government credentials. We also found that program adjudicators do not use clear criteria when reviewing TWIC applicants with extensive, nondisqualifying criminal convictions, such as larceny and theft. This is an important issue, as about 461,000 TWIC holders have a criminal record, based on the results from the FBI. And this is about 27 percent of the total TWIC-holder population.

Finally, we also found that program controls did not provide reasonable assurance that TWIC holders continue to meet immigration eligibility requirements once they acquire TWIC. For example, the program does not issue TWICs for a term less than 5 years, to match the expiration of a visa. Instead, TSA relies on TWIC holders and employers to report if a worker is no longer legally present in the country.

The weaknesses I've discussed may have contributed to the breach of MTSA-regulated ports and facilities during the covert

tests we ran. During these tests, our investigators were successful in accessing ports using either counterfeit TWICs or real TWICs acquired through fraudulent means, paired with a false business case for entering a facility.

And regarding our second key research objective, in seeking to determine the impact of the program, we found that DHS has not assessed the program's effectiveness in enhancing port security, a key program goal. Thus, it's unclear, at this point, whether the program is more effective or less effective than prior approaches used to enhance port and vessel security. Our report findings would question the other witness' statement that the program significantly enhances national maritime security.

Today's report makes several important recommendations to address the internal control weaknesses we identified. For example, our report is recommending that DHS complete an internal control assessment to identify other potential holes in the system, as well as identifying cost-effective fixes. We also recommended that DHS conduct a formal assessment to clarify how the program will improve security, beyond the port efforts already in place. We also recommended that the Coast Guard improve the quality of the information used to monitor and enforce TWIC compliance. The good news I'd like to report today, Mr. Chairman, is that the DHS, TSA, and the Coast Guard all agreed to implement all our report recommendations.

In closing, before proceeding on the path to full implementation, with potentially billions of dollars at stake, it's important that Congress and industry stakeholders fully understand the program's current strengths, current weaknesses, and the likely cost of mitigating the risks we've identified in the report we're releasing today.

Mr. Chairman, this concludes my prepared testimony. I look forward to answering any questions that you or other members of the Committee may have.

Thank you.

[The prepared statement of Mr. Lord follows:]

PREPARED STATEMENT OF STEPHEN M. LORD, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee:

I am pleased to be here today to discuss credentialing issues associated with the security of U.S. transportation systems and facilities. Securing these systems requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy and international commerce. As we have previously reported, these systems and facilities are vulnerable and difficult to secure given their size, easy accessibility, large number of potential targets, and proximity to urban areas.[1] The Maritime Transportation Security Act of 2002 (MTSA) required regulations preventing individuals from having unescorted access to secure areas of MTSA-regulated facilities and vessels unless they possess a biometric transportation security card and are authorized to be in such an area. MTSA further required that biometric transportation security cards be issued to eligible individuals unless determined that an applicant poses a security risk warranting denial of the card. The Transportation Worker Identification Credential (TWIC) pro-

[1] See GAO, Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers, GAO–10–43 (Washington, D.C.: Nov. 18, 2009).

gram is designed to implement these biometric maritime security card requirements.[2]

The TWIC program, once implemented, aims to meet the following stated mission needs:

> Positively identify authorized individuals who require unescorted access to secure areas of the nation's transportation system.
>
> Determine the eligibility of individuals to be authorized unescorted access to secure areas of the transportation system by conducting a security threat assessment.
>
> Ensure that unauthorized individuals are not able to defeat or otherwise compromise the access system in order to be granted permissions that have been assigned to an authorized individual.
>
> Identify individuals who fail to maintain their eligibility requirements subsequent to being permitted unescorted access to secure areas of the Nation's transportation system and immediately revoke the individual's permissions.

Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) and the U.S. Coast Guard are responsible for implementing and enforcing the TWIC program. In addition, DHS's Screening Coordination Office facilitates coordination among the various DHS components involved in TWIC.

My statement is based on a report we are releasing publicly today on the TWIC program.[3] Like the report, it will discuss the extent to which: (1) TWIC processes for enrollment, background checking, and use are designed to provide reasonable assurance that unescorted access to secure areas of MTSA-regulated facilities and vessels is limited to qualified individuals, and (2) DHS has assessed the effectiveness of TWIC, and whether the Coast Guard has effective systems in place to measure compliance.

For the report, we reviewed applicable laws, regulations, and policies, as well as documentation provided by TSA on the TWIC program systems and processes. We also reviewed the processes and data sources with TWIC program management from TSA and Lockheed Martin (the contractor responsible for implementing the program) and met with officials from TSA and the Coast Guard, as well as the Criminal Justice Information Services Division at the Federal Bureau of Investigation (FBI). We then evaluated the processes against the TWIC program's mission needs and Standards for Internal Control in the Federal Government.[4] Further, our investigators conducted covert testing at enrollment center(s) to identify whether individuals providing fraudulent information could acquire an authentic TWIC, and at maritime ports with MTSA-regulated facilities and vessels to identify security vulnerabilities and program control deficiencies. In addition, we reviewed the type and substance of management information available to the Coast Guard and compared them to Standards for Internal Control in the Federal Government. We conducted this work in accordance with generally accepted government auditing standards. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

---

[2] The program requires maritime workers to complete background checks to obtain a biometric identification card and be authorized to be in the secure area by the owner/operator in order to gain unescorted access to secure areas of MTSA-regulated facilities and vessels. Under Coast Guard regulations, a secure area, in general, is an area over which the owner/operator has implemented security measures for access control in accordance with a Coast Guard-approved security plan. For most maritime facilities, the secure area is generally any place inside the outermost access control point. For a vessel or outer continental shelf facility, such as off-shore petroleum or gas production facilities, the secure area is generally the whole vessel or facility. Biometrics refers to technologies that measure and analyze human body characteristics for authentication purposes. The Department of Homeland Security (DHS) has estimated that implementing the TWIC program could cost the Federal Government and the private sector a combined total of between $694.3 million and $3.2 billion over a ten-year period. However, these figures do not include costs associated with implementing and operating readers. A pilot on the use of TWIC with card readers is currently underway and will inform a proposed TWIC regulation, and these figures are to be updated as part of this process.

[3] See GAO, Transportation Worker Identification Credential: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Objectives, GAO–11–657 (Washington, D.C.: May 10, 2011).

[4] GAO, Standards for Internal Control in the Federal Government, GAO/AIMD–00–21.3.1 (Washington, D.C.: November 1999).

Internal Control Weaknesses in DHS's Biometric Transportation ID Program Hinder Efforts to Ensure Security Objectives Are Fully Achieved

DHS has established a system of TWIC-related processes and controls. However, internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limit the program's ability to meet the program's stated mission needs or provide reasonable assurance that access to secure areas of MTSA-regulated facilities is restricted to qualified individuals. Specifically, internal controls[5] in the enrollment and background checking processes are not designed to provide reasonable assurance that: (1) only qualified individuals can acquire TWICs; (2) adjudicators follow a process with clear criteria for applying discretionary authority when applicants are found to have extensive criminal convictions; or (3) once issued a TWIC, TWIC holders have maintained their eligibility.

To meet the stated program purpose, TSA's focus in designing the TWIC program was on facilitating the issuance of TWICs to maritime workers. However, TSA did not assess the internal controls in place to determine whether they provided reasonable assurance that the program could meet defined mission needs for limiting access to only qualified individuals. For example, controls that the TWIC program has in place to identify the use of potentially counterfeit identity documents are not used to routinely inform background checking processes. Additionally, controls are not in place to determine whether an applicant has a need for a TWIC. For example, regulations governing the TWIC program security threat assessments require applicants to disclose their job description and location(s) where they will most likely require unescorted access, if known, among other things. However, TSA enrollment processes do not require that this information be provided by applicants.

In addition, TWIC program controls are not designed to require that adjudicators follow a process with clear criteria for applying discretionary authority when applicants are found to have extensive criminal convictions. Being convicted of a felony does not automatically disqualify a person from being eligible to receive a TWIC; however, prior convictions for certain crimes are automatically disqualifying.[6] For example, offenses such as espionage or treason would permanently disqualify an individual from obtaining a TWIC. Other offenses, such as murder or the unlawful possession of an explosive device, while categorized as permanent disqualifiers, are also eligible for a waiver under TSA regulations. These offenses might not permanently disqualify an individual from obtaining a TWIC if TSA determines that an applicant does not represent a security threat. As of September 8, 2010, the agency reported 460,786 cases where the applicant was approved, but had a criminal record based on the results from the FBI. This represents approximately 27 percent of individuals approved for a TWIC at the time. Although TSA has the discretion and authority to consider the totality of an individual's criminal record, including the existence of: (1) extensive criminal convictions, (2) criminal offenses not defined as a permanent or interim disqualifying criminal offense, such as theft or larceny, and (3) certain periods of imprisonment, TSA has not developed a definition for what extensive foreign or domestic criminal convictions means, or developed guidance to ensure that adjudicators apply this authority consistently. In commenting on our report, DHS concurred with our related recommendation, and consequently may address this weakness as part of its efforts to correct internal control weaknesses in the TWIC program.

Further, TWIC program controls are not designed to provide reasonable assurance that TWIC holders have maintained their eligibility once issued TWICs. For example, controls are not designed to determine whether TWIC holders have committed disqualifying crimes at the Federal or state level after being granted a TWIC. Although existing policies may hamper TSA's ability to check FBI-held fingerprint-based criminal history records for the TWIC program on an ongoing basis after TWIC issuance, TSA has not explored alternatives for addressing this weakness, such as informing facility and port operators of this weakness and identifying solutions for leveraging existing state criminal history information, where available. In

---

[5] In accordance with Standards for Internal Control in the Federal Government, the design of the internal controls is to be informed by identified risks the program faces from both internal and external sources; the possible effect of those risks; control activities required to mitigate those risks; and the cost and benefits of mitigating those risks.

[6] Threat assessment processes for the TWIC program include conducting background checks to determine whether each TWIC applicant poses a security threat. These checks, in general, can include checks for criminal history records, immigration status, terrorism databases and watchlists, and records indicating an adjudication of a lack of mental capacity, among other things. As defined in TSA implementing regulations, the term security threat means an individual who TSA determines or suspects of posing a threat to national security, to transportation security, or of terrorism.

addition, controls are not designed to provide reasonable assurance that TWIC holders continue to meet immigration status eligibility requirements. For example, if a TWIC holder's stated period of legal presence in the United States is about to expire or has expired, the TWIC program does not request or require proof from TWIC holders to show that they continue to maintain legal presence in the United States. Additionally, although it has regulatory authority to do so, the program does not issue TWICs for a term less than 5 years to match the expiration of a visa.[7]

Internal control weaknesses in TWIC enrollment, background checking, and use could have contributed to the breach of selected MTSA-regulated facilities during covert tests conducted by our investigators. During these tests at several selected ports, our investigators were successful in accessing ports using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases (*i.e.,* reasons for requesting access). Our investigators did not gain unescorted access to a port where a secondary port-specific identification was required in addition to the TWIC. TSA and Coast Guard officials stated that the TWIC card alone is not sufficient and that the cardholder is also required to present a business case. However, our covert tests demonstrated that having an authentic TWIC and a legitimate business case were not always required in practice.

Prior to fielding the program, TSA did not conduct a risk assessment of the TWIC program to identify program risks and the need for controls to mitigate existing risks and weaknesses, as called for by internal control standards. Such an assessment could help provide reasonable assurance that control weaknesses in one area of the program do not undermine the reliability of other program areas or impede the program from meeting mission needs. TWIC program officials told us that control weaknesses were not addressed prior to initiating the TWIC program because they had not previously identified them, or because they would be too costly to address. However, as we noted in our report, officials did not provide: (1) documentation to support their cost concerns and (2) did not complete an assessment of whether they needed to implement additional compensating controls or of the risks associated with not correcting for existing internal control weaknesses. In our May 2011 report, we recommended that the Secretary of Homeland Security perform an internal control assessment of the TWIC program by: (1) analyzing existing controls, (2) identifying related weaknesses and risks, and (3) determining cost-effective actions needed to correct or compensate for those weaknesses so that reasonable assurance of meeting TWIC program objectives can be achieved. This assessment should consider weaknesses we identified in this report among other things. DHS officials concurred with our recommendation.

TWIC's Effectiveness at Enhancing Security Has Not Been Assessed, and the Coast Guard Lacks the Ability to Assess Trends in TWIC Compliance

DHS asserted in its 2009 and 2010 budget submissions that the absence of the TWIC program would leave America's critical maritime port facilities vulnerable to terrorist activities.[8] However, to date, DHS has not assessed the effectiveness of TWIC at enhancing security or reducing risk for MTSA-regulated facilities and vessels. Further, DHS has not demonstrated that TWIC, as currently implemented and planned with card readers, is more effective than prior approaches used to limit access to ports and facilities, such as using facility-specific identity credentials with business cases.

According to TSA and Coast Guard officials, because the program was mandated by Congress as part of MTSA, DHS did not conduct a risk assessment to identify and mitigate program risks prior to implementation. Further, according to these officials, neither the Coast Guard nor TSA analyzed the potential effectiveness of

[7] Instead, TSA relies on: (1) TWIC holders to self-report if they no longer have legal presence in the country, and (2) employers to report if a worker is no longer legally present in the country. TWIC-related regulations provide, for example, that individuals disqualified from holding a TWIC for immigration status reasons must surrender the TWIC to TSA. In addition, the regulations provide that TWICs are deemed to have expired when the status of certain lawful nonimmigrants with a restricted authorization to work in the United States (*e.g.,* H–1B1 Free Trade Agreement) expires, the employer terminates the employment relationship with such an applicant, or such applicant otherwise ceases working for the employer, regardless of the date on the face of the TWIC. Upon the expiration of such nonimmigrant status for an individual who has a restricted authorization to work in the United States, the employer and employee both have related responsibilities—the employee is required to surrender the TWIC to the employer, and the employer is required to retrieve the TWIC and provide it to TSA.

[8] See DHS, DHS Exhibit 300 Public Release BY10/TSA—Transportation Worker Identification Credentialing (TWIC) (Washington, D.C.: Apr. 17, 2009) and DHS Exhibit 300 Public Release BY09/TSA—Transportation Worker Identification Credentialing (TWIC) (Washington, D.C.: July 27, 2007).

TWIC in reducing or mitigating security risk—either before or after implementation—because they were not required to do so by Congress. However, internal control weaknesses raise questions about the effectiveness of the TWIC program. Moreover, as we have previously reported, Congress also needs information on whether and in what respects a program is working well or poorly to support its oversight of agencies and their budgets, and agencies' stakeholders need performance information to accurately judge program effectiveness. Therefore, we recommended in our May 2011 report that the Secretary of Homeland Security conduct an effectiveness assessment that includes addressing internal control weaknesses and, at a minimum, evaluates whether use of TWIC in its present form and planned use with readers would enhance the posture of security beyond efforts already in place given costs and program risks. DHS concurred with our recommendation.

Further, Executive Branch requirements provide that prior to issuing a new regulation, agencies are to conduct a regulatory analysis, which is to include an assessment of costs, benefits, and risks. Therefore, DHS is required to issue a new regulatory analysis for its proposed regulation on the use of TWIC with biometric card readers. Conducting a regulatory analysis using the information from the internal control and effectiveness assessments could better inform the new regulatory analysis and could help DHS identify and assess the full costs and benefits of implementing the TWIC program. Therefore, in our May 2011 report, we recommended that the Secretary of Homeland Security use the information from the internal control and effectiveness assessments as the basis for evaluating the costs, benefits, security risks, and corrective actions needed to implement the TWIC program. This should be done in a manner that will meet stated mission needs and mitigate existing security risks as part of the regulatory analysis being completed for the new TWIC biometric card reader regulation. DHS concurred with our recommendation.

Finally, the Coast Guard's approach for monitoring and enforcing TWIC compliance nationwide could be improved by enhancing its collection and assessment of related maritime security information. For example, the Coast Guard tracks TWIC program compliance, but the processes involved in the collection, cataloguing, and querying of information cannot be relied on to produce the management information needed to assess trends in compliance with the TWIC program or associated vulnerabilities. The Coast Guard uses its Marine Information for Safety and Law Enforcement (MISLE) database to monitor activities related to MTSA-regulated facility and vessel oversight, including observations of TWIC-related deficiencies. Coast Guard officials reported that they are making enhancements to the MISLE database and plan to distribute updated guidance on how to collect and input information. However, as of May 2011, the Coast Guard had not yet set a date for implementing these changes. Further, these enhancements do not address all weaknesses identified in our report that hamper the Coast Guard's efforts to conduct trend analysis of the deficiencies as part of its compliance reviews. Therefore, in our May 2011 report, we recommended that the Secretary of Homeland Security direct the Commandant of the Coast Guard to design effective methods for collecting, cataloguing, and querying TWIC-related compliance issues to provide the Coast Guard with the enforcement information needed to assess trends in compliance with the TWIC program and identify associated vulnerabilities. DHS concurred with our recommendation.

As the TWIC program continues on the path to full implementation—with potentially billions of dollars needed to install TWIC card readers in thousands of the nation's ports, facilities, and vessels at stake—it is important that Congress, program officials, and maritime industry stakeholders fully understand the program's potential benefits and vulnerabilities, as well as the likely costs of addressing these potential vulnerabilities. The report we are releasing today aims to help inform stakeholder views on these issues.

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, this concludes my prepared testimony. I look forward to answering any questions that you may have.

ATTACHMENT

U.S. Government Accountability Office (GAO)—Report to Congressional Requesters—May 2011—Transportation Worker Identification Credential

Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives

Abbreviations

ATSA—Aviation and Transportation Security Act
CSOC—Colorado Springs Operations Center
DHS—Department of Homeland Security
FBI—Federal Bureau of Investigation
FEMA—Federal Emergency Management Agency
IAFIS—Integrated Automated Fingerprint Identification System
III—Interstate Identification Index
MISLE—Marine Information for Safety and Law Enforcement
MSRAM—Maritime Security Risk Analysis Model
MTSA—Maritime Transportation Security Act
NCIC—National Crime Information Center
NIPP—National Infrastructure Protection Plan
SAFE Port Act—Security and Accountability For Every Port Act
SAVE—Systematic Alien Verification for Entitlements
TSA—Transportation Security Administration
TWIC—Transportation Worker Identification Credential

May 10, 2011

CONGRESSIONAL REQUESTERS

Securing transportation systems and facilities requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the United States economy and necessary for supporting international commerce. As we have previously reported, these systems and facilities are vulnerable and difficult to secure given their size, easy accessibility, large number of potential targets, and proximity to urban areas.[1]

The Maritime Transportation Security Act of 2002[2] (MTSA) required the Secretary of Homeland Security to prescribe regulations preventing individuals from having unescorted access to secure areas of MTSAregulated facilities and vessels unless they possess a biometric transportation security card and are authorized to be in such an area.[3] MTSA further tasked the Secretary with the responsibility to issue biometric transportation security cards to eligible individuals unless the Secretary determines that an applicant poses a security risk warranting denial of the card. The Transportation Worker Identification Credential (TWIC) program is designed to implement these biometric maritime security card requirements. The program requires maritime workers to complete background checks to obtain a biometric identification card and be authorized to be in the secure area by the owner/operator in order to gain unescorted access to secure areas of MTSA-regulated facilities

---

[1] See GAO, *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO–10–43 (Washington, D.C.: Nov. 18, 2009); *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO–06–982 (Washington, D.C.: Sept. 29, 2006); and *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO–05–106 (Washington, D.C.: Dec. 10, 2004).

[2] Pub. L. No. 107–295, 116 Stat. 2064 (2002).

[3] Under Coast Guard regulations, a secure area, in general, is an area over which the owner/operator has implemented security measures for access control in accordance with a Coast Guard-approved security plan. For most maritime facilities, the secure area is generally any place inside the outer-most access control point. For a vessel or outer continental shelf facility, such as off-shore petroleum or gas production facilities, the secure area is generally the whole vessel or facility.

and vessels.[4] According to the Coast Guard, as of December 2010 and January 2011, there were 2,509 facilities and 12,908 vessels, respectively, which are subject to MTSA regulations and must implement TWIC provisions.[5]

Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) and the U.S. Coast Guard are responsible for implementing and enforcing the TWIC program. TSA's responsibilities include enrolling TWIC applicants, conducting background checks to assess the individual's security threat, and issuing TWICs. The Coast Guard is responsible for developing TWIC-related security regulations and ensuring that MTSA-regulated maritime facilities and vessels are in compliance with these regulations. In addition, DHS's Screening Coordination Office facilitates coordination among the various DHS components involved in TWIC, such as TSA and the Coast Guard, as well as the U.S. Citizenship and Immigration Services, which personalizes the credentials,[6] and the Federal Emergency Management Agency, which administers grant funds in support of the TWIC program.

In January 2007, a federal regulation (known as the TWIC credential rule) set a compliance deadline, subsequently extended to April 15, 2009, whereby each maritime worker seeking unescorted access to secure areas of MTSA-regulated facilities and vessels must possess a TWIC.[7] In September 2008, we reported that TSA, the Coast Guard, and maritime industry stakeholders (*e.g.,* operators of MTSA-regulated facilities and vessels) had faced challenges in implementing the TWIC program, including enrolling and issuing TWICs to a larger population than was originally anticipated, ensuring that TWIC access control technologies perform effectively in the harsh maritime environment, and balancing security requirements with the flow of maritime commerce.[8] In November 2009, we reported that progress had been made in enrolling workers and activating TWICs, and recommended that TSA develop an evaluation plan to guide pilot efforts and help inform the future implementation of TWIC with electronic card readers.[9] DHS generally concurred and discussed actions to implement the recommendations, but these actions have not yet fully addressed the intent of all of the recommendations. Currently, TWICs are primarily used as visual identity cards—known as a flashpass—where a card is to be visually inspected before a cardholder is allowed unescorted access to a secure area of a MTSA-regulated port or facility.[10] As of January 6, 2011, TSA reported over 1.7 million enrollments and 1.6 million cards issued and activated.[11]

In response to your request, we evaluated the extent to which TWIC program controls provide reasonable assurance that unescorted access to secure areas of MTSA-regulated facilities and vessels is limited to those possessing a legitimately issued TWIC and who are authorized to be in such an area. Specifically, this report addresses the following questions:

1. To what extent are TWIC processes for enrollment, background checking, and use designed to provide reasonable assurance that unescorted access to secure areas of MTSA-regulated facilities and vessels is limited to qualified individuals?

2. To what extent has DHS assessed the effectiveness of TWIC, and does the Coast Guard have effective systems in place to measure compliance?

This report is a public version of a related sensitive report that we issued to you in May 2011. DHS and TSA deemed some of the information in the prior report as sensitive security information, which must be protected from public disclosure.

---

[4] Biometrics refers to technologies that measure and analyze human body characteristics—such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements—for authentication purposes.

[5] 33 C.F.R. Part 105, for example, governs maritime facility security and sets forth general security requirements along with requirements for facility security assessments and facility security plans, among other things. General maritime security requirements pertaining to vessels are set out in 33 C.F.R. Part 104.

[6] A card is personalized when the card holder's personal information, such as photograph and name, are added to the card.

[7] 72 Fed. Reg. 3492 (2007); Extension of deadline to April 15, 2009 by 73 Fed. Reg. 25562 (2008).

[8] GAO, *Transportation Worker Identification Credential: A Status Update*, GAO–08–1151T (Washington, D.C.: Sept. 17, 2008).

[9] GAO–10–43.

[10] TWIC guidance provides that possession of a TWIC is required for an individual to be eligible for unescorted access to secure areas of vessels and facilities. With the issuance of a TWIC, it is still the responsibility of facility and vessel owners to determine who should be granted access to their facilities or vessels.

[11] Prior to issuing a TWIC, each TWIC is activated, or turned on, after the person being issued the TWIC provides a personal identification number.

Therefore, this report omits sensitive information about the TWIC program, including techniques used to enroll and conduct a background check on individuals and assess an individual's eligibility for a TWIC, and the technologies that support TWIC security threat assessment determinations and Coast Guard inspections. In addition, at TSA's request, we have redacted data on specific enrollment center(s) and maritime ports where our investigators conducted covert testing. Although the information provided in this report is more limited in scope, it addresses the same questions and includes the same recommendations as the sensitive report. Also, the overall methodology used for both reports is the same.

To assess the extent to which TWIC program processes were designed to provide reasonable assurance that unescorted access to secure areas of MTSA-regulated facilities and vessels is limited to qualified individuals, we reviewed applicable laws, regulations, and policies.[12] We also reviewed documentation provided by TSA on the TWIC program systems and processes, such as the TWIC User Manual for Trusted Agents, Statement of Objectives, and Concept of Operations. We further reviewed the processes and data sources with TWIC program management from TSA and Lockheed Martin (the contractor responsible for implementing the program).[13] We also met with: (1) the Director of Vetting Operations at TSA's Colorado Springs Operations Center (CSOC), where background checks for links to terrorism and continual vetting of TWIC holders is to take place; (2) the Operations Manager for the Adjudication Center, where secondary background checks are to be conducted for applicants with identified criminal or immigration issues; and (3) the Director at DHS's Screening Coordination Office responsible for overseeing credentialing programs across DHS. Additionally, we met with the Criminal Justice Information Services Division at the Federal Bureau of Investigation (FBI) to discuss criminal vetting processes and policies. We then evaluated the processes against the TWIC program's mission needs and *Standards for Internal Control in the Federal Government*.[14] As part of our assessment of TWIC program controls, we also did the following:

- We visited four TWIC enrollment and activation centers located in areas with high population density and near ports participating in the TWIC pilot to observe how TWIC enrollments are conducted.[15] The results are not generalizable to all enrollment and activation centers; however, because all centers are to conduct the same operations following the same guidance, the locations we visited provided us with an overview of the TWIC enrollment and activation/issuance processes.
- We had our investigators conduct covert testing at enrollment center(s) operating at the time to identify whether individuals providing fraudulent information could acquire an authentic TWIC. The information we obtained from the covert testing at enrollment center(s) is not generalizable across all TWIC enrollment centers. However, because all enrollments are to be conducted following the same established processes, we believe that the information from our covert tests provided us with important perspective on TWIC program enrollment and background checking processes, as well as potential challenges in verifying an individual's identity.

Further our investigators conducted covert testing at several selected maritime ports with MTSA-regulated facilities and vessels to identify security vulnerabilities and program control deficiencies. These locations were selected based on their geographic location across the country (east coast, gulf coast, and west coast) and port

---

[12] See, for example, MTSA, Security and Accountability For Every Port Act (SAFE Port Act) of 2006 (Pub. L. No. 109–347, 120 Stat. 1884 (2006)) amendments to MTSA, Navigation and Vessel Inspection Circular Number 03–07: *Guidance for the Implementation of the Transportation Worker Identification Credential Program in the Maritime Sector* (Washington, D.C.: July 2, 2007), Coast Guard Policy Advisory Council (PAC) decisions, and Commandant Instruction M16601.01: *Coast Guard Transportation Worker Identification Credential Verification and Enforcement Guide* (Washington, D.C.: Oct. 10, 2008).

[13] To assess the reliability of data on the number of TWIC enrollments, the number of self-identified U.S. citizens or nationals asserting themselves to be born in the United States or in a U.S. territory, and the number of TWICs approved after the initial background check, we reviewed program systems documentation and interviewed knowledgeable agency officials about the source of the data and the controls the TWIC program and systems had in place to maintain the integrity of the data. We determined that the data were sufficiently reliable for the purposes of our report. The data we reviewed were collected between October 2007 and December 2010.

[14] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD–00–21.3.1 (Washington, D.C.: November 1999).

[15] We visited the Howland Hook enrollment center in Staten Island, New York, the Whitehall Ferry Terminal enrollment center in New York, New York, the Terminal Island enrollment center in San Pedro, California, and the Long Beach enrollment center in Long Beach, California.

size in terms of cargo volume. We also visited or met with officials at each of the seven original pilot sites being used to test TWIC card readers,[16] interviewed port security officials at two additional ports responsible for implementing TWIC at their port,[17] and met with nine maritime or transportation industry associations [18] to obtain information on: (1) the use of TWIC as a flashpass and with biometric readers where they are in use, (2) experiences with TWIC card performance, and (3) any suspected or reported cases of TWIC card fraud. The information we obtained from the security officials at the 9 ports or pilot participants we visited is not generalizable across the maritime transportation industry as a whole, but collectively, the ports we visited accounted for 56 percent of maritime container trade in the United States, and the ports our investigators visited as part of our covert testing efforts accounted for 54 percent of maritime container trade in the United States in 2009. As such, we believe that the information from these interviews, site visits, and covert tests provided us with important additional perspective and context on the TWIC program, as well as information about potential implementation challenges faced by MTSA-regulated facilities/vessels, transportation workers, and mariners.

To assess the extent to which DHS has assessed the effectiveness of TWIC, and determine whether the Coast Guard has effective systems in place to measure compliance, we reviewed applicable laws, regulations, and policies.[19] We also met with TWIC program officials from TSA and the Coast Guard, as well as Coast Guard officials responsible for assessing maritime security risk, and reviewed related documents, to identify how TWIC is to enhance maritime security.[20] In addition, we met with Coast Guard TWIC program officials, data management staff, and Coast Guard officials stationed at four port areas across the United States with enforcement responsibilities to assess the agency's approach to enforcing compliance with TWIC regulations and measuring program effectiveness.[21] As part of this effort, we reviewed the type and substance of management information available to the Coast Guard for assessing compliance with TWIC. In performing this work, we evaluated the Coast Guard's practices against TWIC program mission needs and *Standards for Internal Control in the Federal Government*.

We conducted this performance audit from November 2009 through March 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.[22]

---

[16] We visited pilot participants at the Ports of Los Angeles, Long Beach, and Brownsville, and the Port Authority of New York and New Jersey. We also interviewed and or met with officials at vessel operations participating in the TWIC pilot, including the Staten Island Ferry in Staten Island, New York; Magnolia Marine Transports in Vicksburg, Mississippi; and Watermark Cruises in Annapolis, Maryland.

[17] We met with officials responsible for implementing TWIC at the Port of Baltimore and the Port of Houston. We selected the Port of Baltimore based on proximity to large population centers and we selected the Port of Houston because it was using TWICs with readers.

[18] We interviewed representatives from the Association of the Bi-State Motor Carriers, the New Jersey Motor Truck Association, the Association of American Railroads, the American Public Transportation Association, the American Association of Port Authorities, the International Liquid Terminals Association, the International Longshore and Warehouse Union, the National Employment Law Project, and the Passenger Vessel Association. These organizations were selected because together they represent the key constituents of port operations.

[19] See, for example, MTSA, Security and Accountability For Every Port Act (SAFE Port Act) of 2006 (Pub. L. No. 109–347, 120 Stat. 1884 (2006)) amendments to MTSA, Navigation and Vessel Inspection Circular Number 03–07: *Guidance for the Implementation of the Transportation Worker Identification Credential Program in the Maritime Sector* (Washington, D.C.: July 2, 2007), Coast Guard Policy Advisory Council (PAC) decisions, and Commandant Instruction M16601.01: *Coast Guard Transportation Worker Identification Credential Verification and Enforcement Guide* (Washington, D.C.: Oct. 10, 2008).

[20] See, for example, the Coast Guard's 2008 Analysis of Transportation Worker Identification Credential (TWIC) Electronic Reader Requirements in the Maritime Sector, and the Homeland Security Institute's 2008 Independent Verification and Validation of Development of Transportation Worker Identification Credential (TWIC) Reader Requirements.

[21] We interviewed Coast Guard officials in New York and New Jersey; Los Angeles and Long Beach, California; Corpus Christi, Texas; and Baltimore, Maryland. We met with these Coast Guard officials because the facilities, vessels, and enrollment centers we visited are housed in these officials' area(s) of responsibility.

[22] During the course of the audit, we provided briefings on the preliminary results of our work in May and October 2010.

Background

TWIC History and Purpose

In November 2001, the Aviation and Transportation Security Act (ATSA)[23] was enacted, requiring TSA to, among other things, work with airport operators to strengthen access control points to secured areas and to consider using biometric access control systems, or similar technologies, to verify the identity of individuals who seek to enter a secure airport area. In response to ATSA, TSA established the TWIC program in December 2001.[24] In November 2002, MTSA was enacted and required the Secretary of Homeland Security to issue a maritime worker identification card that uses biometrics to control access to secure areas of maritime transportation facilities and vessels.[25] In addition, the Security and Accountability For Every Port Act (SAFE Port Act) of 2006 amended MTSA and directed the Secretary of Homeland Security to, among other things, implement the TWIC pilot project to test TWIC use with biometric card readers and inform a future regulation on the use of TWIC with electronic readers.

In requiring the issuance of transportation security cards for entry into secure areas of a facility or vessel as part of MTSA, Congress noted in the "Findings" section of the legislation that ports in the United States are a major location for Federal crime such as cargo theft and smuggling, and are susceptible to large-scale acts of terrorism.[26] For example, according to the Coast Guard's January 2008 National Maritime Terrorism Threat Assessment, al Qaeda leaders and supporters have identified western maritime assets as legitimate targets.[27] Moreover, according to the Coast Guard assessment, al Qaeda-inspired operatives are most likely to use vehicle bombs to strike U.S. cargo vessels, tankers, and fixed coastal facilities such as ports. Studies have demonstrated that attacks on ports could have serious consequences. For example, a study by the Center for Risk and Economic Analysis of Terrorist Events on the impact of a dirty bomb attack on the Ports of Los Angeles and Long Beach estimated that the economic consequences from a shutdown of the harbors due to the contamination could result in significant losses in the tens of billions of dollars, including the decontamination costs and the indirect economic impacts due to the port shutdown.[28]

As defined by DHS, the purpose of the TWIC program is to design and field a common credential for all transportation workers across the United States who require unescorted access to secure areas at MTSA-regulated maritime facilities and vessels.[29] As such, the TWIC program, once implemented, aims to meet the following stated mission needs:

- Positively identify authorized individuals who require unescorted access to secure areas of the Nation's transportation system.
- Determine the eligibility of individuals to be authorized unescorted access to secure areas of the transportation system by conducting a security threat assessment.
- Ensure that unauthorized individuals are not able to defeat or otherwise compromise the access system in order to be granted permissions that have been assigned to an authorized individual.
- Identify individuals who fail to maintain their eligibility requirements subsequent to being permitted unescorted access to secure areas of the Nation's transportation system and immediately revoke the individual's permissions.

---

[23] Pub. L. No. 107–71, 115 Stat. 597 (2001).

[24] TSA was transferred from the Department of Transportation to DHS pursuant to requirements in the Homeland Security Act, enacted on November 25, 2002 (Pub. L. No. 107–296, 116 Stat. 2135, 2178 (2002)).

[25] Prior to TWIC, facilities and vessels administered their own approaches for controlling access based on the perceived risk at the facility. These approaches, among others, included requiring people seeking access to have a reason for entering, facility-specific identification, and in some cases, a background check. Some ports and port facilities still maintain their own credentials.

[26] Maritime Transportation Security Act of 2002 (Pub. L. No. 107–295,116 Stat. 2064 (2002)). The FBI estimates that in the United States, cargo crime amounts to $12 billion annually and finds that most cargo theft occurs in or near seaports.

[27] U.S. Coast Guard Intelligence Coordination Center, *National Maritime Terrorism Threat Assessment* (Washington, D.C.: Jan. 7, 2008).

[28] H. Rosoff and D. von Winterfeldt, "A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach," *Journal of Risk Analysis*, vol. 27, no. 3 (2007). This research was supported by DHS through the Center for Risk and Economic Analysis of Terrorist Events by grant funding.

[29] This is defined in the TWIC System Security Plan and the DHS Budget Justification to Congress for Fiscal Years 2009 and 2010.

TWIC Program Processes for Ensuring TWIC-Holder Eligibility

TSA is responsible for enrolling TWIC applicants and conducting background checks to ensure that only eligible individuals are granted TWICs.[30] In addition, pursuant to TWIC-related regulations, MTSAregulated facility and vessel operators are responsible for reviewing each individual's TWIC as part of their decision to grant unescorted access to secure areas of their facilities. The Coast Guard is responsible for assessing and enforcing operator compliance with TWIC-related laws and regulations. Described below are key components of each process for ensuring TWIC-holder eligibility.

Enrollment: Transportation workers are enrolled by providing biographic information, such as name, date of birth, and address, and proof of identity documents, and then being photographed and fingerprinted at enrollment centers by trusted agents. A trusted agent is a member of the TWIC team who has been authorized by the Federal Government to enroll transportation workers in the TWIC program and issue TWIC cards.[31] Appendix I summarizes key steps in the enrollment process.

Background checking: TSA conducts background checks on each worker who applies for a TWIC to ensure that individuals who enroll do not pose a security risk to the United States. A worker's potential link to terrorism, criminal history, immigration status, and mental capacity are considered as part of the security threat assessment. Workers have the opportunity to appeal negative results of the threat assessment or request a waiver of certain specified criminal offenses, and immigration or mental capacity standards. Specifically, the TWIC background checking process includes two levels of review.

> *First-level review: Initial automated background checking*. The initial automated background checking process is conducted to determine whether any derogatory information is associated with the name and fingerprints submitted by an applicant during the enrollment process. This check is conducted against the FBI's criminal history records. These records contain information from Federal and state and local sources in the FBI's National Crime Information Center (NCIC) database and the FBI's Integrated Automated Fingerprint Identification System (IAFIS)/Interstate Identification Index (III), which maintain criminal records and related fingerprint submissions. Rather than positively confirming each individual's identity using the submitted fingerprints, the FBI's criminal history records check is a negative identification check, whereby the fingerprints are used to confirm that the associated individual is not on the FBI criminal history list. If an individual is identified as being on the FBI's criminal history list, relevant information is to be forwarded to TSA for adjudication.[32] The check is also conducted against Federal terrorism information from the Terrorist Screening Data base, including the Selectee and No-Fly Lists.[33] To determine an applicant's immigration/citizenship status and eligibility, TSA also runs applicant information against the Systematic Alien Verification for Entitlements (SAVE) system. If the applicant is identified as a U.S.-born citizen with no related derogatory information, the system can approve the issuance of a TWIC with no further review of the applicant or human intervention.

---

[30] TWIC program threat assessment processes include conducting a background check to determine whether each TWIC applicant is a security risk to the United States. These checks, in general, can include checks for criminal history records, immigration status, terrorism databases and watchlists, and records indicating an adjudication of lack of mental capacity, among other things. TSA security threat assessment-related regulations define the term security threat to mean an individual whom TSA determines or suspects of posing a threat to national security; to transportation security; or of terrorism.

[31] Trusted agents are subcontractor staff acquired by Lockheed Martin as part of its support contract with TSA for the TWIC program.

[32] Not all TWIC applicants will have readable fingerprints. As we have previously reported, it is estimated that about 2 percent to 5 percent of people cannot be easily fingerprinted because their fingerprints have become dry or worn from age, extensive manual labor, or exposure to corrosive chemicals (See GAO, *Technology Assessment: Using Biometrics for Border Security*, GAO–03–174 (Washington, D.C.: Nov. 15, 2002).

[33] Pursuant to Homeland Security Presidential Directive 6, dated September 16, 2003, the Terrorist Screening Center—under the administration of the FBI—was established to develop and maintain the U.S. government's consolidated terrorist screening database (the watch list) and to provide for the use of watch-list records during security-related screening processes. The Selectee List contains information on individuals who should receive enhanced screening (*e.g.,* additional physical screening or a hand-search of carryon baggage) before proceeding through the security checkpoint at airports. The No Fly List contains information on individuals who should be precluded from boarding flights. The No Fly and Selectee lists contain applicable records from the FBI Terrorist Screening Center's consolidated database of known or appropriately suspected terrorists.

Second-level review: TSA's Adjudication Center Review. A second-level review is conducted as part of an individual's background check if: (1) the applicant has self-identified themselves to be a non-U.S. citizen or non-U.S.-born citizen or national, or (2) the first-level review uncovers any derogatory information. As such, not all TWIC applicants will be subjected to a second-level review. The second-level review consists of staff at TSA's adjudication center reviewing the applicant's enrollment file.[34]

Card use and compliance: Once a TWIC has been activated and issued, the worker may present his or her TWIC to security officials when he or she seeks unescorted access to a secure area. Currently, visual inspections of TWICs are required for controlling access to secure areas of MTSAregulated facilities and vessels.[35] Approaches for inspecting TWICs using biometric readers at individual facilities and vessels across the nation are being considered as part of a pilot but are not yet required. Pursuant to Coast Guard policy,[36] Coast Guard inspectors are required to verify TWIC cards during annual compliance exams, security spot checks, and in the course of other Coast Guard duties as determined by the Captain of the Port[37] based on risk and resource availability. The Coast Guard's primary means of verification is shifting toward the use of biometric handheld readers with the continued deployment of readers to each of its Sectors and Marine Safety Units.[38] As of December 21, 2010, the Coast Guard reports to have deployed biometric handheld readers to all of its 35 Sectors and 16 Marine Safety Units.

TWIC Regulations and Cost

In August 2006, DHS officials decided, based on industry comment, to implement TWIC through two separate regulations, or rules. The first rule, issued in January 2007, directs the use of the TWIC as an identification credential, or flashpass. The second rule, the card reader rule, is currently under development and is expected to address how the access control technologies, such as biometric card readers, are to be used for confirming the identity of the TWIC holder against the biometric information on the TWIC. On March 27, 2009, the Coast Guard issued an Advance Notice of Proposed Rule Making for the card reader rule.[39]

To inform the rulemaking process, TSA initiated a pilot in August 2008, known as the TWIC reader pilot, to test TWIC-related access control technologies.[40] This pilot is intended to test the technology, business processes, and operational impacts of deploying TWIC readers at secure areas of the marine transportation system. As such, the pilot is expected to test the feasibility and functionality of using TWICs

---

[34] If an applicant has asserted him/herself to be a non-U.S. citizen or non-U.S.-born citizen, TSA staff at the adjudication center are to positively identify the individual by confirming aspects of the individual's biographic information, inclusive of their alien registration number and other physical descriptors, against available databases. For those individuals, TSA requires that at least one of the documents provided as proof of identity demonstrates immigration status or United States citizenship. According to TWIC officials, the program is able to validate immigration status and citizenship-related documents required of noncitizens and non-U.S.-born citizens—such as certificates of naturalization—with the originating source. For individuals with derogatory information, staff at the adjudication center reviews each applicant's file to determine if the derogatory information accurately applies to the individual or includes disqualifying information.

[35] Coast Guard regulations require that such an inspection include: (1) a match of the photo on the TWIC to the individual presenting the TWIC, (2) verification that the TWIC has not expired, and (3) a visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

[36] See United States Coast Guard, Commandant Instruction Manual 16601.1: *Coast Guard Transportation Worker Identification Credential (TWIC) Verification and Enforcement Guide* (Washington, D.C.: Oct. 10, 2008).

[37] The Captain of the Port is the Coast Guard officer designated by the Commandant to enforce within his or her respective areas port safety and security and marine environmental protection regulations, including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities.

[38] Coast Guard Sectors run all Coast Guard missions at the local and port levels, such as search and rescue, port security, environmental protection, and law enforcement in ports and surrounding waters, and oversee a number of smaller Coast Guard units, including small cutters and small-boat stations.

[39] 74 Fed. Reg. 13360 (2009). An advanced notice of proposed rulemaking is published in the *Federal Register* and contains notices to the public of the proposed issuance of rules and regulations. The purpose of this advanced notice of proposed rulemaking was to encourage the discussion of potential TWIC reader requirements prior to the rulemaking process.

[40] The pilot initiation date is based on the first date of testing identified in the TWIC pilot schedule. This date is not inclusive of time taken for planning the pilot prior to the first test. The SAFE Port Act required the pilot to commence no later than 180 days after the date of enactment (Oct. 13, 2006) of the SAFE Port Act. See GAO–06–982.

with biometric card readers within the maritime environment. After the pilot has concluded, a report on the findings of the pilot is expected to inform the development of the card reader rule. DHS currently estimates that a notice of proposed rulemaking will be issued late in calendar year 2011 and that the final rule will be promulgated no earlier than the end of calendar year 2012.

According to agency officials, from Fiscal Years 2002 through 2010, the TWIC program had funding authority totaling $420 million. In issuing the credential rule, DHS estimated that implementing the TWIC program could cost the Federal Government and the private sector a combined total of between $694.3 million and $3.2 billion over a 10-year period. However, these figures did not include costs associated with implementing and operating readers.[41] Appendix II contains additional program funding details.

Standards for Internal Control

Standards for Internal Control in the Federal Government underscores the need for developing effective controls for meeting program objectives and complying with applicable regulations.[42] Effective internal controls provide for an assessment of the risks the agency faces from both internal and external sources. Once risks have been identified, they should be analyzed for their possible effect. Management then has to decide upon the internal control activities required to mitigate those risks and achieve the objectives of efficient and effective operations. As part of this effort, management should design and implement internal controls based on the related cost and benefits.

In addition, internal control standards highlight the need for the following:

- capturing information needed to meet program objectives;
- designing controls to assure that ongoing monitoring occurs in the course of normal operations;
- determining that relevant, reliable, and timely information is available for management decisionmaking purposes;
- conducting reviews and testing of development and modification activities before placing systems into operation;
- recording and communicating information to management and others within the entity who need it and in a form and within a time-frame that enables them to carry out their internal control and other responsibilities; and
- designing internal controls to provide reasonable assurance that compliance with applicable laws and regulations is being achieved, and provide appropriate supervisory review of activities to help provide oversight of operations. This includes designing and implementing appropriate supervisory review activities to help provide oversight and analyzing data to compare trends in actual performance to expected results to identify any areas that may require further inquiries or corrective action.

Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. An internal control weakness is a condition within an internal control system worthy of attention. A weakness, therefore, may represent a perceived, potential, or real shortcoming, or an opportunity to strengthen internal controls to provide a greater likelihood that the entity's objectives will be achieved.

Internal Control Weaknesses in DHS's Biometric Transportation ID Program Hinder Efforts to Ensure Security Objectives Are Fully Achieved

DHS has established a system of TWIC-related processes and controls. However, internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limit the program's ability to provide reasonable assurance that access to secure areas of MTSA-regulated facilities is restricted to qualified individuals. Specifically, internal controls[43] in the enrollment and background checking processes are not designed to provide reasonable assurance that: (1) only qualified individuals can acquire TWICs; (2) adjudicators follow a process with clear cri-

[41] See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Final Rule, 72 Fed. Reg. 3492, 3571 (2007).

[42] GAO/AIMD–00–21.3.1.

[43] In accordance with *Standards for Internal Control in the Federal Government*, the design of the internal controls is to be informed by identified risks the program faces from both internal and external sources; the possible effect of those risks; control activities required to mitigate those risks; and the cost and benefits of mitigating those risks.

teria for applying discretionary authority when applicants are found to have extensive criminal convictions; or (3) once issued a TWIC, TWIC holders have maintained their eligibility. To meet the stated program mission needs, TSA designed TWIC program processes to facilitate the issuance of TWICs to maritime workers. However, TSA did not assess the internal controls designed and in place to determine whether they provided reasonable assurance that the program could meet defined mission needs for limiting access to only qualified individuals. Further, internal control weaknesses in TWIC enrollment, background checking, and use could have contributed to the breach of selected MTSA-regulated facilities during covert tests conducted by our investigators.

TWIC Program Controls Are Not Designed to Provide Reasonable Assurance That Only Qualified Applicants Can Acquire TWICs

DHS has established a system of TWIC-related processes and controls that as of April 2011 has resulted in TWICs being denied to 1,158 applicants based on a criminal offense, criminal immigration offense, or invalid immigration status.[44] However, the TWIC program's internal controls for positively identifying an applicant, arriving at a security threat determination for that individual, and approving the issuance of a TWIC, are not designed to provide reasonable assurance that only qualified applicants can acquire TWICs.[45] Assuring the identity and qualifications of TWIC-holders are two of the primary benefits that the TWIC program is to provide MTSA-regulated facility and vessel operators making access control decisions. If an individual presents an authentic TWIC acquired through fraudulent means when requesting access to the secure areas of a MTSA-regulated facility or vessel, the cardholder is deemed not to be a security threat to the maritime environment because the cardholder is presumed to have met TWIC-related qualifications during a background check. In such cases, these individuals could better position themselves to inappropriately gain unescorted access to secure areas of a MTSAregulated facility or vessel.[46]

As confirmed by TWIC program officials, there are ways for an unqualified individual to acquire an authentic TWIC. According to TWIC program officials, to meet the stated program purpose, TSA's focus in designing the TWIC program was on facilitating the issuance of TWICs to maritime workers. However, TSA did not assess internal controls prior to implementing the program. Further, prior to fielding the program, TSA did not conduct a risk assessment of the TWIC program to identify program risks and the need for controls to mitigate existing risks and weaknesses, as called for by internal control standards. Such an assessment could help provide reasonable assurance that control weaknesses in one area of the program do not undermine the reliability of other program areas or impede the program from meeting mission needs. TWIC program officials told us that control weaknesses were not addressed prior to initiating the TWIC program because they had not previously identified them, or because they would be too costly to address. However, officials did not provide documentation to support their cost concerns and told us that they did not complete an assessment that accounted for whether the program could achieve defined mission needs without implementing additional or compensating controls to mitigate existing risks, or the risks associated with not correcting for existing internal control weaknesses.

Our investigators conducted covert tests at enrollment center(s) to help test the rigor of the TWIC enrollment and background checking processes. The investigators fully complied with the enrollment application process. They were photographed and fingerprinted, and asserted themselves to be U.S.-born citizens.[47] The investigators were successful in obtaining authentic TWIC cards despite going through the background-checking process. Not having internal controls designed to provide reasonable assurance that the applicant has: (1) been positively identified, and (2) met all

---

[44] TSA further reports that as of April 2011 there have been 34,503 cases out of 1,841,122 enrollments, or 1.9 percent of TWIC enrollments, where enrollees have not been approved for a TWIC because TSA has identified that the enrollees have at least one potentially disqualifying criminal offense, criminal immigration offense, or invalid immigration status, and the enrollee did not respond to an initial determination of threat assessment. Under the TWIC vetting process, an applicant that receives an initial determination of threat assessment is permitted to provide additional information to respond to or challenge the determination, or to request a waiver for the disqualifying condition, and subsequently be granted a TWIC.

[45] For the purposes of this report, routinely is defined as a process being consistently applied in accordance with established procedure so as to render consistent results.

[46] The TWIC program requires individuals to both hold a TWIC and be authorized to be in the secure area by the owner/operator in order to gain unescorted access to secure areas of MTSA-regulated facilities and vessels.

[47] The details related to the means used by the investors in the tests could not be detailed here because they were deemed sensitive security information by TSA.

TWIC eligibility requirements, including not posing a security threat to MTSA-regulated facilities and vessels, could have contributed to the investigators' successes. Specifically, we identified internal control weaknesses in the following three areas related to ensuring that only qualified applicants are able to obtain a TWIC.

Controls to identify the use of potentially counterfeit identity documents are not used to inform background checking processes. As part of TWIC program enrollment, a trusted agent is to review identity documents for authenticity and use an electronic authentication device to assess the likelihood of the document being counterfeit.[48] According to TWIC program officials, the trusted agent's review of TWIC applicant identity documents and the assessment provided by the electronic authentication device are the two steps intended to serve as the primary controls for detecting whether an applicant is presenting counterfeit identity documents. Additionally, the electronic device used to assess the authenticity of identification credentials renders a score on the likelihood of the document being authentic and produces an assessment report in support of the score. Assessing whether the applicant's credential is authentic is one source of information for positively identifying an applicant. Our investigators provided counterfeit or fraudulently acquired documents, but they were not detected.

However, the TWIC program's background checking processes are not designed to routinely consider the results of controls in place for assessing whether an applicant's identity documents are authentic. For example, assessments of document authenticity made by a trusted agent or the electronic document authentication device as part of the enrollment process are not considered as part of the first-level background check. Moreover, TWIC program officials agree that this is a program weakness. As of December 1, 2010, approximately 50 percent of TWICs were approved after the first-level background check without undergoing further review.[49] As an initial step toward addressing this weakness, and in response to our review, TWIC program officials told us that since April 17, 2010, the comments provided at enrollment by trusted agents have been sent to the Screening Gateway—a TSA system for aggregating threat assessment data. However, this change in procedure does not correct the internal control weaknesses we identified.[50] Attempts to authenticate copies of documents are limited because it is not possible to capture all of the security features when copies of the identity documents are recorded, such as holograms or color-shifting ink. Using information on the authenticity of identity documents captured during enrollment to inform the background check could help TSA better assess the reliability and authenticity of such documents provided at enrollment.

Controls related to the legal status of self-reported U.S.-born citizens or nationals.[51] The TWIC program does not require that applicants claiming to be U.S.-born citizens or nationals provide identity documents that demonstrate proof of citizenship, or lawful status in the United States. See appendix III for the list of documents U.S.-born citizens or nationals must select from and present when applying for a TWIC.[52] For example, an applicant could elect to provide one document, such a U.S. passport, which, according to TSA officials, serves as proof of U.S. citizenship or proof of nationality. However, an applicant could elect to submit documents that do not provide proof of citizenship. As of December 1, 2010, nearly 86 percent of ap-

---

[48] As designed, the TWIC program's enrollment process relies on a trusted agent—a contract employee—to collect an applicant's identification information. The trusted agent is provided basic training on how to detect a fraudulent document. The training, for example, consists of checking documents for the presence of a laminate that is not peeling, typeset that looks legitimate, and seals on certain types of documents.

[49] Of the 1,697,160 enrollments approved for a TWIC, 852,540 were approved using TSA's automated process as part of the first-level background check without undergoing further review.

[50] Details from this section were removed because the agency deemed them sensitive security information.

[51] National means a citizen of the United States or a noncitizen owing permanent allegiance to the United States. In general, U.S.-born nationals who are not U.S. citizens at birth are individuals born in an outlying possession of the United States. Details from this section were removed because the agency deemed them sensitive security information.

[52] Various identity documents can be provided by U.S.-born citizens or nationals when applying for a TWIC. For certain documents, such as an unexpired U.S. passport, TSA requires one document as a proof of identity. For other documents, such as a Department of Transportation Medical Card or United States Military Dependents Identification Card, TSA requires that TWIC applicants provide two identity documents from a designated list, with one being a government-issued photo identification.

proved TWIC enrollments were by self-identified United States citizens or nationals asserting that they were born in the United States or a United States territory.[53]

Verifying a U.S.-born citizen's identity and related lawful status can be costly and is a challenge faced by U.S. Government programs such as passports.[54] However, reaching an accurate determination of a TWIC applicant's potential security threat in meeting TWIC mission needs is dependant on positively identifying the applicant. Given such potential cost constraints, consistent with internal control standards, identifying alternative mechanisms to positively identify individuals to the extent that the benefits exceed the costs and TWIC program mission needs are met could enhance TSA's ability to positively identify individuals and reduce the likelihood that criminals or terrorists could acquire a TWIC fraudulently.

Controls are not in place to determine whether an applicant has a need for a TWIC.[55] Regulations governing the TWIC program security threat assessments require applicants to disclose their job description and location(s) where they will most likely require unescorted access, if known, and the name, telephone number, and address of the applicant's current employer(s) if the applicant works for an employer that requires a TWIC.[56] However, TSA enrollment processes do not require that this information be provided by applicants. For example, when applying for a TWIC, applicants are to certify that they may need a TWIC as part of their employment duties. However, the enrollment process does not request information on the location where the applicant will most likely require unescorted access, and enrollment processes include asking the applicant if they would like to provide employment information, but informing the applicant that employer information is not required.

While not a problem prior to implementing the TWIC program, according to TSA officials, a primary reason for not requiring employer information be captured by applicant processes is that many applicants do not have employers, and that many employers will not accept employment applications from workers who do not already have a TWIC. However, TSA could not provide statistics on: (1) how many individuals applying for TWICs were unemployed at the time of their application; or (2) a reason why the TWIC-related regulation does not prohibit employers from denying employment to non-TWIC holders who did not previously have a need for a TWIC. Further, according to TSA and Coast Guard officials, industry was opposed to having employment information verified as part of the application process, as industry representatives believed such checks would be too invasive and time-consuming. TSA officials further told us that confirming this information would be too costly.

We recognize that implementing mechanisms to capture this information could be time-consuming and involve additional costs. However, collecting information on present employers or operators of MTSA-regulated facilities and vessels to be accessed by the applicant, to the extent that the benefits exceed the costs and TWIC program mission needs are met, could help ensure TWIC program mission needs are being met, and serve as a barrier to individuals attempting to acquire an authentic TWIC through fraudulent means. Therefore, if TSA determines that implementing such mechanisms are, in fact, cost prohibitive, identifying and implementing appropriate compensating controls could better position TSA to positively identify the

---

[53] As of December 1, 2010, TSA reported that 1,697,160 TWIC enrollments have been approved, of which 1,457,337 were self-identified United States citizens or nationals asserting that they were born in the United States or in a United States territory.

[54] See GAO, *State Department: Significant Vulnerabilities in the Passport Issuance Process*, GAO–09–681T (Washington, D.C.: May 5, 2009) and State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts, GAO–05–477 (Washington, D.C.: May 20, 2005).

[55] TWIC is unlike other federally-sponsored access control credentials, such as the Department of Defense's Common Access Card—the agencywide standard identification card—for which sponsorship by an employer is required. For these Federal credentialing programs, employer sponsorship begins with the premise that an individual is known to need certain access as part of their employment. Further, the employing agency is to conduct a background investigation on the individual and has access to other personal information, such as prior employers, places of residency, and education, which they may confirm as part of the employment process and use to establish the individual's identity.

[56] Implementing regulations at 49 C.F.R. § 1572.17 require that when applying for or renewing a TWIC, the applicant provide, among other information: (1) the reason that the applicant requires a TWIC, including, as applicable, the applicant's job description and the primary facility, vessel, or maritime port location(s) where the applicant will most likely require unescorted access, if known; (2) the name, telephone number, and address of the applicant's current employer(s) if the applicant works for an employer that requires a TWIC; and (3) if the applicant works for an employer that does not require possession of a TWIC, does not have a single employer, or is self-employed, the primary vessel or port location(s) where the applicant requires unescorted access, if known. The regulation states that this information is required to establish eligibility for a TWIC and that TSA is to review the applicant information as part of the intelligence-related check.

TWIC applicant. Not taking any action increases the risk that individuals could gain unescorted access to secure areas of MTSAregulated facilities and vessels.

As of September 2010, TSA's background checking process had identified no instances of nonimmigration-related document or identity fraud. This is in part because of previously discussed weaknesses in TWIC program controls for positively identifying applicants, and the systems and procedures the TWIC program relies on not being designed to effectively monitor for such occurrences, in accordance with internal control standards. Though not an exhaustive list, through a review of Coast Guard reports and publicly available court records, we identified five court cases where the court documents indicate that illegal immigrants acquired, or in one of the cases sought to acquire, an authentic TWIC through fraudulent activity such as providing fraudulent identity information and, in at least one of the cases and potentially up to four, used the TWIC to access secure areas of MTSA-regulated facilities. Four of these cases were a result of, or involved, United States Immigration and Customs Enforcement efforts after individuals had acquired, or sought to acquire, a TWIC. As of September 2010, the program's background checking process identified 18 instances of potential fraud out of the approximately 1,676,000 TWIC enrollments. These instances all involved some type of fraud related to immigration.[57] The 18 instances of potential fraud were identified because the 18 individuals asserted themselves to be non-U.S.- born applicants and, unlike processes in place for individuals asserting to be U.S.-born citizens, TSA's background checking process includes additional controls to validate such individuals' identities. For example, TSA requires that at least one of the documents provided by such individuals at enrollment show proof of their legal status and seeks to validate each non-U.S.-born applicant's identity with the U.S. Citizenship and Immigration Services.

Internal control standards highlight the need for capturing information needed to meet program objectives; ensuring that relevant, reliable, and timely information is available for management decisionmaking purposes; and providing reasonable assurance that compliance with applicable laws and regulations is being achieved.[58] Conducting a control assessment of the TWIC program's processes to address existing weaknesses could enhance the TWIC program's ability to prevent and detect fraud and positively identify TWIC applicants. Such an assessment could better position DHS in strengthening the program to ensure it achieves its objectives in controlling access to MTSA-regulated facilities and vessels.

TWIC Program Controls Are Not Designed to Require Adjudicators to Follow a Process with Clear Criteria for Applying Discretionary Authority When Applicants Are Found to Have Extensive Criminal Convictions

Being convicted of a felony does not automatically disqualify a person from being eligible to receive a TWIC; however, prior convictions for certain crimes are automatically disqualifying. Threat assessment processes for the TWIC program include conducting background checks to determine whether each TWIC applicant poses a security threat.[59] Some of these offenses, such as espionage or treason, would permanently disqualify an individual from obtaining a TWIC. Other offenses, such as murder or the unlawful possession of an explosive device, while categorized as permanent disqualifiers, are also eligible for a waiver under TSA regulations and might not permanently disqualify an individual from obtaining a TWIC if TSA determines upon subsequent review that an applicant does not represent a security threat.[60] Table 1 presents examples of disqualifying criminal offenses set out in statute and implementing regulations for consideration as part of the adjudication process.

---

[57] According to TSA, as of September 8, 2010, a total of 18 TWIC applicants were issued an Initial Determination of Threat Assessment for invalid immigration documents. Upon submission to the U.S. Citizenship and Immigration Services, the documentation was reported to be altered or counterfeit. Of these 18 instances, only 1 applicant submitted additional documentation following an Initial Determination of Threat Assessment to challenge TSA's determination. The single applicant was subsequently awarded a TWIC.

[58] GAO/AIMD–00–21.3.1.

[59] These checks, in general, can include checks for criminal history records, immigration status, terrorism databases and watchlists, and records indicating an adjudication of a lack of mental capacity, among other things. As defined in TSA implementing regulations, the term security threat means an individual whom TSA determines or suspects of posing a threat to national security; to transportation security; or of terrorism. 49 C.F.R. § 1570.3.

[60] These permanent disqualifying offenses for which no waiver can be issued include espionage, sedition, treason, a Federal crime of terrorism, or conspiracy to commit any of these offenses.

Table 1.—Examples of Disqualifying Offenses for TWIC Eligibility

Permanent disqualifying offenses [a]	Permanent disqualifying offenses that can be waived [b]	Interim disqualifying offenses [c]
Espionage	Murder	Bribery
Sedition	Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device	Smuggling
Treason	A crime involving a transportation security incident	Arson
A federal crime of terrorism	Making any threat concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportation system, or an infrastructure facility	Extortion
		Robbery

Source: GAO analysis of regulations and TSA.
Notes: See appendix IV for a list of all disqualifying offenses.
[a] Permanent disqualifying offenses are offenses defined in 49 C.F.R. 1572.103(a) for which no waiver can be granted under 49 C.F.R. 1515.7(a)(i).
[b] Permanent disqualifying offenses that can be waived are offenses defined in 49 C.F.R. 1572.103(a) for which a waiver can be granted in accordance with 49 C.F.R. 1515.7(a)(i). Applicants with certain permanent criminal offenses and all interim disqualifying criminal offenses may request a waiver of their disqualification. TSA regulations provide that in determining whether to grant a waiver, TSA will consider: (1) the circumstances of the disqualifying act or offense; (2) restitution made by the applicant; (3) any Federal or state mitigation remedies; (4) court records or official medical release documents indicating that the applicant no longer lacks mental capacity; and (5) other factors that indicate the applicant does not pose a security threat warranting denial of a hazardous materials endorsement or TWIC.
[c] Interim disqualifying offenses are offenses defined in 49 C.F.R. 1572.103(b) for which the applicant has either been: (1) convicted, or found not guilty by reason of insanity, within a 7-year period preceding the TWIC application, or (2) incarcerated for within a 5-year period preceding the TWIC application.

TSA also has the authority to add to or modify the list of interim disqualifying crimes. Further, in determining whether an applicant poses a security threat, TSA officials stated that adjudicators have the discretion to consider the totality of an individual's criminal record, including criminal offenses not defined as a permanent or interim disqualifying criminal offenses, such as theft or larceny.[61] More specifically, TSA's implementing regulations provide, in part, that with respect to threat assessments, TSA may determine that an applicant poses a security threat if the search conducted reveals extensive foreign or domestic criminal convictions, a conviction for a serious crime not listed as a permanent or interim disqualifying offense, or a period of foreign or domestic imprisonment that exceeds 365 consecutive days. Thus, if a person was convicted of multiple crimes, even if each of the crimes were not in and of themselves disqualifying, the number and type of convictions could be disqualifying.

Although TSA has the discretion and authority to consider criminal offenses not defined as a disqualifying offense, such as larceny and theft, and periods of imprisonment, TSA has not developed a definition for what extensive foreign or domestic criminal convictions means, or developed guidance to ensure that adjudicators apply this authority consistently in assessing the totality of an individual's criminal record. For example, TSA has not developed guidance or benchmarks for adjudicators to consistently apply when reviewing TWIC applicants with extensive criminal convictions but no disqualifying offense. This is particularly important given TSA's reasoning for including this authority in TWICrelated regulation. Specifically, TSA noted that it understands that the flexibility this language provides must be used cautiously and on the basis of compelling information that can withstand judicial review. They further noted that the decision to determine whether an applicant poses a threat under this authority is largely a subjective judgment based on many facts and circumstances.

While TSA does not track metrics on the number of TWICs provided to applicants with specific criminal offenses not defined as disqualifying offenses, as of September 8, 2010, the agency reported 460,786 cases where the applicant was approved, but had a criminal record based on the results from the FBI. This represents approximately 27 percent of individuals approved for a TWIC at the time. In each of these cases, the applicant had either a criminal offense not defined as a disqualifying offense or an interim disqualifying offense that was no longer a disqualification based on conviction date or the applicant's release date from incarceration. Consequently, based on TSA's background checking procedures, all of these cases would have been reviewed by an adjudicator for consideration as part of the second-level background

[61] The U.S. government's Adjudicative Desk Reference, used in adjudicating security clearances, states that multiple criminal offenses indicate intentional continuing behavior that raises serious questions about a person's trustworthiness and judgment.

check because derogatory information had been identified. As such, each of these cases had to be examined and a judgment had to be made as to whether to deny an applicant a TWIC based on the totality of the offenses contained in each applicant's criminal report.

While there were 460,786 cases where the applicant was approved, but had a criminal record, TSA reports to have taken steps to deny 1 TWIC applicant under this authority. However, in the absence of guidance for the application of this authority, it is not clear how TSA applied this authority in approving the 460,786 applications and denying the 1. Internal control standards call for controls and other significant events to be clearly documented in directives, policies, or manuals to help ensure operations are carried out as intended.

According to TSA officials, the agency has not implemented guidance for adjudicators to follow on how to apply this discretion in a consistent manner because they are confident that the adjudicators would, based on their own judgment, identify all applicants where the authority to deny a TWIC based on the totality of all offenses should be applied. However, in the absence of criteria, we were unable to analyze or compare how the approximately 30 adjudicators who are assigned to the TWIC program at any given time made determinations about TWIC applicants with extensive criminal histories. Given that 27 percent of TWIC holders have been convicted of at least one nondisqualifying offense, defining what extensive criminal convictions means and developing guidance or criteria for how adjudicators should apply this discretionary authority could help provide TSA with reasonable assurance that applications are consistently adjudicated. Defining terms and developing guidance is consistent with internal control standards.

TWIC Program Controls Are Not Designed to Provide Reasonable Assurance That TWIC Holders Have Maintained Their Eligibility Once Issued TWICs

DHS's defined mission needs for TWIC include identifying individuals who fail to maintain their eligibility requirements once issued a TWIC, and immediately revoking the individual's card privileges. Pursuant to TWICrelated regulations, an individual may be disqualified from holding a TWIC and be required to surrender the TWIC to TSA for failing to meet certain eligibility criteria related to, for example, terrorism, crime, and immigration status. However, weaknesses exist in the design of the TWIC program's internal controls for identifying individuals who fail to maintain their eligibility that make it difficult for TSA to provide reasonable assurance that TWIC holders continue to meet all eligibility requirements.

Controls are not designed to determine whether TWIC holders have committed disqualifying crimes at the Federal or state level after being granted a TWIC. TSA conducts a name-based check of TWIC holders against Federal wants [62] and warrants on an ongoing basis. According to FBI and TSA officials, policy and statutory provisions hamper the program from running the broader FBI fingerprint-based check using the fingerprints collected at enrollment on an ongoing basis. More specifically, because the TWIC background check is considered to be for a noncriminal justice purpose,[63] to conduct an additional fingerprint-based check as part of an ongoing TWIC background check, TSA would have to collect a new set of fingerprints from the TWIC-holder,[64] if the prints are more than 1 year old, and submit those prints to the FBI each time they want to assess the TWIC-holder's criminal history. According to TSA officials, it would be cost prohibitive to run the fingerprint-based check on an ongoing basis, as TSA would have to pay the FBI $17.25 per check.

Although existing policies may hamper TSA's ability to check FBI-held fingerprint-based criminal history records for the TWIC program, TSA has not explored alternatives for addressing this weakness, such as informing facility and port operators of this weakness and identifying solutions for leveraging existing state criminal history information, where available. For instance, state maritime organizations may have other mechanisms at their disposal for helping to identify TWIC-holders

---

[62] Federal wants generally consist of information on wanted persons, or individuals, for whom Federal warrants are outstanding.

[63] Under the National Crime Prevention and Privacy Compact Act of 1998 (Pub. L. No. 105-251, 112 Stat. 1870, 1874 (1998) (codified as amended at 42 U.S.C. §§ 14601–14616)), which established an infrastructure by which states and other specified parties can exchange criminal records for noncriminal justice purposes authorized under Federal or state law, the term noncriminal justice purposes means uses of criminal history records for purposes authorized by Federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

[64] Under the 1998 Act, subject fingerprints or other approved forms of positive identification must be submitted with all requests for criminal history record checks for noncriminal justice purposes.

who may no longer meet TWIC qualification requirements. Specifically, laws governing the maritime environment in New York and New Jersey provide for credentialing authorities being notified if licensed or registered longshoremen have been arrested. Further, other governing entities, such as the State of Florida and the Alabama State Port Authority, have access to state-based criminal records checks. While TSA may not have direct access to criminal history records, TSA could compensate for this control weakness, for example, by leveraging existing mechanisms available to maritime stakeholders across the country to better ensure that only qualified individuals retain TWICs.

Controls are not designed to provide reasonable assurance that TWIC holders continue to meet immigration status eligibility requirements. If a TWIC holder's stated period of legal presence in the United States is about to expire or has expired, the TWIC program does not request or require proof from TWIC holders to show that they continue to maintain legal presence in the United States. Additionally, although they have the regulatory authority to do so, the program does not issue TWICs for a term less than 5 years to match the expiration of a visa. Instead, TSA relies on: (1) TWIC holders to self-report if they no longer have legal presence in the country, and (2) employers to report if a worker is no longer legally present in the country.[65] As we have previously reported, government programs for granting benefits to individuals face challenges in confirming an individual's immigration status.[66] TWIC program officials stated that the program uses a United States Citizenship and Immigration Services system during the background checking process prior to issuing a TWIC as a method for confirming the legal status of non-U.S. citizens.[67] TSA has not, however, consistent with internal control standards, implemented alternative controls to compensate for this limitation and provide reasonable assurance that TWIC holders remain eligible. For instance, the TWIC program has not compensated for this limitation by: (1) using its authority to issue TWICs with shorter expiration dates to correspond with each individual's legal presence, or (2) updating the TWIC system to systematically suspend TWIC privileges for individuals who no longer meet immigration eligibility requirements until they can provide evidence of continued legal presence.[68]

TWIC program officials stated that implementing these compensating measures would be too costly, but they have not conducted an assessment to identify the costs of implementing these controls, or determined if the benefits of mitigating related security risks would outweigh those costs, consistent with internal control standards. Not implementing such measures could result in a continued risk of individuals no longer meeting TWIC legal presence requirements continuing to hold a federally issued identity document and gaining unescorted access to secure areas of MTSAregulated facilities and vessels.[69] Thus, implementing compensating measures, to the extent that the benefits outweigh the costs and meet the program's defined mission needs, could provide TSA, the Coast Guard, and MTSA-regulated

---

[65] TWIC-related regulations provide, for example, that individuals disqualified from holding a TWIC for immigration status reasons must surrender the TWIC to TSA. In addition, the regulations provide that TWICs are deemed to have expired when the status of certain lawful nonimmigrants with a restricted authorization to work in the United States (*e.g.,* H–1B1 Free Trade Agreement) expires, the employer terminates the employment relationship with such an applicant, or such applicant otherwise ceases working for the employer, regardless of the date on the face of the TWIC. Upon the expiration of such nonimmigrant status for an individual who has a restricted authorization to work in the United States, the employer and employee both have related responsibilities—the employee is required to surrender the TWIC to the employer, and the employer is required to retrieve the TWIC and provide it to TSA. According to TSA officials, the TWIC program could not provide a count of the total number of TWIC holders whose employers reported that the TWIC holders no longer have legal status, as they do not track this information.

[66] See, for example, GAO, *EmploymentVerification: Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO–11–146 (Washington, D.C.: Dec. 17, 2010), and *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts*, GAO–05–813 (Washington, D.C.: Aug. 31, 2005).

[67] Details from this section were removed because the agency deemed them sensitive security information.

[68] The TWIC program accepts various documents, such as visas, Interim Employment Authorizations, and form I–94 Arrival and Departure Records, as evidence of legal presence in the United States.

[69] TWIC is a federally issued identity document that can be used as proof of identity for nonmaritime activities, such as boarding airplanes at United States airports and certain Department of Defense facilities in accordance with Department of Defense policy, Directive-Type Memorandum (DTM) 09–012, "Interim Policy Guidance for DOD Physical Access Control," dated December 8, 2009.

stakeholders with reasonable assurance that each TWIC holder continues to meet TWIC-related eligibility requirements.

Internal Control Weaknesses in TWIC Enrollment, Background Checking, and Use Could Have Contributed to Breach of MTSA-Regulated Ports

As of January 7, 2011, the Coast Guard reports that it has identified 11 known attempts to circumvent TWIC requirements for gaining unescorted access to MTSA-regulated areas by presenting counterfeit TWICs. The Coast Guard further reports to have identified 4 instances of individuals presenting another person's TWIC as their own in attempts to gain access. Further, our investigators conducted covert tests to assess the use of TWIC as a means for controlling access to secure areas of MTSA-regulated facilities. During covert tests of TWIC at several selected ports, our investigators were successful in accessing ports using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases (*i.e.,* reasons for requesting access).[70] Our investigators did not gain unescorted access to a port where a secondary port specific identification was required in addition to the TWIC.

In response to our covert tests, TSA and Coast Guard officials stated that, while a TWIC card is required for gaining unescorted access to secure areas of a MTSA-regulated facility, the card alone is not sufficient. These officials stated that the cardholder is also required to present a business case, which security officials at facilities must consider as part of granting the individual access. In addition, according to DHS's Screening Coordination Office, a credential is only one layer of a multi-layer process to increase security. Other layers of security might include onsite law enforcement, security personnel, cameras, locked doors and windows, alarm systems, gates, and turnstiles. Thus, a weakness in the implementation of TWIC will not guarantee access to the secure areas of a MTSA-regulated port or facility.

However, as our covert tests demonstrated, having an authentic TWIC and a legitimate business case were not always required in practice. The investigators' possession of TWIC cards provided them with the appearance of legitimacy and facilitated their unescorted entry into secure areas of MTSA-regulated facilities and ports at multiple locations across the country. If individuals are able to acquire authentic TWICs fraudulently, verifying the authenticity of these cards with a biometric reader will not reduce the risk of undesired individuals gaining unescorted access to the secure areas of MTSA-regulated facilities and vessels.

Given existing internal control weaknesses, conducting a control assessment of the TWIC program's processes to address existing weaknesses could enhance the TWIC program's ability to prevent and detect fraud and positively identify TWIC applicants. Such an assessment could better position DHS in strengthening the program to ensure it achieves its objectives in controlling unescorted access to MTSA-regulated facilities and vessels. It could also help DHS identify and implement the minimum controls needed to: (1) positively identify individuals, (2) provide reasonable assurance that control weaknesses in one area of the program would not undermine the reliability of other program areas or impede the program from meeting mission needs, and (3) provide reasonable assurance that the threat assessments are based on complete and accurate information. Such actions would be consistent with internal control standards, which highlight the need for capturing information needed to meet program objectives; determining that relevant, reliable, and timely information is available for management decision-making purposes; and designing internal controls to provide reasonable assurance that compliance with applicable laws and regulations is being achieved, as part of implementing effective controls. Moreover, our prior work on internal controls has shown that management should design and implement internal controls based on the related costs and benefits and continually assess and evaluate its internal controls to assure that the controls being used are effective and updated when necessary.[71]

---

[70] Existing vulnerabilities with TWIC to date have included, for example, problems with deteriorating TWIC card security features. Cards fading and delaminating have been reported by stakeholders across the country from places such as New York, Virginia, Texas, and California, with a range of climate conditions. According to stakeholders, these problems make it difficult for security guards to distinguish an authentic TWIC that is faded from a fraudulent TWIC. TSA and the Coast Guard have also received reports of problems with the card's chip or antenna connection not working from locations where TWICs are being used with readers. The total number of damaged TWICs with a damaged chip or antenna is unknown because TWICs are not required to be used with readers.

[71] GAO/AIMD–00–21.3.1.

TWIC's Effectiveness at Enhancing Security Has Not BeenAssessed, and the Coast Guard Lacks the Ability to Assess Trends in TWIC Compliance

The TWIC program is intended to improve maritime security by using a federally sponsored credential to enhance access controls to secure areas at MTSA-regulated facilities and vessels, but DHS has not assessed the program's effectiveness at enhancing security. In addition, Coast Guard's approach for monitoring and enforcing TWIC compliance nationwide could be improved by enhancing its collection and assessment of related maritime security information. For example, the Coast Guard tracks TWIC program compliance, but the processes involved in the collection, cataloguing, and querying of information cannot be relied on to produce the management information needed to assess trends in compliance with the TWIC program or associated vulnerabilities.

TWIC Has Not Been Assessed to Measure Effectiveness at Enhancing Security

DHS asserted in its 2009 and 2010 budget submissions that the absence of the TWIC program would leave America's critical maritime port facilities vulnerable to terrorist activities.[72] However, to date, DHS has not assessed the effectiveness of TWIC at enhancing security or reducing risk for MTSA-regulated facilities and vessels. Such assessments are consistent with DHS's National Infrastructure Protection Plan, which recognizes that metrics and other evaluation procedures should be used to measure progress and assess the effectiveness of programs designed to protect key assets.[73] Further, DHS has not demonstrated that TWIC, as currently implemented and planned with readers, is more effective than prior approaches used to limit access to ports and facilities, such as using facility specific identity credentials with business cases. According to TSA and Coast Guard officials, because the program was mandated by Congress as part of MTSA, DHS did not conduct a risk assessment to identify and mitigate program risks prior to implementation. Further, according to these officials, neither the Coast Guard nor TSA analyzed the potential effectiveness of TWIC in reducing or mitigating security risk—either before or after implementation—because they were not required to do so by Congress. Rather, DHS assumed that the TWIC program's enrollment and background checking procedures were effective and would not allow unqualified individuals to acquire and retain authentic TWICs.

The internal control weaknesses that we discuss earlier in the report, as well as the results of our covert tests of TWIC use, raise questions about the effectiveness of the TWIC program. According to the Coast Guard official responsible for conducting assessments of maritime risk, it may now be possible to assess TWIC effectiveness and the extent to which, or if, TWIC use could enhance security using current Maritime Security Risk Analysis Model (MSRAM) data. Since MSRAM's deployment in 2005, the Coast Guard has used its MSRAM to help inform decisions on how to best secure our nation's ports and how to best allocate limited resources to reduce terrorist risks in the maritime environment.[74] Moreover, as we have previously reported, Congress also needs information on whether and in what respects a program is working well or poorly to support its oversight of agencies and their budgets, and agencies' stakeholders need performance information to accurately

---

[72] See DHS, DHS Exhibit 300 Public Release BY10/TSA—Transportation Worker Identification Credentialing (TWIC) (Washington, D.C.: Apr. 17, 2009) and DHS Exhibit 300 Public Release BY09/TSA—Transportation Worker Identification Credentialing (TWIC) (Washington, D.C.: July 27, 2007).

[73] DHS, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington, D.C.: 2009). The NIPP, first issued in June 2006 by DHS, established a six-step risk management framework to establish national priorities, goals, and requirements for Critical Infrastructure and Key Resources (CIKR) protection so that Federal funding and resources are applied in the most effective manner to deter threats, reduce vulnerabilities, and minimize the consequences of attacks and other incidents. The NIPP states that comprehensive risk assessments are necessary for determining which assets or systems face the highest risk, for prioritizing risk mitigation efforts and the allocation of resources, and for effectively measuring how security programs reduce risks.

[74] The Coast Guard uses MSRAM to assess risk for various types of vessels and port infrastructure in accordance with the guidance on assessing risk from DHS's National Infrastructure Protection Plan (NIPP). The Coast Guard uses the analysis tool to help implement its strategy and concentrate maritime security activities when and where relative risk is believed to be the greatest. The model assesses the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios; that is, it combines potential targets with different means of attack, as recommended by the risk assessment aspect of the NIPP. Also in accordance with the NIPP, the model is designed to support decisionmaking for the Coast Guard. At the national level, the model's results are used, among other things, for identifying capabilities needed to combat future terrorist threats.

judge program effectiveness.[75] Conducting an effectiveness assessment that evaluates whether use of TWIC in its present form and planned use with readers would enhance the posture of security beyond efforts already in place given costs and program risks could better position DHS and policymakers in determining the impact of TWIC on enhancing maritime security.

Further, pursuant to Executive Branch requirements, prior to issuing a new regulation, agencies are to conduct a regulatory analysis, which is to include an assessment of costs, benefits, and associated risks.[76] Prior to issuing the regulation on implementing the use of TWIC as a flashpass, DHS conducted a regulatory analysis, which asserted that TWIC would increase security. The analysis included an evaluation of the costs and benefits related to implementing TWIC. However, DHS did not conduct a risk-informed cost-benefit analysis that considered existing security risks. For example, the analysis did not account for the costs and security risks associated with designing program controls to prevent an individual from acquiring an authentic TWIC using a fraudulent identity and limiting access to secure areas of MTSA-regulated facilities and vessels to those with a legitimate need, in accordance with stated mission needs. As a proposed regulation on the use of TWIC with biometric card readers is under development, DHS is to issue a new regulatory analysis. Conducting a regulatory analysis using the information from the internal control and effectiveness assessments as the basis for evaluating the costs, benefits, security risks, and needed corrective actions could better inform and enhance the reliability of the new regulatory analysis. Moreover, these actions could help DHS identify and assess the full costs and benefits of implementing the TWIC program in a manner that will meet stated mission needs and mitigate existing security risks, and help ensure that the TWIC program is more effective and cost-efficient than existing measures or alternatives at enhancing maritime security.

Coast Guard's Approach for Monitoring and Enforcing TWIC Compliance Could Be Improved by Enhancing Its Collection and Assessment of Maritime Security Information

Internal control standards state that: (1) internal controls should be designed to ensure that ongoing monitoring occurs in the course of normal operations, and (2) information should be communicated in a form and within a time-frame that enables management to carry out its internal control responsibilities.[77] Further, our prior work has stated that Congress also needs information on whether and in what respects a program is working well or poorly to support its oversight of agencies and their budgets, and agencies' stakeholders need performance information to accurately judge program effectiveness.[78] The Coast Guard uses its Marine Information for Safety and Law Enforcement (MISLE) database to meet these needs by recording activities related to MTSA-regulated facility and vessel oversight, including observations of TWIC-related deficiencies.[79] The purpose of MISLE is to provide the capability to collect, maintain, and retrieve information necessary for the administration, management, and documentation of Coast Guard activities. In February 2008, we reported that flaws in the data in MISLE limit the Coast Guard's ability to accurately portray and appropriately target oversight activities.[80]

---

[75] GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD–96–118 (Washington, D.C.: June 1996).

[76] Office of Management and Budget, Circular A–4, *Regulatory Analysis* (Revised Sept. 17, 2003) provides guidance to Federal agencies on the development of regulatory analysis as required by Executive Order 12866 of September 30, 1993, as amended by Executive Order 13258 of February 26, 2002, and Executive Order 13422 of January 18, 2007, "Regulatory Planning and Review." According to Executive Order 12866, agencies should adhere to certain specified principles, such as: (1) with respect to setting regulatory priorities, each agency shall consider, to the extent reasonable, the degree and nature of the risks posed by various substances or activities within its jurisdiction, and (2) each agency shall base its decisions on the best reasonably obtainable scientific, technical, economic, and other information concerning the need for, and consequences of, the intended regulation. According to Circular A–4, a regulatory analysis should include the following three basic elements: (1) a statement of the need for the proposed action, (2) an examination of alternative approaches, and (3) an evaluation of the benefits and costs—quantitative and qualitative—of the proposed action and the main alternatives identified by the action. The evaluation of benefits and costs is to be informed by a risk assessment.

[77] See GAO/AIMD–00–21.3.1.

[78] See GAO/GGD–96–118.

[79] MISLE began operating in December 2001 and is the Coast Guard's primary data system for documenting facility oversight and other activities.

[80] We recommended that, among other things, the Coast Guard assess MISLE compliance data, including the completeness of the data, data entry, consistency, and data field problems, and make any changes needed to more effectively use MISLE data. DHS concurred with this

Continued

In accordance with Coast Guard policy, Coast Guard inspectors are required to verify TWIC cards during annual compliance exams and security spot checks, and may do so in the course of other Coast Guard duties. As part of each inspection, Coast Guard inspectors are, among other things, to: (1) ensure that the card is authentic by examining it to visually verify that it has not been tampered with; (2) verify identity by comparing the photograph on the card with the TWIC holder to ensure a match; (3) check the card's physical security features; and (4) ensure the TWIC is valid—a check of the card's expiration date. Additionally, Coast Guard inspectors are to assess the proficiency of facility and vessel security personnel in complying with TWIC requirements through various means including oral examination, actual observation, and record review. Coast Guard inspectors randomly select workers to check their TWICs during inspections. The number of TWIC cards checked is left to the discretion of the inspectors.

As of December 17, 2010, according to Coast Guard data, 2,135 facilities have undergone at least 2 MTSA inspections as part of annual compliance exams and spot checks. In reviewing the Coast Guard's records of TWICrelated enforcement actions, we found that, in addition to verifying the number of inspections conducted, the Coast Guard is generally positioned to verify that TWIC cards are being checked by Coast Guard inspectors and, of the card checks that are recorded, the number of cardholders who are compliant and noncompliant. For instance, the Coast Guard reported inspecting 129,464 TWIC holders' cards from May 2009 through January 6, 2011. The Coast Guard reported that 124,203 of the TWIC holders, or 96 percent, were found to be compliant—possessed a valid TWIC.[81] However, according to Coast Guard officials, local Coast Guard inspectors may not always or consistently record all inspection attempts. Consequently, while Coast Guard officials told us that inspectors verify TWICs as part of all security inspections, the Coast Guard could not reliably provide the number of TWICs checked during each inspection.

Since the national compliance deadline in April 2009 requiring TWIC use at MTSA-regulated facilities and vessels, the Coast Guard has not identified major concerns with TWIC implementation nationally. However, while the Coast Guard uses MISLE to track program compliance, because of limitations in the MISLE system design, the processes involved in the collection, cataloguing, and querying of information cannot be relied upon to produce the management information needed to assess trends in compliance with the TWIC program or associated vulnerabilities. For instance, when inspectors document a TWIC card verification check, the system is set up to record the number of TWICs reviewed for different types of workers and whether the TWIC holders are compliant or noncompliant. However, other details on TWIC-related deficiencies, such as failure to ensure that all facility personnel with security duties are familiar with all relevant aspects of the TWIC program and how to carry them out, are not recorded in the system in a form that allows inspectors or other Coast Guard officials to easily and systematically identify that a deficiency was related to TWIC. For example, from January 2009 through December 2010, the Coast Guard reported issuing 145 enforcement actions as a result of annual compliance exams or security spot checks at the 2,135 facilities that have undergone the inspections.[82] These included 57 letters of warning, 40 notices of violation, 32 civil penalties, and 16 operations controls (suspension or restriction of operations). However, it would be labor-intensive for the Coast Guard to identify how many of the 57 letters of warning or 40 notices of violation were TWIC related, according to a Coast Guard official responsible for TWIC compliance, because there is not an existing query designed to extract this information from the system. Someone would have to manually review each of the 97 inspection reports in the database indicating either a letter of warning or a notice of violation to verify whether or not the deficiencies were TWIC related. As such, the MISLE system is not designed to

---

recommendation. The Coast Guard acknowledged the need for improvement in MISLE compliance data and has taken initial steps to reduce some of the database concerns identified in our previous work. However, as of January 2011, the recommendation has not been fully addressed. See GAO, *Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data*, GAO–08–12 (Washington, D.C.: Feb. 14, 2008).

[81] These numbers represent a combination of visual and electronic verifications because the TWIC verification window in MISLE is not currently designed to capture whether cards are verified visually or electronically. According to Coast Guard officials, with the recent deployment of handheld readers to Coast Guard units, the Coast Guard is in the process of enhancing MISLE to include the ability to distinguish between the number of visual inspections of cards and the number of verifications conducted using the handheld readers.

[82] According to the Coast Guard, 2,509 facilities are subject to MTSA and must actively implement TWIC provisions.

readily provide information that could help management measure and assess the overall level of compliance with the TWIC program or existing vulnerabilities.

According to a Coast Guard official responsible for TWIC compliance, Coast Guard headquarters staff has not conducted a trend analysis of the deficiencies found during reviews and inspections and there are no other analyses they planned to conduct regarding enforcement until after readers are required to be used. According to the Coast Guard, it can generally identify the number of TWICs checked and recorded in the MISLE system. However, it cannot perform trend analysis of the deficiencies as it would like to do, as it requires additional information. In the interim, as of January 7, 2011, the Coast Guard reported deploying 164 handheld biometric readers nationally to units responsible for conducting inspections.[83] These handheld readers are intended to be the Coast Guard's primary means of TWIC verification. During inspections, Coast Guard inspectors use the card readers to electronically check TWICs in three ways: (1) verification—a biometric one-to-one match of the fingerprint; (2) authentication—electronically confirming that the certificates on the credential are authentic; and (3) validation—electronically check the card against the "hotlist" of invalid or revoked cards. The Coast Guard believes that the use of these readers during inspections will greatly improve the effectiveness of enforcement efforts and enhance record keeping through the use of the readers' logs.

As a result of limitations in MISLE design and the collection and recording of inspection data, it will be difficult for the Coast Guard to identify trends nationwide in TWIC-related compliance, such as whether particular types of facilities or a particular region of the country have greater levels of noncompliance, on an ongoing basis. Coast Guard officials acknowledged these deficiencies and reported that they are in the process of making enhancements to the MISLE database and plan to distribute updated guidance on how to collect and input information into MISLE to the Captains of the Port. However, as of January 2011, the Coast Guard had not yet set a date for implementing these changes. Further, while this is a good first step, these enhancements do not address weaknesses related to the collection process and querying of MISLE information so as to facilitate the Coast Guard performing trend analysis of the deficiencies as part of its compliance reviews. By designing and implementing a cost-effective and practical method for collecting, cataloging, and querying TWIC-related compliance information, the Coast Guard could be better positioned to identify and assess TWIC-related compliance and enforcement trends, and to obtain management information needed to assess and understand existing vulnerabilities with the use of TWIC.

Conclusions

As the TWIC program continues on the path to full implementation—with potentially billions of dollars needed to install TWIC card readers in thousands of the Nation's ports, facilities, and vessels at stake—it is important that Congress, program officials, and maritime industry stakeholders fully understand the program's potential benefits and vulnerabilities, as well as the likely costs of addressing these potential vulnerabilities. Identified internal control weaknesses and vulnerabilities include weaknesses in controls related to preventing and detecting identity fraud, assessing the security threat that individuals with extensive criminal histories pose prior to issuing a TWIC, and ensuring that TWIC holders continue to meet program eligibility requirements. Thus, conducting an internal control assessment of the program by analyzing controls, identifying related weaknesses and risks, and determining cost-effective actions to correct or compensate for these weaknesses could better position DHS to provide reasonable assurance that control weaknesses do not impede the program from meeting mission needs.

In addition, conducting an effectiveness assessment could help provide reasonable assurance that the use of TWIC enhances the posture of security beyond efforts already in place or identify the extent to which TWIC may possibly introduce security vulnerabilities because of the way it has been designed and implemented. This assessment, along with the internal controls assessment, could be used to enhance the regulatory analysis to be conducted as part of implementing a regulation on the use of TWIC with readers. More specifically, considering identified security risks and needed corrective actions as part of the regulatory analysis could provide insights on the full costs and benefits of implementing the TWIC program in a manner that will meet stated mission needs and mitigate existing security risks. This is important because, unlike prior access control approaches which allowed access to a specific facility, the TWIC potentially facilitates access to thousands of facilities once the Federal Government attests that the TWIC holder has been positively identified

[83] The Coast Guard estimated a need for 300 handheld biometric readers, based on an estimate of 5 readers for each of the Coast Guard's major field inspections units across the country.

and is deemed not to be a security threat. Further, doing so as part of the regulatory analysis could better assure DHS, Congress, and maritime stakeholders that TWIC program security objectives will be met. Finally, by designing and implementing a cost-effective and practical method for collecting, cataloging, and querying TWIC-related compliance information, the Coast Guard could be better positioned to identify trends and to obtain management information needed to assess and understand existing vulnerabilities with the use of TWIC.

Recommendations for Executive Action

To identify effective and cost-efficient methods for meeting TWIC program objectives, and assist in determining whether the benefits of continuing to implement and operate the TWIC program in its present form and planned use with readers surpass the costs, we recommend that the Secretary of Homeland Security take the following four actions:

- Perform an internal control assessment of the TWIC program by: (1) analyzing existing controls, (2) identifying related weaknesses and risks, and (3) determining cost-effective actions needed to correct or compensate for those weaknesses so that reasonable assurance of meeting TWIC program objectives can be achieved. This assessment should consider weaknesses we identified in this report among other things, and include:
  - strengthening the TWIC program's controls for preventing and detecting identity fraud, such as requiring certain biographic information from applicants and confirming the information to the extent needed to positively identify the individual, or implementing alternative mechanisms to positively identify individuals;
  - defining the term extensive criminal history for use in the adjudication process and ensuring that adjudicators follow a clearly defined and consistently applied process, with clear criteria, in considering the approval or denial of a TWIC for individuals with extensive criminal convictions not defined as permanent or interim disqualifying offenses; and
  - identifying mechanisms for detecting whether TWIC holders continue to meet TWIC disqualifying criminal offense and immigration-related eligibility requirements after TWIC issuance to prevent unqualified individuals from retaining and using authentic TWICs.
- Conduct an effectiveness assessment that includes addressing internal control weaknesses and, at a minimum, evaluates whether use of TWIC in its present form and planned use with readers would enhance the posture of security beyond efforts already in place given costs and program risks.
- Use the information from the internal control and effectiveness assessments as the basis for evaluating the costs, benefits, security risks, and corrective actions needed to implement the TWIC program in a manner that will meet stated mission needs and mitigate existing security risks as part of conducting the regulatory analysis on implementing a new regulation on the use of TWIC with biometric card readers.
- Direct the Commandant of the Coast Guard to design effective methods for collecting, cataloguing, and querying TWIC-related compliance issues to provide the Coast Guard with the enforcement information needed to assess trends in compliance with the TWIC program and identify associated vulnerabilities.

Agency Comments and Our Evaluation

We provided a draft of the sensitive version of this report to the Secretary of Homeland Security for review and comment on March 18, 2011. DHS provided written comments on behalf of the Department, the Transportation Security Administration, and the United States Coast Guard, which are reprinted in full in appendix IV. In commenting on our report, DHS stated that it concurred with our four recommendations and identified actions planned or under way to implement them.

While DHS did not take issue with the results of our work, DHS did provide new details in its response that merit additional discussion. First, DHS noted that it is working to strengthen controls around applicant identity verification in TWIC, but that document fraud is a vulnerability to credential-issuance programs across the Federal Government, state and local governments, and the private sector. DHS further noted that a governmentwide infrastructure does not exist for information sharing across all entities that issue documents that other programs, such as TWIC, use to positively authenticate an individual's identity. We acknowledge that such a government-wide infrastructure does not exist, and, as discussed in our report, recognize that there are inherent weaknesses in relying on identity documents alone

to confirm an individual's identity. However, positively identifying individuals—or confirming their identity—and determining their eligibility for a TWIC is a key stated program goal. Issuing TWICs to individuals without positively identifying them and subsequently assuring their eligibility could, counter to the program's intent, create a security vulnerability. While we recognize that additional costs could be imposed by requiring positive identification checks, taking actions to strengthen the existing identity authentication process, such as only accepting documents that TSA can and does confirm to be authentic with the issuing agency, and verifying an applicant's business need, could enhance TWIC program efforts to prevent and detect identity fraud and enhance maritime security.

Second, DHS stated that it is working to continually verify TWIC-holder eligibility after issuance but also noted the limitations in the current process. While TSA does receive some criminal history records information when it sends fingerprints to the FBI, the information is not provided recurrently, nor is the information necessarily complete. DHS stated that to provide the most robust recurrent vetting against criminal records, TSA would need access to additional state and Federal systems, and have additional authority to do so. As we reported, FBI and TWIC officials stated that because the TWIC background check is considered to be for a noncriminal justice purpose, policy and statutory provisions hamper the program from running the broader FBI fingerprint-based check using the fingerprints collected at enrollment on an ongoing basis. However, we continue to believe that TSA could compensate for this weakness by leveraging existing mechanisms available to maritime stakeholders. For example, other governing entities—such as the Alabama State Port Authority—that have an interest in ensuring the security of the maritime environment, might be willing to establish a mechanism for independently sharing relevant information when warranted. Absent efforts to leverage available information sources, TSA may not be successful in tempering existing limitations.

Lastly, DHS sought clarification on the reporting of our investigators' success at breaching security at ports during covert testing. Specifically, in its comments, DHS noted that it believes that our report's focus on access to port areas rather than access to individual facilities can be misleading. DHS noted that we do not report on the number of facilities that our investigators attempted to gain access to within each port area. DHS stated that presenting the breaches in terms of the number of port areas breached rather than the number of facilities paints a more troublesome picture of the actual breaches that occurred. We understand DHS's concern but continue to believe that the results of our investigators' work, as reported, fairly and accurately represents the results and significance of the work conducted. The goal of the covert testing was to assess whether or not weaknesses exist at ports with varying characteristics across the nation, not to define the pervasiveness of existing weaknesses by type of facility, volume, or other characteristic. Given the numerous differences across facilities and the lack of publicly available information and related statistics for each of the approximately 2,509 MTSA-regulated facilities, we identified covert testing at the port level to be the proper unit of analysis for our review and reporting purposes. Conducting a detailed assessment of the pervasiveness of existing weaknesses by type of facility, volume, or other characteristics as suggested by DHS would be a more appropriate tasking for the Coast Guard as part of its continuing effort to ensure compliance with TWIC-related regulations.

In addition, with regard to covert testing, DHS further commented that the report does not distinguish among breaches in security using a counterfeit TWIC or an authentic TWIC card obtained with fraudulent documents. DHS noted that because there is no "granularity" with the report as to when a specific card was used, one can be left with the unsupported impression that individual facilities in all cases were failing to implement TWIC visual inspection requirements. For the above noted reason, we did not report on the results of covert testing at the facility level. However, our records show that use of counterfeit TWICs was successful for gaining access to more than one port where our investigators breached security. Our investigators further report that security officers never questioned the authenticity of TWICs presented for acquiring access. Our records show that operations at the locations our investigators breached included cargo, containers, and fuel, among others.

In addition, TSA provided written technical comments, which we incorporated into the report, as appropriate.

We are sending copies of this report to the Secretary of Homeland Security, the Assistant Secretary for the Transportation Security Administration, the Commandant of the United States Coast Guard, and appropriate congressional committees. In addition, this report is available at no charge on the GAO website at *http://www.gao.gov*.

If you or your staff have any questions about this report, please contact me.

STEPHEN M. LORD
Director, Homeland Security and Justice Issues

List of Requesters

The Honorable John D. Rockefeller, IV
Chairman
Committee on Commerce, Science, and Transportation
U.S. Senate

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
U.S. Senate

The Honorable John L. Mica
Chairman
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Frank R. Lautenberg
Chairman
Subcommittee on Surface Transportation and Merchant Marine Infrastructure, Safety, and Security
Committee on Commerce, Science, and Transportation
U.S. Senate

The Honorable Olympia J. Snowe
Ranking Member
Subcommittee on Oceans, Atmosphere, Fisheries, and Coast Guard
Committee on Commerce, Science, and Transportation
U.S. Senate

The Honorable Frank A. LoBiondo
Chairman
Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Mike Rogers
Chairman
Subcommittee on Transportation Security
Committee on Homeland Security
House of Representatives

The Honorable Candice S. Miller
Chairwoman
Subcommittee on Border and Maritime Security
Committee on Homeland Security
House of Representatives

APPENDIX I: KEY STEPS IN THE TWIC ENROLLMENT PROCESS

Transportation workers are enrolled by providing biographic information, such as name, date of birth, and address, and proof of identity documents, and then photographed and fingerprinted at 1 of approximately 149 enrollment centers by trusted agents. A trusted agent is a member of the TWIC team who has been authorized by the Federal Government to enroll transportation workers in the TWIC program and issue TWIC cards. Trusted agents are subcontractor staff acquired by Lockheed Martin as part of its support contract with TSA for the TWIC program. Table 2 below summarizes key steps in the enrollment process.

Table 2.—TWIC Enrollment Process Summary

1.	The TWIC applicant fills out a TWIC Application and Disclosure Form and affirms that the information he or she is providing to TSA is truthful.
2.	The applicant is required to present documentation to establish his or her identity to the trusted agent at the enrollment center. The documentation required is dependant upon the applicant's legal presence in the United States or whether the applicant was born in the United States.
3.	The trusted agent (government contractor) captures the applicant's biographic information, such as name and date of birth, in the TWIC system. This can be done in various ways, such as by scanning fingerprints and certain identity documents or by manually typing information into the system.
4.	The trusted agent reviews the identity documents to establish and confirm the applicant's identity and to confirm the documents' authenticity by reviewing the physical security features on the documents.
5.	The trusted agent scans the identity documents to record a digital image of the applicant's identity information.
6.	The trusted agent uses a machine-readable document scanning device to assess the risk of certain documents being fraudulent. Not all documents can be assessed using this device.
7.	The applicant's 10 fingerprints (where available) are captured in the system. The presence of non-suitable fingerprints or lack of a finger for biometric use is documented in the system by the trusted agent.
8.	The applicant's digital picture is taken.
9.	The enrollment record is completed, encrypted, and is forwarded by the trusted agent to undergo the TWIC program's background checking procedures.

Source: GAO analysis of the TWIC program enrollment process and documentation.

APPENDIX II: TWIC PROGRAM FUNDING

According to TSA and Federal Emergency Management Agency (FEMA) program officials, from Fiscal Year 2002 through 2010, the TWIC program had funding authority totaling $420 million. Through Fiscal Year 2009, $111.5 million in appropriated funds, including reprogramming and adjustments, had been provided to TWIC (see table 3 below). An additional $196.8 million in funding was authorized from Fiscal Years 2008 through 2010 through the collection of TWIC enrollment fees by TSA, and $111.7 million had been made available to maritime facilities implementing TWIC from FEMA grant programs—the Port Security Grant Program and the Transit Security Grant Program—from Fiscal Years 2006 through 2010. In addition, industry has spent between approximately $185.7 million and $234 million to purchase 1,765,110 TWICs as of January 6, 2011.[1] The costs for implementing the TWIC program, as estimated by TSA for informing the regulation on requiring the use of TWIC as an identification credential, is from $694.3 million to $3.2 billion over a 10-year period. This estimate includes the costs related to purchasing TWICs and visually inspecting them. However, this estimate does not include the costs related to implementing TWIC with biometric card readers or related access control systems.[2]

Table 3.—TWIC Program Funding from Fiscal Years 2002 through 2010

Dollars in millions

Fiscal year	Appropriated	Reprogramming	Adjustments	TWIC fee authority[a]	Federal security grant awards related to TWIC[b]	Total funding authority
2002	0	0	0	0	0	0
2003	$5.0	0	$20	0	0	$25.0
2004	$49.7	0	0	0	0	$49.7
2005	$5.0	0	0	0	0	$5.0
2006	0	$15.0	0	0	$24.3	$39.3
2007	0	$4.0	$4.7	0	$31.5[c]	$40.2

[1] Range based on a reduced fee of $105.25 per TWIC for workers with current, comparable background checks or a $132.50 fee per TWIC for those without.

[2] See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Final Rule, 72 Fed. Reg. 3492, 3571 (2007).

Table 3.—TWIC Program Funding from Fiscal Years 2002 through 2010—Continued

Dollars in millions

Fiscal year	Appropriated	Reprogramming	Adjustments	TWIC fee authority [a]	Federal security grant awards related to TWIC [b]	Total funding authority
2008	$8.1	0	0	$42.5	$18.0	$68.6
2009	0	0	0	$109.3	$22.2 [d]	$131.5
2010	0	0	0	$45.0	$15.7	$60.7
Total	*$67.8*	*$19.0*	*$24.7*	*$196.8*	*$111.7*	*$420*

Source: GAO analysis of TWIC program funding reported by TSA and FEMA.

[a] Figures in the TWIC fee authority column represent the dollar amount TSA is authorized to collect from TWIC enrollment fees and not the actual dollars collected. TSA reports to have collected $41.7 million for Fiscal Year 2008, $76.2 million for Fiscal Year 2009, and $30.6 million for Fiscal Year 2010.

[b] According to FEMA, many of these awards are issued as cooperative agreements and, as such, the scope and amounts may change as the project(s) proceed. Also, FEMA has not received projects from all grant recipients so the total number of projects may increase slightly over time.

[c] Federal security grant funding subtotal for Fiscal Year 2007 includes $19.2 million in Fiscal Year Port Security Grant Program funding, $10.8 million in supplemental funding, and $1.5 million in Transit Security Grant Program funding.

[d] Federal security grant funding subtotal for Fiscal Year 2009 includes $3.9 million in Fiscal Year Port Security Grant Program funding and an additional $18.3 million in American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111–5, 123 Stat. 115 (2009)) funding.

APPENDIX III: LIST OF DOCUMENTS U.S.-BORN CITIZENS OR NATIONALS MUST SELECT FROM TO PRESENT WHEN APPLYING FOR A TWIC

TWIC applicants who are citizens of the United States (or its outlying possessions) and were born inside the United States (or its outlying possessions), must provide one document from list A or two documents from list B. If two documents from list B are presented, at least one of them must be a government-issued photo identification, such as a state-issued driver's license, military ID card, or state identification card.

List A

- Unexpired United States passport book or passport card
- Unexpired Merchant Mariner Document
- Unexpired Free and Secure Trade Card [1]
- Unexpired NEXUS Card [2]
- Unexpired Secure Electronic Network for Travelers Rapid Inspection Card

List B

- Unexpired driver's license issued by a state or outlying possession of the United States
- Unexpired identification card issued by a state or outlying possession of the United States. Must include a state or state agency seal or logo (such as state port authority identification or state university identification)
- Original or certified copy of birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal
- Voter's registration card
- United States military identification card or United States retired military identification
- United States military dependent's card
- Expired United States passport (within 12 months of expiration)
- Native American tribal document (with photo)
- United States Social Security card
- United States military discharge papers (DD–214)
- Department of Transportation medical card

[1] The Free and Secure Trade (FAST) Card is to be issued to approved commercial drivers to facilitate the travel of low-risk screened shipments across the borders between the U.S.-Canadian border and to the U.S. from Mexico.

[2] The NEXUS card can be used as an alternative to the passport for air, land, and sea travel into the United States for U.S. and Canadian citizens. The NEXUS program allows prescreened travelers expedited processing by United States and Canadian officials at dedicated processing lanes at designated northern border ports of entry, at NEXUS kiosks at Canadian Preclearance airports, and at marine reporting locations.

- United States civil marriage certificate
- Unexpired Merchant Mariner License bearing an official raised seal, or a certified copy
- Unexpired Department of Homeland Security/Transportation Security Administration Transportation Worker Identification Credential Card
- Unexpired Merchant Mariner Credential

APPENDIX IV: CRIMINAL OFFENSES THAT MAY DISQUALIFY APPLICANTS FROM ACQUIRING A TWIC

Listed below are criminal offenses that can prevent TWIC applicants from being issued a TWIC. Pursuant to TSA implementing regulations, permanent disqualifying offenses are offenses defined in 49 C.F.R. 1572.103(a). Permanent disqualifying offenses that can be waived are those offenses defined in 49 C.F.R. 1572.103(a) for which a waiver can be granted in accordance with 49 C.F.R. 1515.7(a)(i). Interim disqualifying offenses are offenses defined in 49 C.F.R. 1572.103(b) for which the applicant has either been: (1) convicted, or found not guilty by reason of insanity, within a 7-year period preceding the TWIC application, or (2) incarcerated for within a 5-year period preceding the TWIC application. Applicants with certain permanent criminal offenses and all interim disqualifying criminal offenses may request a waiver of their disqualification. In general, TSA may issue such a waiver and grant a TWIC if TSA determines that an applicant does not pose a security threat based upon the security threat assessment.

Permanent disqualifying criminal offenses for which no waiver may be granted.

1. Espionage, or conspiracy to commit espionage.

2. Sedition, or conspiracy to commit sedition.

3. Treason, or conspiracy to commit treason.

4. A Federal crime of terrorism as defined in 18 U.S.C. 2332b(g), or comparable state law, or conspiracy to commit such crime.

Permanent disqualifying criminal offenses for which a waiver may be granted.

1. A crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. § 70101. The term economic disruption does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employer-employee dispute.

2. Improper transportation of a hazardous material under 49 U.S.C. § 5124, or a state law that is comparable.

3. Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device. An explosive or explosive device includes, but is not limited to, an explosive or explosive material as defined in 18 U.S.C. §§ 232(5), 841(c) through 841(f), and 844(j); and a destructive device, as defined in 18 U.S.C. § 921(a)(4) and 26 U.S.C. § 5845(f).

4. Murder.

5. Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportations system, or an infrastructure facility.

6. Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §1961, et seq. , or a comparable state law, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the crimes listed in paragraph 49 C.F.R. § 1572.103(a).

7. Attempt to commit the crimes in paragraphs listed under 49 C.F.R. § 1572.103(a)(1) through (a)(4).

8. Conspiracy or attempt to commit the crimes in 49 C.F.R. § 1572.103(a)(5) through (a)(10).

The interim disqualifying felonies.

1. Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited

to, firearms as defined in 18 U.S.C. § 921(a)(3) or 26 U.S.C. § 5845(a), or items contained on the United States Munitions Import List at 27 CFR § 447.21.

2. Extortion.

3. Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering where the money laundering is related to a crime described in 49 C.F.R. § 1572.103(a) or (b). Welfare fraud and passing bad checks do not constitute dishonesty, fraud, or misrepresentation for purposes of this paragraph.

4. Bribery.

5. Smuggling.

6. Immigration violations.

7. Distribution of, possession with intent to distribute, or importation of a controlled substance.

8. Arson.

9. Kidnapping or hostage taking.

10. Rape or aggravated sexual abuse.

11. Assault with intent to kill.

12. Robbery.

13. Fraudulent entry into a seaport as described in 18 U.S.C. § 1036, or a comparable state law.

14. Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961, et seq., or a comparable state law, other than the violations listed in paragraph 49 C.F.R. § 1572.103(a)(10).

15. Conspiracy or attempt to commit the interim disqualifying felonies.

APPENDIX V: COMPARISON OF AUTHENTIC AND COUNTERFEIT TWICS

Figure 1: Comparison of Authentic and Counterfeit TWICs
Details from this section were removed because the agency deemed them to be sensitive security information.

APPENDIX VI: COMMENTS FROM THE DEPARTMENT OF HOMELAND SECURITY

U.S. DEPARTMENT OR HOMELAND SECURITY
Washington, DC, May 5, 2011

Mr. STEPHEN M. LORD,
Director, Homeland Security and Justice Issues,
U.S. Government Accountability Office,
Washington, DC.

Dear Mr. Lord:

Re: GAO–11–657, Draft Report, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Objectives*

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

Transportation Worker Identification Credential (TWIC) is a vital security program that is jointly administered by the U.S. Coast Guard (USCG) and the Transportation Security Administration (TSA). TSA is responsible for enrollment, vetting, and card production, with the support of the U.S. Citizenship and Immigration Services, while the USCG governs access control requirements and has primary responsibility for enforcement. As of March 2011, TSA has enrolled and vetted more than 1.8 million maritime workers. As a result of DHS's rigorous vetting process, 35,661 individuals were denied from receiving a TWIC. DHS agrees that more work is needed to strengthen existing security controls and has begun efforts to address many of the GAO's findings.

DHS Increasing Applicant Identity Verification Controls

DHS is working to strengthen controls around applicant identity verification in TWIC, knowing that document fraud is a vulnerability to credential-issuance programs across Federal, state, and local governments, and the private sector. To establish identity and proof-of-citizenship, TWIC leverages documents issued by mul-

tiple Federal, state, and local entities. However, a government-wide infrastructure does not exist for information sharing across all entities that issue the breeder documents that relying parties use to positively authenticate an identity. TWIC follows best practices to mitigate the risks from not having visibility or control of the physical characteristics or the issuance process for these documents. Specifically. TWIC uses document authentication readers and requires fraudulent document training of its Trusted Agents as safeguards against document fraud.

TWIC will benefit from national efforts to strengthen identity documents. For example, DHS continues to work with the states to implement the requirements of the REAL ID Act for more secure driver's licenses, as well as the underlying issuance processes and procedures. Furthermore, efforts are underway in the Federal Government, state vital records agencies, and departments of motor vehicles to enhance security related to core breeder documents. such as birth certificates, which would assist in positive authentication.

TSA is also actively engaged with the DHS's United States Visitor and Immigrant Status Indicator Technology (US–VISIT) program to include TWIC applicant data into the US–VISIT database, referred to as IDENT. Biometrics placed in IDENT are linked to specific biographic information, enabling a person's identity to be established and then verified by the U.S. Government.

TWIC is also strengthening safeguards against cards being misused after issuance. An upcoming USCG rulemaking will include a requirement for electronic verification of the TWIC card through use of card readers. The use of electronic readers will provide the port or facility authority in charge of access control decisions with a higher level of assurance that the TWIC presented is authentic, valid (not revoked), and unexpired.

DHS Working to Continually Verify TWIC Holder Eligibility after Issuance

DHS strongly agrees on the value of recurrent vetting. DHS is making progress in the effort to reasonably assure that TWIC holders have maintained their eligibility once issued their TWICs. TSA conducts recurrent checks of TWIC holders against the Terrorist Screening Database and other databases. TSA has the authority to revoke TWICs based on the results of recurrent vetting, and use of card readers for electronic verification will strengthen the effectiveness of these processes.

In order to provide the most robust recurrent vetting against criminal history records, TSA needs full access to Criminal History Records Information (CHRI), similar to that of a criminal justice agency or law enforcement officer; this information is available at the state level and accessed via the Interstate Identification Index managed by the U.S. Department of Justice, Federal Bureau of Investigation (FBI). Although TSA receives some CHRI when it sends fingerprints to the FBI for initial vetting, the FBI does not perform recurrent vetting of CHRI on behalf of TSA. The FBI has deemed that TSA's security threat assessments for TWIC are non-criminal justice activities. As a result, TSA is unable to request subsequent CHRI for recurrent vetting without a submission of new fingerprints from the individual. Additionally, TSA may not always receive all available information because of the FBI's designation as "non-criminal justice" purposes for TSA security threat assessments. States may not upload all available information into the FBI biometric system and may not respond to CHRI requests for "non-criminal justice" activities. DHS has and will continue to work with the FBI and states to try to expand access to the CHRI.

While not a final solution to the challenge of recurrent criminal vetting, including TWIC data in IDENT would provide a framework to initiate more recurrent vetting on CURL, where available, for TWIC holders. In addition to supporting identity verification, biometric data from IDENT is used to conduct vetting against criminals and immigration violators. TSA and US–VISIT are working to include TWIC data in the IDENT database.

DHS Clarification on GAO Breaches of MTSA-Regulated Ports

DHS would also like to address aspects of GAO's covert operation defined in the report that we believe warrant further clarification.

DHS believes that the focus on access to port areas rather than access to individual facilities can be misleading. Specifically, the report states that GAO investigators successfully penetrated ports between August 2009 and February 2010. However, the report does not breakdown the number of facilities to which GAO attempted to gain access within each port area. Each port is unique in design and operation—ranging from some ports housing hundreds of individual facilities spread over a large geographic area to other ports containing only a few facilities in a small geographic area with one main access control point. While GAO stated that it did not require its covert investigators to record the individual attempts to access facili-

ties, investigators indicated during discussions with USCG that they were successful in gaining unauthorized access at some individual facilities within the port areas. The presentation of breaches at port versus individual facilities paints a more troublesome picture of the actual breaches that occurred.

Third, the report does not distinguish among fraud committed with counterfeit TWIC cards, authentic TWIC cards obtained with fraudulent documents, and access control decisions made by facility personnel. Each type of fraud has a different mitigation technique. The fact that a Facility Security Officer does not question what appears to be a valid card should not be intertwined with cases in which a counterfeit card was presented to gain access. Because there is no granularity within the report as to when a specific card was used, one can be left with the unsupported impression that individual facilities in all cases were failing to implement TWIC visual inspection requirements. Or, as written in this report, that ports failed to properly implement these requirements.

Recent Developments

The GAO audit was beneficial in helping DHS identify immediate actions that could strengthen the effectiveness of the TWIC program.

TSA has already taken steps to remedy some of the missing internal controls that GAO has identified. Starting in January 2011, the TWIC program initiated a 100-percent review of all fingerprint matches received in the system. These matches could highlight potential fraud in the TWIC enrollment process where one individual could be attempting to enroll under a different identity and possibly with fraudulent documents. During this process, the TWIC program has already referred numerous cases to our Law Enforcement Investigations Unit where investigations are under way.

On February 14, 2011, USCG Headquarters published additional guidance to field units regarding the importance of TWIC inspections and verifications. The guidance directed Captains of the Port to place a higher priority on the review and validation of TWIC verification procedures during the required Maritime Transportation Security Act (MTSA) security inspections. Additionally, the guidance encouraged Captains of the Port and the Facility Security Officers to take advantage of training aids regarding the identification of fraudulent TWICs published on Homeport-the USCG's Internet site for maritime information.

As previously mentioned, the USCG is currently developing an upcoming rulemaking that will include a requirement for card readers at ports and facilities. The TWIC program has completed a pilot that evaluated using card readers for electronic verification of the TWIC card. DHS believes that electronic verification of TWIC cards will significantly enhance protection against counterfeit, tampered, or expired TWIC cards being used to gain access to secure facilities.

TSA is in the initial phases of a modernization effort for its vetting infrastructure. This effort is aimed at consolidating systematic processes related to conducting background checks with the goal of improving the overall security and consistency of our enrollment and vetting processes. As the modernization effort moves forward, the TWIC program will continue to be heavily involved to ensure that any internal control gaps or risks are addressed or further mitigated.

GAO Recommendations

DHS takes the findings of this review very seriously. DHS strongly believes that TWIC has an overall effect of strengthening the security of our nation's ports. We also acknowledge and appreciate GAO's work to identify opportunities to enhance current program controls. We recognize that breaches did occur and that the Department and port facility owners and operators need to take steps to enhance security. DHS appreciates the opportunity to provide GAO with comments to its audit recommendations.

"To identify effective and cost efficient methods for meeting TWIC program objectives, and assist in determining whether the benefits of continuing to implement and operate the TWIC program in its present form and planned use with readers surpass the costs, we recommend that the Secretary of Homeland Security take the following four actions:

Recommendation 1: Perform an internal control assessment of the TWIC program by: (1) analyzing existing controls, (2) identifying related weaknesses and risks, and (3) determining cost-effective actions needed to correct or compensate for those weaknesses so that reasonable assurance of meeting TWIG program objectives can be achieved. This assessment should consider weaknesses we identified in this report, among other things, and include:

- strengthening the TWIC program's controls for preventing and detecting identity fraud, such as requiring certain biographic information from applicants and confirming the information to the extent needed to positively identify the individual, or implementing alternative mechanisms to positively identify individuals;
- defining the term extensive criminal history for use in the adjudication process and ensuring that adjudicators follow a clearly defined and consistently applied process, with clear criteria, in considering the approval and denial of a TWIC for individuals with extensive criminal convictions not defined as a permanent or interim disqualifying offense, and;
- identifying mechanisms for detecting whether TWIC-holders continue to meet TWIC disqualifying criminal offense and immigration-related eligibility requirements after TWIC issuance to prevent unqualified individuals from retaining and using authentic TWICs."

Response: Concur. DHS agrees that an internal control assessment should and will be performed. Once the final GAO report is issued, DHS will initiate a comprehensive review of current internal controls with a specific focus on the controls highlighted in this report. In the interim, TSA and USCG are evaluating and implementing new internal controls as discussed in this letter.

Recommendation 2: "Conduct an effectiveness assessment that includes addressing internal control weaknesses and, at a minimum, evaluates whether use of TWIC in its present form and planned use with readers would enhance the posture of security beyond efforts already in place given costs and program risks."

Response: Concur. DHS agrees that the results of the internal control assessment should be used to further evaluate the effectiveness of the TWIC program.

Recommendation 3: "Use the information from the internal control and effectiveness assessments as the basis for the evaluating the costs, benefits, security risks, and corrective actions needed to implement the TWIC program in a manner that will meet stated mission needs and mitigate existing security risks as part of conducting the regulatory analysis on implementing a new regulation on the use of TWIC with biometric card readers."

Response: Concur. As the internal control assessments progress, any applicable data or risks will be communicated to USCG for consideration during their regulatory analysis.

Recommendation 4: "Direct the Commandant of the Coast Guard to design effective methods for collecting, cataloging, and querying TWIC-related compliance issues to provide the Coast Guard with the enforcement information needed to assess trends in compliance with the TWIC program and identify associated vulnerabilities."

Response: Concur. USCG has already incorporated changes to its current version of Marine Information for Safety and Law Enforcement (MISLE) to enhance data collection since the TWIC compliance date of April 15, 2009. Incorporation of additional changes is planned in a future release of MISLE that will add to current capabilities to collect data and allow for more detailed trend analysis.

Again, thank you for the opportunity to review and comment on this draft report. We look forward to working with you on future Homeland Security issues.

Sincerely,

JIM H. CRUMPACKER,
Director, Departmental GAO/OIG Liaison Office.

APPENDIX VII: GAO CONTACT AND STAFF

Stephen M. Lord at (202) 512–4379 or at *lords@gao.gov*

Staff Acknowledgments

In addition to the contact named above, David Bruno (Assistant Director), Joseph P. Cruz, Scott Fletcher, Geoffrey Hamilton, Richard Hung, Lemuel Jackson, Linda Miller, Jessica Orr, and Julie E. Silvers made key contributions to this report.

Senator LAUTENBERG. Thank you very much, Mr. Lord.

It's astounding to hear your testimony and see the large percentage of those really not qualified to receive the card. And then you said, being convicted of a felony does not automatically disqualify a person from being eligible. And it goes on to detail what kind of offenses: espionage, treason, other offenses, such as murder or the

unlawful possession of explosive device. It sounds like we're not attracting, always, the kinds of applicants that would qualify to get a card. And that's a tough outcome for something that ought to be done much differently.

Through your covert testing, you said you were able to obtain fraudulent TWIC cards, and access secure facilities using these cards. Now, what kind of threats are these to our ports and our other secure facilities?

Mr. LORD. Well, in our report today, we reference a 2008 Coast Guard assessment, in which it states, very clearly, al Qaeda considers U.S. ports and facilities to be legitimate targets. Perhaps the Coast Guard witness could expound on that. But, that to us, that's why this issue is important.

Senator LAUTENBERG. The fact of the matter is that there's a question that invites a view of the magnitude of the problems that are involved in having something that can be stabilized and relied upon. And I wonder what other kinds of approaches there might be in order to get this to be an easier program to manage—one that's more reliable. Anyone want to make a quick suggestion here on that regard?

Mr. Pistole?

Admiral COOK. Mr. Chairman, I would just go back a little bit in history. I happen to have been the Captain of Port for the Houston-Galveston area during 9/11. And at that time, when we tried to bring into account—actually, before the MTSA, but certainly recognizing that access control was very, very important—that we tried to find a document that could be universally recognized from facility to facility which, typically, would have their own card. Sometimes they would recognize driver's license. Sometimes they would recognize other Federal ID cards. That was a very important thing for us to address early on. So, as we move from that initial, you know, implementation, and realizing that we needed to have more secure ports in the future, looking forward to one card that could be universally recognized, that guards could be trained to recognize, security features could be built in. And I think that that has been viewed as a very good thing. The Coast Guard actually looks forward to the opportunity to maximize that card through the use of card readers, which will then provide an additional level of verification, authentication, and validation. But—so, I—from my point of view, I would say that the card has introduced a significant amount of security, and certainly with my past experience——

Senator LAUTENBERG. Well, but there is—Admiral, there is a suggestion that, in some ways, we might have not gained on it, and exposed ourselves to more difficult problems in the future.

So, Mr. Pistole, before we discuss TSA's effort to address port security, it was discovered that al Qaeda was planning an attack on a U.S. rail line. To date, TSA's efforts on rail security have been delayed and nearly nonexistent, compared to aviation security. In light of this information, what immediate steps are we taking to increase rail security measures?

Mr. PISTOLE. Thank you, Mr. Chairman. Well, obviously, as soon as we got the word from the document exploitation from the bin Laden raid and the killing of bin Laden, we engaged, particularly, with our partners in the rail security, particularly Amtrak for the

Northeast Corridor, but all passenger and freight rail, noting the context for this information, coming from February of last year, and talking about an attack on passenger rail for the 10th anniversary of 9/11. So, it's still months away. But, we passed that information immediately and then worked with, particularly, Amtrak Police, and others, in terms of what they were doing, in terms of additional random, unpredictable patrols, both uniformed officers, canines, explosive trace detection—all those things that would serve as a deterrent, knowing that the three things the terrorists are looking for, in terms of deterrent, are additional police patrols, additional canines, or closed-circuit television cameras, as long as they're not suicide bombers, as we saw in London, on July 5 and 21 of 2005.

So, that's what we have done. We're obviously very much interested in the Transportation Security Grant Program and the outcome of Congress's decision on that, in terms of where that will be—how much money we'll have to support both the training efforts and the additional efforts that I've mentioned, in terms of things such as infrastructure protection, whether it's the Port Authority, Trans-Hudson, the PATH tunnels that you're so familiar with, shoring up those vulnerabilities, and other issues. So, those are some of the things we've done since that announcement.

Senator LAUTENBERG. Senator Boozman.

Senator BOOZMAN. Thank you, Mr. Chairman.

Mr. Lord, how much money has been spent on the project?

Mr. LORD. Since the inception of the program, it's approximately $420 million. And that includes $111 million in direct appropriations, $112 million in grants, including port security grants and transit security grants, and approximately $198 million raised in fees. Once you apply for a TWIC, you're to pay $132.50. So, that represents a significant share of the program proceeds.

Senator BOOZMAN. After looking, the ability to essentially very easily obtain a TWIC fraudulently, the fact that it looks like—am I reading it right?—of the 1,676,000, 460,000—over 460,000 criminals, only one has been denied?

Mr. LORD. Actually, we didn't have full visibility over that, but that's our understanding. Most—virtually all were approved, and the one was denied, as part of that adjudication process; once derogatory information is identified in the application process. That's our understanding, which we include in our report.

Senator BOOZMAN. Based on your investigation, would a normal driver's license from the states, now, that are required to do the—you know, much more background check than they used to, as far as who you are—would that be more secure identity than the TWIC card? Or, is it at least as secure?

Mr. LORD. It's at least as secure, probably, in many cases, more secure. That's our point.

Senator BOOZMAN. We've spent all this money, and right now—up to now, what we have is less secure than a driver's license.

Mr. LORD. Yes. And that was the purpose of our report, quite frankly. We identified some design flaws in the system—some holes. We think they can be patched. And we also raised an issue of facility training. The security guards play a key role in the process, and they, perhaps, need to be provided some additional train-

ing. They'll need to be a little more rigorous in scrutinizing the credentials, which are currently being used as a flash pass only. The biometric reader, that's the next stage of the program.

Senator BOOZMAN. And I guess, Admiral Cook, I would take exception to your remark about the TWIC card making us—you know, that we've had improvement by having it. And you can comment on this, too, Mr. Lord, and you, Mr. Pistole. But, the fact that we have this card that means nothing, or very little, because Mr. Lord's group has demonstrated it's very easy to get around it—to me, it makes us less secure than ever, because when your guys check this card, they, in good faith, feel like they're dealing—you know, this system—they have no idea that the card wasn't valid—then it gives them a false sense that they really shouldn't have at this point. Is that true or false?

Admiral COOK. Senator—and this is not to be argumentative in any way—the—I pretty—I'm starting, pre-9/11, in my mind. But, then one of the things that—as I said, we're looking forward to being able to move to the electronic reader. And what the Coast Guard has done to try to move ahead on that is, we deployed over 200 portable readers so that we can take advantage of that biometrics. It still does not account for someone that had a TWIC obtained based on fraudulent documents, because then the—biometric in the card.

Senator BOOZMAN. The point is, it's so easy to obtain these things fraudulently.

Admiral COOK. Well, the—as the mariners and workers——

Senator BOOZMAN. And this is not your problem. You're just the guy that's checking. I don't——

Admiral COOK. Right.

Senator BOOZMAN. But, again, I think it puts—you're all at a disadvantage.

Mr. Lord, who initiated the GAO study?

Mr. LORD. It was this committee and eight other Congressional committees.

Senator BOOZMAN. Did you find any evidence, as you were investigating, that anybody—the Coast Guard, TSA—were concerned about this prior to your investigating the—was this—did this seem something that was at the top of their radar, as far as concerns about safety and security in this area?

Mr. LORD. Oh, I think, absolutely, it was on their agenda; it was on their radar. But just contextually, we have completed a large body of work on TWIC-related issues over the last 5 years. We've worked very closely with TSA and the Coast Guard on this. We have a good, collaborative relationship, and they have taken steps to address some of the issues we identified in our report.

Senator BOOZMAN. Mr. Pistole, who in your agency—I find it remarkable—you know, if you talk to the truckers and people like that, you know checking records—and just employers, in general, you know, with drug screenings and—this doesn't have anything to do with drug screenings—but, just in general, checking people out, whether or not they're going to drive a schoolbus or whatever—it's remarkable that, of your people with a criminal record, there's such a low, low, low percentage of people that were flagged. Who in your

agency—who's responsible for that? What entity within TSA is responsible for making that decision?

Mr. PISTOLE. Well, of course, I'm responsible, overall, but the——

Senator BOOZMAN. No, but you don't check——

Mr. PISTOLE. Yes.

Senator BOOZMAN.—these things off.

Mr. PISTOLE. Right. But——

Senator BOOZMAN. Who does that?

Mr. PISTOLE.—TTAC, which is our credentialing group, is responsible for that.

And just, if I could, Senator——

Senator BOOZMAN. So, what is the name of that group?

Mr. PISTOLE. TTAC. It's T-T-A-C, the credentialing group.

And just for context, I think—so, I would say—I agree with a number of your comments—I would say we are more secure from the standpoint of, prior to any of these cards, somebody could use a driver's license, a union card, whatever it may be, that they just used to get access to the ports, with no——

Senator BOOZMAN. Mr. Lord has just testified that a driver's license is more secure than the card.

Mr. PISTOLE. So, if I could just finish, there—without any background check, necessarily—and so, at least, we're doing background checks now. Obviously, there are statutory provisions for people with criminal histories. And just by the nature of the workforce, a number of dockworkers may have had some criminal history. So——

Senator BOOZMAN. Right.

Thank you, Mr. Chairman.

Senator LAUTENBERG. Thank you very much.

Senator Begich?

STATEMENT OF HON. MARK BEGICH,
U.S. SENATOR FROM ALASKA

Senator BEGICH. Thank you very much, Mr. Chairman.

First, I want to thank you, Administrator Pistole, for one program called "Enroll Your Own," which is very important in our rural parts of Alaska, as you know. In order to have people to get the TWIC card is very expensive, complex for—and the travel in some of our fishing communities. And so, first I want to say thank you for that. We do have some suggestions we want to share with you—we'll do it for the record—from our police departments, who you work with.

Mr. PISTOLE. Good.

Senator BEGICH. And I think they have some very positive suggestions that I would hope you would consider as you continue to roll this program out.

Mr. PISTOLE. Sure.

Senator BEGICH. And I just want to issue a cautionary note, on the discussion here on criminal records and so forth—you hinted to it—in some of these industries, not everyone's going to have a stellar background, but are working in jobs that pay sometimes very low wages, and a variety of other things. So, I know that's a careful balance that you have to have.

My concern—and I don't know who wants to answer this. Let me, first, start with one example. And I may be a little off, here, but I'm using an example from my own—one of my own staff people, a loaner from one of the agencies, NOAA. Because he works on a ship and works on a dock, he goes through a whole process to get his card, his common access card—fingerprinting, all the 9 yards. Then he has to get a TWIC card, go through the same process. That seems such a simple fix, that if you've got a Coast Guard person that's required to go through and get their card, or a NOAA person, or any of these Federal agencies or government agencies, like a police department or maritime enforcement office, depending on if you're a coastal area, that, once they've done that, they shouldn't have to repeat that. Is that an easy fix that you can do?

Mr. PISTOLE. I will take that, Senator. It's not easy, unfortunately, but you've identified a key issue which is really overriding all these individual issues that we're talking about here today, and that's not only for the whole U.S. Government, in terms of having a universal access card, whatever that may be—of course every state has different standards. The National Institute of Standards Technology, of course, sets some standards that we abide by. But, that's the challenge that we deal with, that this goes—even in my last job, at the FBI, where there were all types of fraudulent documents because of differing standards by state and the federal government.

Senator BEGICH. But, you'll probably never get to the unified card of any kind. So, we have to take that as a given, even though I know, from a law-enforcement—as someone who was a mayor that managed a police department, you know, they would love to have one card, one place, one location. But, that will never happen, because of states' rights, and many other things. But, it seems, even in the Federal agencies—I think if a NOAA person or a Coast Guard person or—pick the agency—that goes through this already, that they shouldn't have to go through it again.

Mr. PISTOLE. So, there's——

Senator BEGICH. First, let me ask, does that make sense, that logic?

Mr. PISTOLE. Yes.

Senator BEGICH. OK.

Mr. PISTOLE. Absolutely.

Senator BEGICH. So, why not figure out—I know what we'd like to do, it seems, in the federal government, as I've learned now, is always get the big pitch, try to do it all at once, and do everything, which is disastrous. Example A, $300 million. You know, maybe we'll learn a little bit out of this. But, it seems like—why don't we just take one piece of the pie and try to deal with it and get it to work, rather than this holistic, which—you know, it sounds like another contractor making a lot of money on a system that doesn't work, that we'll probably never recoup anything from, and then they'll charge us more to do some more work.

Mr. PISTOLE. So, I agree, completely.

Senator BEGICH. It's the——

Mr. PISTOLE. You would think, Senator——

Senator BEGICH.—the federal M.O.

Mr. PISTOLE. Right. So, we are working on some proposed rulemaking that would help in that regard. Obviously, industry has a lot of interest and input into that. And so, as we work through this, unfortunately I believe it's a longer-term rather than a short-term fix. But, I agree completely with your philosophical approach of trying to consolidate and make it more efficient and effective for those who need these access cards.

Senator BEGICH. And then—but, I just give you a cautionary note. The standard thought is, "Well, let's try to figure out all the Federal—just take the Coast Guard, get them cleared up. Get the NOAA, get them cleared up." In other words, piecemeal it out so, each one, you're just trying to incrementally do. Is that a realistic approach, rather than this—it just makes me very nervous that we're going to try to do all of it at once and then, maybe a year and a half or 2 years from now, we'll have the same conversation, maybe with different people, maybe the same people, talking about more expense. Is that——

Admiral I don't know who. Mr. Lord? Whoever.

Mr. LORD. No, it makes perfect sense. I believe you're referring to consolidating the so-called security threat assessment process. Typically, when you go in for a credential now, they'll run a STA on you. To complete an STA, you may need another credential. They'll do it again. What they're doing is accessing the same—essentially, the same databases. So, they have an effort. They just started. They're trying to consolidate that. So, they, the Department of Homeland Security, wholeheartedly would agree with your position. And they're already taking steps to do that. Initial steps. But, that's the vision. You want to consolidate——

Senator BEGICH. Right.

Mr. LORD.—all that so-called background-checking process, and just have one person, one check——

Senator BEGICH. Right.

Mr. LORD.—rather than having one person, multiple checks. It's currently——

Senator BEGICH. Doesn't make sense, that latter part.

Mr. LORD.—inefficient, and it costs the consumer, the person applying for the card, more money.

Senator BEGICH. Let me just end with one question. The people that initiated this process—I know it wasn't under some of you folks, because some of you are new, obviously—but, the people below you who deal with all this, are they the same people that initiated this process, or are they new people? And the reason I ask that, sometimes—you know, there's my question. Because, I just heard a little knock on—to the left.

[Laughter.]

Senator BEGICH. Yes or no?

Mr. PISTOLE. Yes, mostly the same people.

Senator BEGICH. That's a problem. I'll leave it at that.

Senator LAUTENBERG. Thank you very much.

Senator Wicker.

STATEMENT OF HON. ROGER F. WICKER,
U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Thank you.

Gentleman, the results of the GAO report, I must say, are absolutely breathtaking. TSA has failed to implement and evaluate the TWIC Program in a way that provides reasonable assurance that only qualified individuals have access. GAO investigators were able to access secure facilities at U.S. ports during covert tests in which they presented either counterfeit TWIC cards, authentic TWIC cards, or cards obtained through fraud. GAO found that controls to identify the use of potentially counterfeit identity documents were not used to inform the background- checking process. TSA does not have clear criteria for applying discretionary authority to applicants who have past criminal convictions. And controls are not designed to determine whether cardholders have committed disqualifying crimes at the federal and state level after being granted a TWIC.

It seems to me that a decade of work has resulted in a system that would put Rube Goldberg to shame, and it almost argues for starting over from scratch and trying to design something that would work. I would mention again what Senator Boozman has pointed out, that of 460,000 TWIC applicants with a criminal record, TSA was able to deny access to one of those 460,000-plus applicants. I mean, it is absolutely astounding. But, the requirement has succeeded in making things harder on the applicants. And I have a report here from a constituent group, regarding TWIC card applications and the two-trip requirement. And I'll quote from this business, "The requirement that applicants make two trips to a TWIC enrollment center that may be hundreds of miles from their workplace or home represents a substantial burden on transportation workers across the country. A resident living in West Plains, Missouri, for example, must make, at minimum, two 350-mile round-trips to apply for and activate their card at the nearest enrollment center located in Memphis. Another worker in Meridian, Mississippi, must make, at minimum, two 267-mile round-trips to apply for and activate their card at the nearest enrollment center in Mobile."

So, for the honest worker who doesn't have a criminal background, he's got to make two trips. Mr. Lord, is there some way, in your judgment, that we could devise a system that does not require the two trips? I have confidence in the mail system. And it seems to me that receiving a card in the mail, then calling with secure information to verify that that card has been received, and then activated at that point, much like the credit cards are done, that something of that nature should be used to apply some common sense to the honest people that are being inconvenienced, to the tune of hundreds of miles.

Mr. LORD. No, that's an excellent question, sir. We recently looked at that, whether you could simply mail a TWIC card to an applicant's place of residence. It sounds easy. But, like many things, once you start looking into it, it's a little more complicated. And what we found was, the current policy of the Department is to remain aligned with the so-called FIPS 201 standard. This is a biometric security standard that pertains to all government credentials. As long as the policy is to remain aligned with that standard, it would preclude you from mailing it to an applicant's place of residence. Why? Because you have to do a biometric match, in person,

to ensure security. That helps limit potential fraud. And it's a key security enhancement. We had discussions with the NIST officials who crafted the standard—TSA, DHS; they agreed with our assessment. So, as long as that's their policy, the current policy is to remain aligned with that standard. Obviously, they could change the policy and have to reengineer their business processes, but as long as that policy remains unchanged, they cannot mail the TWIC to a person's place of residence.

To TSA's credit, they did add some flexibility to the program. In February 2009, they allowed the applicant to designate what enrollment center they'd like to pick it up. Sometimes people move. You apply for a TWIC in Seattle, say, and move to Memphis. You can now say, "I'd like to pick up my card in Memphis," without having to drive all the way back to Seattle. So, there has been some effort to respond to the needs of applicants. But, I cannot criticize them for requiring the in-person biometric match. That's a key part of the process.

Senator WICKER. Well, I would just simply suggest, as I yield back, that there are so many aspects of this program that are obviously going to have to be rethought, that we ought to put up the best minds in the country on some way to make this less burdensome on the honest folks that actually do comply.

Thank you.

Mr. PISTOLE. Mr. Chairman——

Senator LAUTENBERG. Yes.

Mr. PISTOLE. I'm sorry.

Senator LAUTENBERG. I'm sorry. Yes.

Mr. PISTOLE. If I may just respond on the one part to the Senator's question——

Senator LAUTENBERG. Sure.

Mr. PISTOLE.—just briefly.

Senator on the one denial, the overall numbers—we've actually denied over 35,000 people, for various disqualifying criteria. The one you're referring to is one who is an individual who had several criminal convictions, none of which was individually disqualifying, but, taken in totality, was disqualifying. So, it has actually been over 35,000. So, that's the whole purpose of that. We've also had several people who, it turned out, are on the terrorist watch list, who've applied for TWIC card, that have also been denied. And I could go into more detail in a closed setting on that.

Senator LAUTENBERG. Thank you.

Senator Snowe.

STATEMENT OF HON. OLYMPIA J. SNOWE,
U.S. SENATOR FROM MAINE

Senator SNOWE. Thank you, Mr. Chairman.

And just to follow up on the question on the enrollment centers which is obviously a problem in a state like Maine, where we only have two enrollment centers, one in Bangor and one in Portland. So, I'm going to explore with you the issue of distance. Do have you have any information regarding the impact it has on these workers to go long distances in order to secure the card and then have to go back and get it approved, and so on, and requiring two different

trips for these identity cards? And so, do you have any information on that? Who's——

Mr. LORD. Just to clarify, we audited the program, but we did speak to many applicants. And that was a persistent pain point, having to make two trips to get your credential. And I know there has been various discussions about how to mitigate that. They have portable enrollment centers. You can move certain enrollment centers around the country. But, again, I'm from GAO, not TSA. So, that's probably a better question for TSA.

Senator SNOWE. Mr. Pistole?

Mr. PISTOLE. So, Senator, yes, it's clearly less than ideal for most persons who are not located close. I have a map of where the permanent enrollment centers are. And, of course, they're located where most of these workers that would need them. We've also done several dozen of the mobile centers. And if there's a need in Maine that you've identified that would need one of these mobile centers, I'd be glad to take a look at that to try to facilitate that. So, we're—and also, by allowing the applicants to pick up their card at a different location, as noted, because they do move around and are—work in different places, it is a challenge, in trying to comply with the NIST standards, in terms of the best security, while also providing for the best convenience. So, that's the dynamic we deal with.

Senator SNOWE. Well, there is obviously a gap between the enrolled and the activated. So, is it your surmisal that they travel from one place to another—activate at one—enroll in one area and activate it in another location?

Mr. PISTOLE. Some of the applicants request that, because they're jobs have changed——

Senator SNOWE. Do they have to get prior approval for doing that?

Mr. PISTOLE. You know, I don't know that. I'll have to check on that.

Senator SNOWE. Well, somehow, we're going to just have to make this simpler. I just think it's cumbersome and bureaucratic. I mean, only 167 centers nationwide. So, it just—there must be a better way. I mean, I think about the amount of money that has already been spent on this program. Frankly, I think—the Chairman and I are probably one of the few members that were here on the Committee post-9/11, working on this very issue, and this was one of the issues that was identified as a priority. And that was back in the aftermath of 9/11. In 2002, we began this process. I think it was then former President Bush identified as, you know, having the identity of these workers established, and developing a system. And we will have spent $3.2 billion, and we've yet to clear all the hurdles to say that it's fully implemented and satisfied.

And so, I think it's—it—presenting enormous difficulties and complexity and failing to uphold the major standard, which is to confirm the identity of a cardholder. I mean, ultimately, that is not something that's been achieved at this point, it seems to me. And so, now we're going to spend all this money on biometric reading and digital devices, which are going to cost, as I understand it, up to $8,000 apiece. Is that correct?

Admiral COOK. That is correct, yes.

Senator SNOWE. It is. So—I mean, so there's another monumental cost. And next year, we're supposed to have—mandate the use of these cards. Are we going to be prepared for that?

Mr. PISTOLE. So, that is one of our challenges. And that's exactly why I've asked, along with Coast Guard and the Department, to—asking GAO to look the cost-benefit analysis of this whole program, because we do have hundreds of millions invested in it, between us, the U.S. Government, taxpayers, and industry. The question is, what's our return on investment? Are we clearly safer? Yes, we are. But, at what cost? And so, that's why we've asked for GAO to follow up on this.

Senator SNOWE. Well, I guess it's a red flag for all of us in Congress. I mean, I think if it takes so long to get a program up and running, something must be truly wrong, and we've got to decide differently, because it has been the better part of the decade, obviously, and we still haven't completed it. And yet, it's going to cost a great deal. I mean, it has been practically, what, from 2002 to 2012, essentially, and we're still not that much further ahead, in terms of where we need to be, and all the other problems that have been exposed.

In 2006, I introduced an amendment to the SAFE Port Acts that required a GAO report to review the various background checks among various agencies. Now, is there any way that we can sort of synchronize these background checks, you know, so that we can have one unified background check, in credentials, for workers, instead of, you know, multiplicity?

Mr. PISTOLE. So, that's what——

Senator SNOWE. Admiral Cook, and Mr. Pistole?

Admiral COOK. Well, Senator——

Senator SNOWE. Who's in charge on this one?

Admiral COOK. I'll go ahead and——

Senator SNOWE. OK.

Admiral COOK.—step up, Senator. But, I think the—you know, to answer your question, we're kind of at a pivotal time right now in the program, because the pilot reader program is being concluded. I don't know if you were in here when we mentioned it would—the Administrator mentioned that that data for the final report will be closed out at the end of this month. And then that report will come over to the Coast Guard, and that will be part of the background for our notice of proposed rulemaking to establish the readers.

So, I think, you know, in terms of the GAO audit, the work that has already been put into the TWIC, we are on the verge of being able to exploit the fundamental biometric data that we all wanted to achieve. And I know that the industry, who has been—you know, used to having the TWIC cards just flash passed us for the last few years, is anxious to move to that phase. They understand there'll be some costs. They're anxious to participate and help us get it right. And I think that's what I can offer at this time.

Senator SNOWE. Well, is it going to be interoperable in any way? I mean, are you—talking about this, you know, electronic reader—is that all going to be interoperable with other systems within government, or is it going to be stove-pipe?

Admiral COOK. The standards are—should be set, such that they were—have the ability to read several different kinds of cards. And

that's the—that will be a plus, right there. The—but, they'll be focused back to databases which relate to the TWIC, from what I understand right now. But, as I say, as a pivotal point, we can start integrating different aspects that the GAO has brought to our attention and that we already have some internal programs for.

Senator SNOWE. Well, is it—can we understand, then, that there's going to be harmonization of these security credentials, among agencies, or not? I guess that's the question.

Mr. Pistole?

Mr. PISTOLE. So, that's—Senator, that's one of the things, at least within the Department of Homeland Security, the Secretary is focused on, to ensure that, for example, just within TSA, we do vetting and credentialing for up to 15 million people in 28 different categories. So, there's a lot of that just within what we're doing. And that's what the Secretary is focused on.

Senator SNOWE. Thank you.

I ask unanimous consent to include my statement in the record, Mr. Chairman. Thank you.

Senator LAUTENBERG. Without any objection, certainly.

[The prepared statement of Senator Snowe follows:]

PREPARED STATEMENT OF HON. OLYMPIA J. SNOWE, U.S. SENATOR FROM MAINE

Thank you, Mr. Chairman for holding this hearing. As an original requestor of the GAO report presented today, I have great concerns about the Transportation Worker Identification Credential, or TWIC card, and the security of our nation's ports. For nearly a decade we have been grappling with many port security questions, and I think the report we see today identifies a need for review of current security practices. When we joined several of our colleagues to request this critical review of the TWIC, I believe you and I shared the view that when it comes to maritime security, we can, and must do better to protect our country's 360 ports and maritime facilities.

Biometric identification cards for transportation workers were one of the first security challenges addressed by Congress following September 11 in the Aviation and Transportation Security Act of 2001. In subsequent years, the mandate for identification for port workers was amended several times to define the ID we now call the TWIC. Since 2007, more than 1.7 million truckers, merchant mariners, longshoreman, and port workers have been issued these cards. Even the students at the Maine Maritime Academy have these $132 Federal security credentials to access the secure port facility on campus.

Secure ID cards like the TWIC are vital in insuring that access to critical port facilities is restricted to known-persons. In 2004, President Bush issued Homeland Security Presidential Directive Number 12, which among other things, required the Federal Government to establish a standard for "secure and reliable forms of identification" that must: (1) reliably identify an employee's identity, (2) be resistant to tampering or counterfeiting, (3) be rapidly authenticated electronically, and (4) be issued by providers whose reliability has been established. Unfortunately, we can see from today's report that the TWIC credential has failed on all counts.

The truth of the matter is, the implementation of the TWIC card has not increased the level of security at our ports as designed, and has become another example of bureaucracy at its worst. Not only do the cards fail to accurately establish that transportation workers are who they say they are, they fail to work as designed, require an unwieldy process to obtain, and add yet another redundant credential to the list of federal security cards.

Today's report indicates that the TWIC card may fail the first fundamental challenge of a security credential- accurately confirming the identity of the cardholder. GAO investigators were able to obtain TWIC cards by misrepresenting themselves as natural born U.S. citizens and by presenting forged birth certificates and drivers licenses. We're told that the documents presented can even be noted in the system as forgeries, but that these red flags are not accessible by the final adjudicator! Even if the TWIC processing center indicates a probable forgery, there is no path for review of the original documents presented.

Even worse, the production of a false card does not seem to be beyond the capability of a common criminal. Since the cards are often used as "flash passes" where card holders simply wave the card at a gate agent, the cards only need a passing resemblance to the true card. GAO inspectors were able to enter port facilities with false cards, unchallenged on a number of occasions! The lack of digital verification of TWIC cards is a critical failure in ensuring the effective use of the credential, and we must move forward quickly in deploying cost effective, equipment designed for a marine environment.

The TWIC cards have also so far failed to be rapidly authenticated electronically—most are worn as another badge, or presented for visual inspection, often from a distance of several feet. And the deployment of mobile readers suitable for ports has been slow at best. The substantial Federal investment of more than $400 million in the past 8 years, combined with the industry investment of approximately $200 million was designed to enhance and protect our nations ports, but I question if the program has been administered to provide the greatest security benefit.

In the next year, a mandate for the use of TWIC card readers will begin to roll out, and we must ensure that we invest wisely in technology that will add to our security, and not just our bottom line. I would like additional information from our witnesses on the costs associated with the technology requirements, and how to best utilize the readers to maximize their security impact.

The GAO report which we receive today also highlights significant concerns with the process used to vet applicants and reliably confirm the identity of individuals granted these security credentials. From asking workers to self identify a need for access to ports, and their place of birth, to incomplete verification of identity documents, it is clear that the security process for reviewing TWIC applicants has significant loopholes. I look forward to hearing from Administrator Pistole how TSA plans to address the concerns noted in the report.

Frustratingly, this is not only a security problem; the two separate visits needed to process TWIC credentials has a impact on trucking, shipping, and port workers and managers. Workers must first take the time to visit the enrollment center nearest them, which in some cases may be many miles away. At this time, Maine has only two TWIC enrollment centers of 167 nationwide. Students from the Maine Maritime Academy must travel the 50 miles from Castine, where the Academy is located, to Bangor, where the nearest TWIC processing center is located to begin the application, and back to the center again several weeks later to activate and pick up their TWIC card. While most of these locations are at, or near busy ports, with a highly mobile work force, this is a poorly thought out process that does not mirror the distribution of other Federal documents like passports which can be mailed to applicants.

Port workers, truckers, and other maritime professionals find themselves forced to obtain this additional security, often in addition to several other Federal issue identifications or endorsements. The TWIC is often carried in addition to Merchant Mariner Licenses, Merchant Mariner Credentials, and Commercial Drivers Licenses with Hazardous Materials Endorsements. How many times must the Federal Government screen and provide access credentials to a single individual? Can the departments of the Federal Government not work together to grant a single document to port and maritime workers to access and secure their workplace?

In 2006, I offered an amendment to the SAFE Ports Act, which required GAO to look into these Federal background checks for credentials like these. While GAO and DHS identified several credentials which can use the same background check information, I believe we must take additional steps to reduce duplication of effort and the unnecessary repetition of these background checks. We must implement common sense reform to ensure efficiency and maximize cost savings—credentialing operations should be streamlined by reducing the number of redundant offices and procedures.

I look forward to the testimony of today's witnesses, and I will be looking for information on how we can improve the credentialing process, the use of the card, and how we can adapt the use of the document to ensure the security of our nation's ports.

Thank you, Mr. Chairman.

Senator LAUTENBERG. And thank you, Senator Snowe, for your diligence in matters of security for our country, and particularly because the state of Maine has so much water access and ports that mean a lot. We thank you for your efforts.

The questions that have arisen here are obviously a small number of the questions that actually exist. And we kind of feel like we're looking at a Rubik's Cube here. You know, you don't know where to start and quite where to stop. And we're talking about somewhat safer, but I wonder if that can be—if that sentence can end—or, that expression can end with "somewhat safer," because I think there's also larger risk accompanying this because of the fraudulent nature of things.

And I ask, Mr. Pistole, when we know that GAO investigators were able to fraudulently obtain TWIC cards, use them for access to secure facilities—and these cards can be used to access literally thousands of facilities nationwide—so, what's being done to prevent fraudulently obtained cards from being used to access the airports, military bases? I think Senator Snowe was going there, as well. And can we do something that says, "OK, these cards are good for limited use, limited time periods—reenrollment is the question that you raised—biometric—I don't know—things that are visually protected. When I hear of the number of ineligibles that wanted to sign up for a card, it tells me that there is something really amiss in the basic structure.

And I ask you, any one of you, what—has there been an assessment of the program of any significance since its origination, some years ago?

Mr. LORD. Sure. We've, again, done a large body of work on this. I'd like to think we contributed to some better understanding of what some of the program's successes and weaknesses are. And when I think about this holistically, we're trying to apply this program, on a very large scale, in a so-called one-size-fits-all manner. I think that when you do something of this magnitude, it's really important to design it very carefully, number one, and, two, make sure your staff are well trained in implementing it. In our report, that's essentially what we found wrong, that we found some design imperfections; some of the information they collect at the front end isn't acted upon; and some of the security guards and trusted agents, which are delegated a large responsibility for making this thing successful, they had some lapses. Some of our covert investigators used fraudulent documents and the trusted agents should have flagged them. I can't really discuss any of the details, because it's sensitive security information. But, you know, we found some holes at the front end and at the back end, when the security guards are looking at these things and letting people on their facilities.

Senator LAUTENBERG. I'd almost like to ask that you—on a scale of 1 to 10, how comfortable we are with the progress that we've made, and this is not intended to be accusatory; it's intended to understand better where the problems are. I mean, the problems—we keep on, I think, discovering new problems as we move along here. And is the design an impossible one to make sense from? Or, what—anybody—I—you want to volunteer a quick opinion, Mr. Pistole?

Mr. PISTOLE. Sure, Chairman.

Senator LAUTENBERG. Admiral Cook?

Mr. PISTOLE. No, I think this hearing has identified a lot of the challenges in trying to deploy a biometric card to a civilian popu-

lation in—on a large-scale basis. And I think, although some progress has been made, it is clearly not what anybody intended, especially those going back to post-9/11. So, I have my own concerns. And that's why I've asked for the GAO to do, basically, a—just a top-to-bottom review to assess what that return on investment is.

The thing that I do have some comfort in is that we largely know about those who are working in ports now, and docks. The fact that they have access to a dock doesn't mean they have access to the ship or anything else. I mean, there are obviously multiple layers of security, here. What I'm concerned about is the ease of using a fraudulent document. We know there's, you know, tens of thousands, perhaps 35,000 places in the country you can get a birth certificate, hopefully legitimate, but perhaps not. And if that's a breeder document, that's a document you're using to establish your bona fides; that makes it very difficult. The social engineering, which Mr. Lord referred to, simply having one of his folks—undercover officers go in and, you know, say, "I have an appointment here," even though the card doesn't work, or, "I need to use the restroom." So, that gets to this—to the training of the guards. And so, there—it is a complex issue.

In answer to your question about 1-to-10, I would put it at a 3 right now.

Senator LAUTENBERG. Either one of you—I'm going to go to my colleagues for a second round of questions—in response to my question—it sounds like what we've got—we've got a new idea: we'll make prisons without bars, and maybe that will help control behavior. I don't think we're quite getting there.

Admiral Cook, do you——

Admiral COOK. Senator, I would say that I'm anxious to move to a phase where I believe we'll provide—we'll wring out some of the uncertainty when we go to more biometrics. And the reason I would say I'm anxious is, we have anecdotal evidence, because we have a strong network, through our area maritime security committees, where we're in constant contact with the facility security officers, the actual people paid, on the waterfront facilities, by their companies, to maintain security. And we have feedback that things like pilferage and other small crimes have been reduced. I don't have statistical evidence. I'm just saying it's all anecdotal. So, I would like to move past the anecdotes, past the feeling of the area maritime security.

Senator LAUTENBERG. Well, we agree.

Admiral COOK. And that—so, that's where I am.

Senator LAUTENBERG. Past the anecdotes. But, I'd like to move past the difficulties and the experiences that we've had.

Mr. Lord, before I call on Senator Ayotte, do you have anything you want to volunteer, here?

Mr. LORD. Again, a key program goal—I always like to go back to the program goals—there are four key program goals. One of them was to positively identify individuals applying for a TWIC. It's difficult to positively identify someone. What they do now is negatively identify. And all that means is, they run your fingerprints past the FBI criminal records checks, and if there's not derogatory information that comes back on that or the other database

checks, you're given a TWIC card. You could say you're Joe Blow, essentially have your fingerprints run, name checked; as long as no derogatory information comes back, you could be provided a card. And that's not positively identifying; that's a negative ID. So, it costs more, up front. It's more rigorous. They have to make a judgment whether there are additional steps they can take, up front, to positively identify someone, like you do with a driver's license; you have to show them your electric bill, show them some proof of documentation that you're a resident in the state with that name. There's more rigor, up front, involved. But, it makes for a better system.

Senator LAUTENBERG. Senator Ayotte.

Senator AYOTTE. Thank you, Chairman.

I wanted to ask, as I understand it—and whoever's most appropriate to answer this question—that part of the screening process would be to match it up against the terrorist watch list. And this, of course, makes sense, in terms of making sure that those individuals on the list don't receive cards. So, that is part of the screening process. Is that right?

Mr. PISTOLE. That's correct, Senator.

Senator AYOTTE. And have you ever had a situation where a TWIC applicant has actually been on the list—a known or suspected terrorist?

Mr. PISTOLE. Yes.

Senator AYOTTE. Can you give us a sense on how frequently that has occurred?

Mr. PISTOLE. So—infrequently, fortunately. And the actual number is sensitive security information. But——

Senator AYOTTE. Right.

Mr. PISTOLE.—it's a small number, out of the 1.8 million. But, yes, we do have—and I can give you the exact number—but, we do have a small number of people who are on the watch list who have applied and been denied.

Senator AYOTTE. And if that occurs, is the process denial?

Mr. PISTOLE. So, it would probably be denial. But, there may be an instance, because of the reason the person's on the watch list; and so we have to go back to the FBI or the intelligence community to see why they're on the watch list. Is there something—because, there are all different levels of reasons, whether it's material support, fund raisers, as opposed to bomb throwers. So, there may be something in there that would be mitigating.

Senator AYOTTE. So, is there a procedure in place to coordinate with other agencies—for example, the FBI—in terms of how you deal with someone on the watch list that applies for the TWIC?

Mr. PISTOLE. Yes. So, there is. But, in the process of preparing for this hearing, I've found something that we can improve that I don't want to go into in an open hearing. But, yes, there is a vulnerability there that we need to address, both between us and with the FBI.

Senator AYOTTE. Is that something that we could learn about in a more appropriate——

Mr. PISTOLE. Yes, absolutely.

Senator AYOTTE.—classified setting?

Mr. PISTOLE. Sure.

Senator AYOTTE. Because, I think it's very important. Because, obviously, one of the issues we wanted to address, post-9/11, was the coordination among agencies——

Mr. PISTOLE. Right.

Senator AYOTTE.—and making sure that, if we have that situation, that, if we need to create a situation where further intelligence-gathering has to occur, we're all working from the same page. So, I would really appreciate that answer in a more appropriate setting.

Mr. PISTOLE. Absolutely. I'd be glad to do it after this, if you have time. But, yes.

Senator AYOTTE. Great. Thank you. I appreciate that.

I also just wanted to share the concerns, as I understand, that have already been raised by my colleagues, and I raised in my opening statement, about figuring out a way where the multiple trips by the transportation workers to the enrollment centers, particularly those that live in areas that aren't so close to some of those centers. Is there a better way to do it? Can we do it in a more efficient way? And I know that many of my colleagues asked you about that, so I won't repeat that. But, I would echo their concerns.

Mr. PISTOLE. Noted.

Senator AYOTTE. And finally, to the extent you haven't answered this, but if you can help me with it—when you're in a position where DHS is doing multiple screening processes—and you mentioned it in your opening statement—so, one facility, for example, could be going through one type of process, and that same facility may have to get a screening from you in another process. What is it that you are doing to eliminate those redundancies that—you know, one of the concerns—it's not just a cost issue of how much the redundancies cost on both the applicant and the government cost, but also, when you've got the right hand and the left hand, you can end up in confusion. So, if you could address that, I'd appreciate it.

Mr. PISTOLE. Sure, Senator. So, there are a couple aspects to this. One is what we're doing, in terms of trying to limit the number of security threat assessments, the STAs, that would be done for somebody who has any type of government-issued ID that gives them access to something. So, we—15 million people, that I've mentioned, in the private sector, that we do some type of background and credentialing for them—so, do they—if they have, for example, a TWIC card, a hazardous material endorsement card, if they're an aviation worker—have access, or something—any number of things—and, of course, different things for other components—can we use that STA, that security threat assessment, that would apply to all of those? So, that's something that we're working through, just to streamline, make more efficient.

In terms of the enrollment, I know, between Coast Guard and TSA, we have consolidated some centers. So—and I would defer to the Coast Guard, in terms of the details of that—where a person would be able to go into a TWIC enrollment center and apply for something that would be a Coast Guard card. And so——

Senator AYOTTE. Can you help me, also, in thinking about this—is there one universal standard, or are there multiple standards

that—and can we move, in appropriate settings, to one universal standard for, obviously, similarly situated settings for threat?

Mr. PISTOLE. So, there's not——

Senator AYOTTE. That would seem simpler, from——

Mr. PISTOLE. Right.

Senator AYOTTE.—a government perspective.

Mr. PISTOLE. Yes. And that would be—and it would be good for industry in many respects. But, for example, the criteria and standards that would be used—that we use on a national level for TWIC cards is a different standard than individual—450 airports, for the—what they call the SIDA, the S-I-D-A, access—so—which are issued locally by each airport—and so, there—there's not constituency there. And then—so, there are a number of issues that we could peel back on that that would be helpful, that we are moving to try to address. There are a number of challenges there.

Senator AYOTTE. Well, you know, I appreciate that this is challenging. And I hope that, to the extent we can, we do move to a universal screening process for those that are in the same category. I can recognize that there may be additional screening for those in different categories, depending on the amount of risk that could be incurred, based on the activity.

Mr. PISTOLE. Exactly.

Senator AYOTTE. But, it seems to me that that would be a better way to rank it and rate it, based on risk of activity, with screening, so that we could use our resources more efficiently in a universal standard.

Mr. PISTOLE. Agreed. Agreed.

Senator AYOTTE. So——

Senator LAUTENBERG. The record will be open for further submissions.

Senator AYOTTE. Great.

Thank you very much.

Senator LAUTENBERG. I would ask a question, here, related to something Senator Ayotte was talking about, about trying to define risks regarding the individual who's applying for the card. But, I go further, and it's said, and I'm sure you're all aware, that New Jersey is home to the most at-risk area for a terrorist attack in the United States. The FBI said, the distance from the Newark Airport to the harbor is the most dangerous 2 miles in the country for a terrorist attack. There are 12 million people within a short radius of that area. So, shouldn't the TSA, Mr. Pistole—and either one of you, as well—prioritize these high-risk areas for TWIC funding and implementation, and move on these things in some kind of priority basis?

Mr. PISTOLE. Chairman, I think it—yes, exactly. And the—part of this fits in with what we are doing with what we're describing as a risk-based security initiative, and it applies as much to aviation as anything. But, that—this fits within that—that we expedite those in those high-risk areas, recognizing, similar to the Transportation Security Grant Program, that there are a lot of different opinions about how those funds should be allocated. There's also different priorities, depending on what outcome you're trying to achieve. So, clearly, those who have access to the most sensitive high-risk areas should be expedited, and we'll take that back.

Senator LAUTENBERG. Thank you.

This hearing is to be adjourned. And we will keep the record open. And I ask that, within some degree of promptness, that responses be given in writing.

And I thank you, Senator Ayotte, for being here and for your questions.

Thank all of you.

[Whereupon, at 4 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO HON. JOHN S. PISTOLE

Question 1. What specific efforts have been made to partner with the states to ensure that TSA is granted access to states' criminal records, and guarantee that important information is not being neglected from background checks?

Answer. The Department of Homeland Security, including the Transportation Security Administration (TSA), recognizes that there is additional information at the state level not available currently via the criminal history records information provided from the Department of Justice, Federal Bureau of Investigation (FBI).

TSA has worked with the states, FBI and the National Crime Prevention and Privacy Compact Council to convene working groups to identify possible solutions to receive data directly from other states and to identify a standard, automated, cost efficient and effective solution. TSA discovered multiple problems with obtaining information directly from the states:

a. The states have varying data systems, legal and practical constraints, and TSA would likely be required to develop and build a unique solution for each state in order to request data directly for each Security Threat Assessment (STA) case. To minimize these problems, TSA has discussed with the states an option of defining one common technical solution through which states could send their data directly to TSA. TSA is pursuing this effort as part of the Transportation Threat Assessment and Credentialing (TTAC) Infrastructure Modernization (TIM) program, which was established to standardize and consolidate TSA's security threat assessment systems.

b. Because many transportation workers have resided in and continually travel across multiple states, requesting and receiving state level data from only an applicant's state of residence or enrollment may miss criminal history in other states.

c. Some states may require additional fees to request and receive information directly, rather than using the FBI's system. Most TSA STA programs are primarily funded via user fees and this additional cost could dramatically increase the fees charged to workers.

For all these reasons, TSA has determined that using the established FBI Interstate Identification Index (III) system to request and receive data from all states would be the most effective and efficient solution. State level criminal history data may be accessed via the III system managed by the FBI. The extent of access to state level data is based on the purpose for the data request; however, a program must be deemed to have a criminal justice purpose in order to receive the full breadth of Criminal History Records Information (CHRI) available from all 50 states and the District of Columbia. Many states may not upload all available information into the FBI biometric system made available to TSA today, and many states do not provide their III records for "non-criminal justice" activities.

The Department of Justice has deemed that TSA's security threat assessments for TWIC and other similar programs are non-criminal justice activities. As a result, TSA is effectively provided the same access as an employer, and does not receive all available information. Additionally, TSA is not authorized to request subsequent CHRI for the purpose of conducting recurrent criminal background checks without a submission of new fingerprints from the individual.

To provide the most robust recurrent vetting against criminal history records, TSA needs full access to CHRI similar to the access granted to criminal justice agencies and law enforcement officers. TSA, in coordination with the Department of Homeland Security (DHS), has and will continue to work with the FBI, the National Crime Prevention and Privacy Compact Council, and states to expand access to the CHRI.

Question 2. The TWIC program currently does not make an effort to ensure that its holders are legally permitted to work under our immigration laws. Our immigration system is largely administered by the same department in which TSA is contained, the Department of Homeland Security, and it's no secret that individuals are permitted to work for different lengths of time, and that visas expire. Why doesn't the TWIC program reflect the reality of our immigration laws?

Answer. The design of the Transportation Worker Identification Credential (TWIC) vetting program seeks to ensure consistency with current immigration laws, including the need to accommodate visa holders who receive an extension to their stay.

TWIC leverages the capabilities of the Department of Homeland Security (DHS) as related to immigration. TWIC applicants who are not U.S. citizens undergo an immigration check using the U.S. Citizenship and Immigration Services (USCIS) Systematic Alien Verification for Entitlements (SAVE) data base. This check reviews an applicant's immigration status using TWIC-eligible immigration categories, developed as part of the rulemaking effort, that include visa categories that relate to working in the maritime industry. If the immigration check reveals information demonstrating that the individual is not in a TWIC-eligible immigration category, the individual is determined to be ineligible. If the check indicates that the individual may be in the U.S. illegally or improperly, the individual is determined ineligible and the Transportation Security Administration (TSA) coordinates with immigration authorities to take appropriate action.

Input from industry and stakeholders strongly suggested that linking the TWIC expiration date to a non-U.S. citizen's visa expiration date would be problematic. Industry feedback focused on minimizing the disruption to ports and the flow of commerce when a non-U.S. citizen's visa date was extended, as frequently happens. Electronic security features on the current TWIC make it impossible to extend the expiration date to reflect the extension of the visa. Furthermore, the TWIC expiration date is printed on the card. If the TWIC expiration was tied to the original visa expiration, the TWIC holder would have to assume the cost and process to get a new TWIC each time the visa was extended, or each time the individual came to the U.S. to conduct business. The ports would incur the economic cost of the individual's inability to access secure areas.

As an alternative, the determination was made that individual employers—at the local level—should track the visa information on their non-immigrant employees, as they are required to do by law already, independent of TWIC. Per the TWIC regulation, individual TWIC holders are responsible for returning their TWICs if they no longer meet eligibility requirements and employers are responsible for collecting an individual's TWIC upon the expiration of his/her work visa.

TSA believes believe the current process strikes a reasonable balance between ensuring only those who are in lawful status to work in the U.S. have access to regulated facilities and the need to accommodate business needs when visa holders receive an extension to their stay. Changing the requirement for the TWIC expiration date would entail significant changes to the current system and processes, including close integration with other DHS components and the Department of State, as well as oblige the TWIC holder to incur additional costs to obtain new credentials correlated with the duration of the individual's visa.

Question 3. The contractors running the TWIC program have only denied one application that came under their discretionary review authority. What sort of oversight is there for the 460,786 other applicants who were flagged by the first check, but ultimately granted TWICs? Is there any follow up to insure that the proper judgment was made about those individuals?

Answer. The Transportation Worker Identification Credential (TWIC) program employs contractors for the TWIC enrollment and operations, and separate contractors to assist with the high volume of TWIC applications to review background check information. The Transportation Threat Assessment and Credentialing (TTAC) staff makes the vast majority of initial denial decisions and all final denial decisions. The majority of the 460,786 approvals listed were made by the contractor after review of the background check information. TTAC provides a four-phased training program to all new adjudicators, both contractors and Federal employees, during which time the trainees are constantly evaluated. In order for a trainee to obtain status as a self-approver, he/she must pass a test administered by the government. After a trainee has been approved to be a self-approver, the government maintains a quality assurance process, where 5 to 10 percent of each self-approver's decisions are randomly reviewed each day to identify potential errors.

It is important to note that the statement from GAO concerning the adjudicator's denial of "one application that came under their discretionary review authority" relates to a sentence in the TWIC regulations (49 CFR 1572.107(b)) that permits the

Transportation Security Administration (TSA) to disqualify an applicant for "extensive foreign or domestic criminal convictions; a conviction for a crime not listed in 1572.103; or a period of foreign or domestic imprisonment that exceeds 365 consecutive days." TSA created this provision to cover the unusual circumstance of an applicant who appeared to pose a distinct "terrorism security risk" called for by the statute (46 U.S.C. 70105), but did not have serious criminal convictions listed on the specific list of disqualifying offenses. TSA never intended this provision to cover petty or frequent violators of the criminal code who, while perhaps untrustworthy and deceitful, did not pose a "terrorism security risk." TSA intended for the list of criminal disqualifiers and periods for disqualification that are set forth by statute and regulation to be the primary list we would use to evaluate an applicant as to criminal history. (In fact, as of March 2011 TSA has denied TWICs to 35,661 out of 1.8 million applicants.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO HON. JOHN S. PISTOLE

Question 1. It was discovered last week that Al Qaeda was planning an attack on a U.S. rail line. To date, TSA's efforts on rail security have been delayed, incomplete and nearly nonexistent compared to aviation security. In light of this new plot, what immediate steps are you taking to increase rail security measures?

Answer.

Mass Transit and Passenger Railroad Security

In response to the news that Al Qaeda was planning an attack on a U.S. rail line, the Transportation Security Administration (TSA) held teleconference calls with the Transit Policing and Security Peer Advisory Group (PAG) on Monday, May 2, 2011, and Friday, May 6, 2011. The PAG was established under the Sector Coordinating Council structure and serves as a vital component for the mass transit industry.

On the May 2 call, TSA encouraged all public transportation agencies to ramp up visible deterrence measures, and promoted the value of conducting unscheduled Regional Alliances including Local, State, and Federal Effort (RAILSAFE) operations.

During the May 6 call, the PAG members discussed increased rail security measures that their respective public transportation systems were implementing. Such measures include:

- Maintaining high levels of K9 units deployed, including vapor-wake teams on Amtrak trains
- Special briefings of engineers/track employees to emphasize reporting of suspicious activity along Right of Way
- Implementing special operations deployments
- Participating in Visible Intermodal Prevention and Response (VIPR) Team missions in critical locations
- Deploying Anti-Terrorism Teams
- Sending out awareness notices urging vigilance to transit police and employees
- Emphasizing the "See Something, Say Something" campaign
- Adding extra police patrols over the weekend

In addition to the independent security actions taken above, the public transportation agencies across the United States conducted a RAILSAFE exercise on Tuesday, May 5, 2011, which was stood-up in less than 24 hours, and involved over 90 agencies across 29 states and the District of Columbia, incorporating over 1,000 officers.

Going forward, TSA will continue Security Awareness messages and Operational Deterrence Programs, which include training, public awareness, K9 units, and VIPR Teams. The focus will shift from extended periods of time to shorter periods, such as months or weeks. TSA encourages continuing RAILSAFE operations on a random basis to prepare for various security threats.

Freight Rail

For nearly a decade, the freight rail industry, with guidance and assistance from TSA, has taken steps to reduce vulnerabilities within the freight rail network, specifically, the vulnerability of potentially dangerous cargoes. The industry has sought to raise the baseline of security by emphasizing employee training and awareness, and by instituting fundamental changes to daily processes that emphasize deterrence and increase the likelihood of detection of potential acts of terrorism.

Regarding the most recent intelligence that Al Qaeda had plans to attack trains or railroad infrastructure, the information garnered was non-specific and general in nature. As such, TSA immediately communicated with the freight railroad industry and advised them to continue a state of vigilance and awareness. The success of this increased vigilance was evidenced by the increase in reporting of suspicious incidents detected throughout the railroad industry.

In summary, TSA will continue to work closely with the freight railroad industry to ensure appropriate processes are in place that will enable them to meet emerging threats and continue to improve the baseline of security in the industry.

Question 2. The TWIC program has more than one point eight (1.8) million people enrolled across the country, from crane operators to Alaskan fishermen. All of these applicants have access to secure facilities throughout the United States with their TWIC cards. Plus, the current enrollment process doesn't even check to see if these applicants legitimately need access to secure facilities. Are you confident that the TWIC program is making our ports more secure?

Answer. The Transportation Security Administration (TSA) is confident that the Transportation Worker Identification Credential (TWIC) program has made the United States' ports more secure. Although the 1.8 million workers who have been issued TWICs are eligible to be granted unescorted access to secure areas of regulated facilities and vessels, they are not entitled or allowed to enter secure areas of facilities and vessels without the permission of the owners or operators of those facilities.

Prior to the implementation of TWIC, the identity document requirements for access to secure areas of ports and vessels were dependent on each facility's Facility Security Plan. Facilities often accepted a number of documents such as a driver's license, passport, state ID, port/facility specific security card, or a Z-card (now Merchant Mariner Credential). Without uniform credential issuance processes, most facilities were unable to positively authenticate the identity of an individual or determine the authenticity of the identity documents presented. There also were no universal methods for determining if a once-valid credential holder were no longer eligible for access privileges, or to effectively revoke an individual's access permissions or credentials. TWIC enhances maritime security by providing one standardized biometric credential, removing the need to have security personnel discern the authenticity of multiple identity documents. In addition, TWIC standardized the security threat assessment (STA) conducted on workers in these secure areas to include comprehensive terrorism, criminal history, and immigration checks.

In advance of a rule requiring reader use, ports are now made more secure by readers installed and in use through the recently completed TWIC reader pilot; the voluntary installation and use of readers at many facilities; and the more than 200 portable readers used by Coast Guard personnel to check TWICs during routine facility inspections. The use of these readers confirms that a valid TWIC is present, that it has not expired, and that it has not been revoked. In the biometric mode, the worker's identity is confirmed. Port security will continue to be enhanced as more electronic readers are put into use at secure facilities and vessels around the country.

Question 3. When the TWIC program expanded nationwide, most cards were issued within a short period of time—and most of those cards are set to expire in 2012. What is TSA doing to work with labor and industry to prepare for the expiration of the current credentials?

Answer. The Transportation Worker Identification Credential (TWIC) enrollments began in October 2007 when enrollment centers were phased in nationwide. Over the eighteen month period from October 2007 until the national compliance date of April 15, 2009, 1.1 million people applied for a TWIC. The Security Threat Assessment and associated TWIC for each applicant must be renewed every 5 years, for the credential to remain valid. Therefore, the expiration dates for the initial population of TWIC holders is spread out from October 2012 to April 2014 (5 years after the national compliance date). Preparations are being made in advance of the impending initial five-year renewal cycle. The Transportation Security Administration (TSA) is in the process of developing policies and procedures that will ensure a smooth renewal phase for the transportation workers who rely on this card to do their jobs. TSA's enrollment services contract provides for increased hours and days of operation, and additional equipment and personnel to meet fluctuating demands for service. These procedures both minimize the operational impact at TWIC enrollment centers, and ensure that individuals who have completed the redress process are not required to repeat the process when no new criminal information is found. This approach will help expedite adjudication during the expected surge in renewal

enrollments. Throughout this process, TSA will continue to engage the stakeholder community in order to minimize the impact of the renewal cycle on affected workers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JIM DEMINT TO HON. JOHN S. PISTOLE

Question 1. From GAO's "TWIC Security Review" (GAO–11–657):

"While TSA does not track metrics on the number of TWICs provided to applicants with specific criminal offenses not defined as disqualifying offenses, as of September 8, 2010, the agency reported 460,786 cases where the applicant was approved, but had a criminal record based on the results from the FBI. This represents approximately 27 percent of individuals approved for a TWIC at the time. In each of these cases, the applicant had either a criminal offense not defined as a disqualifying offense or an interim disqualifying offense that was no longer a disqualification based on conviction date or the applicant's release date from incarceration. Consequently, based on TSA's background checking procedures, all of these cases would have been reviewed by an adjudicator for consideration as part of the second-level background check because derogatory information had been identified. As such, each of these cases had to be examined and a judgment had to be made as to whether to deny an applicant a TWIC based on the totality of the offenses contained in each applicant's criminal report.

While there were 460,786 cases where the applicant was approved, but had a criminal record, TSA reports to have taken steps to deny 1 TWIC applicant under this authority."

Does the TSA track metrics on the number of TWICs provided to applicants with specific offenses defined as disqualifying offenses? If so, how many TWICs have been provided to such applicants? Is it accurate to conclude that an applicant with specific offenses defined as disqualifying offenses may only be provided a TWIC after receiving a waiver?

Answer. As of March 2011, TSA has enrolled and vetted over 1.8 million maritime workers. As a result of DHS's rigorous vetting process, 35,661 individuals were denied from receiving a TWIC. To clarify the quoted statement from the GAO report in the second paragraph of the question, that only 1 applicant has been denied a TWIC "under this authority", the authority is the 49 CFR 1572.107(b) provision of the TWIC regulation. This provision permits the Transportation Security Administration (TSA) to disqualify an applicant for "extensive foreign or domestic criminal convictions; a conviction for a crime not listed in 1572.103; or a period of foreign or domestic imprisonment that exceeds 365 consecutive days." TSA created this provision to cover the unusual circumstance of an applicant who appeared to pose a distinct "terrorism security risk" called for by the statute (46 U.S.C. 70105), but did not have serious criminal convictions listed on the specific list of disqualifying offenses. TSA never intended this provision to cover petty or frequent violators of the criminal code who, while perhaps untrustworthy and deceitful, did not pose a "terrorism security risk." TSA intended for the list of criminal disqualifiers and periods for disqualification that are set forth by statute and regulation to be the primary list we would use to evaluate an applicant as to criminal history.

TSA tracks metrics on the number of Transportation Worker Identification Credentials (TWICs) provided to applicants, with specific offenses defined as disqualifying, who apply for an appeal or waiver. TSA approved 44,444 appeal requests and 7,962 waiver requests as of June 5, 2011, that involve disqualifying criminal offenses.

An applicant, with specific offenses defined as disqualifying may also be provided a TWIC after approval of his/her request for an appeal where the applicant is able to prove that the disqualifying offense is out of scope (conviction is greater than 7 years old and release from incarceration on that disqualifying offense is greater than 5 years old), the conviction was later reversed on appeal, the applicant is not the person who committed the offense, or other fact that shows that the disqualifying offense standards have not been met.

Question 2. How many applicants with the following criminal offenses as part of their backgrounds have been issued TWICs through a waiver process?

a. A crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. § 70101. The term economic disruption does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employer-employee dispute.

Answer. 4 waivers approved

Question 2b. Improper transportation of a hazardous material under 49 U.S.C. §5124, or a state law that is comparable.

Answer. 22 waivers approved

Question 2c. Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device. An explosive or explosive device includes, but is not limited to, an explosive or explosive material as defined in 18 U.S.C. §§ 232(5), 841(c) through 841(f), and 844(j); and a destructive device, as defined in 18 U.S.C. § 921(a)(4) and 26 U.S.C. § 5845(f).

Answer. All crimes involving explosives, explosives devices, and/ or other lethal devices are classified in the same manner. 89 waivers approved

Question 2d. Murder.

Answer. 564 waivers approved

Question 2e. Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportations system, or an infrastructure facility.

Answer. All crimes involving explosives, explosives devices, and/ or other lethal devices are classified in the same manner. Question c. and e. are tracked as one metric with a total of 89 waivers approved for all explosive crimes.

Question 2f. Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961, *et seq.,* or a comparable state law, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the crimes listed in paragraph 49 C.F.R. § 1572.103(a).

Answer. All crimes involving Violations of the Racketeer Influenced and Corrupt Organizations Act are classified in the same manner. 26 waivers approved

Question 2g. Attempt to commit the crimes in paragraphs listed under 49 C.F.R. § 1572.103(a)(1) through (a)(4).

Answer. Attempts to commit the crimes in paragraphs listed under 49 C.F.R. § 1572.103(a)(1) through (a)(4) are not tracked separately.

Question 2h. Conspiracy or attempt to commit the crimes in 49 C.F.R. § 1572.103(a)(5) through (a)(10).

Answer. Conspiracy or attempt to commit the crimes in 49 C.F.R. § 1572.103(a)(5) through (a)(10) are not tracked separately.

Question 2i. Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. § 921(a)(3) or 26 U.S.C. § 5845(a), or items contained on the United States Munitions Import List at 27 C.F.R. § 447.21.

Answer. 942 waivers approved

Question 2j. Extortion.

Answer. 6 waivers approved

Question 2k. Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering where the money laundering is related to a crime described in 49 C.F.R. § 1572.103(a) or (b). Welfare fraud and passing bad checks do not constitute dishonesty, fraud, or misrepresentation for purposes of this paragraph.

Answer. 922 waivers approved

Question 2l. Bribery.

Answer. 12 waivers approved

Question 2m. Smuggling.

Answer. 9 waivers approved

Question 2m. Immigration violations.

Answer. 0

Question 2o. Distribution of, possession with intent to distribute, or importation of a controlled substance.

Answer. 2,968 waivers approved

Question 2p. Arson.

Answer. 61 waivers approved

Question 2q. Kidnapping or hostage taking.

Answer. 24 waivers approved

Question 2r. Rape or aggravated sexual abuse.

Answer. 281 waivers approved

Question 2s. Assault with intent to kill.

Answer. 4 waivers approved

Question 2t. Robbery.

Answer. 552 waivers approved

Question 2u. Fraudulent entry into a seaport as described in 18 U.S.C. § 1036, or a comparable state law.

Answer. 0 waivers approved

Question 2v. Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961, et seq., or a comparable state law, other than the violations listed in paragraph 49 C.F.R. § 1572.103(a)(10).

Answer. All crimes involving Violations of the Racketeer Influenced and Corrupt Organizations Act are classified in the same manner. Question f. and v. are tracked as one metric with a total of 26 waivers approved for all RICO crimes.

Question 2w. Conspiracy or attempt to commit the interim disqualifying felonies.

Answer. Conspiracy or attempt to commit interim disqualifying felonies are not tracked separately.

Question 3. From GAO's "TWIC Security Review" (GAO–11–657):

"TSA regulations provide that in determining whether to grant a waiver, TSA will consider: (1) the circumstances of the disqualifying act or offense; (2) restitution made by the applicant; (3) any Federal or state mitigation remedies; (4) court records or official medical release documents indicating that the applicant no longer lacks mental capacity; and (5) other factors that indicate the applicant does not pose a security threat warranting denial of a hazardous materials endorsement or TWIC."

These criteria generally, and (5) in particular, seem to grant broad latitude to TSA to grant TWICs to convicted felons. Please detail for the committee the guidance you have provided to your staff regarding the granting of waivers for disqualified individuals.

Answer. The waiver review regulation is designed to provide a framework, for subjective assessment of whether the Transportation Worker Identification Credential (TWIC) applicant has overcome the presumption that he/she poses a security risk, for reviewing the totality of the TWIC applicant's criminal background and circumstances. The Transportation Security Administration (TSA) has maintained extensive communication between TSA's Office of Chief Counsel (OCC) and Office of Transportation Threat Assessment and Credentialing (TTAC) to develop guidelines and training materials to accomplish waiver reviews and make waiver determinations. Each waiver request is assessed by obtaining and reviewing information from the applicant as well as pertinent law enforcement, legal, business, and community officials. Once sufficient material has been obtained and reviewed, a recommendation to grant or deny the waiver is made to the appropriate TTAC decisionmaking official, and the TTAC official makes the waiver decision.

According to 46 U.S.C. 70105(c)(2), TSA must develop a waiver program and give "consideration to the circumstances of any disqualifying act or offense, restitution made by the individual, Federal and State mitigation remedies, and other factors."

TSA proposed a list of disqualifying offenses and did not limit the crimes that are eligible for a waiver in its initial notice of proposed rulemaking, which was subject to broad public comment, and included consultation with the Department of Justice as part of the rulemaking process. Many comments asserted that criminal history generally does not give rise to the "terrorism security risk," as called for by the statute, and the list of disqualifying offenses should be much shorter than TSA's proposed list. Many feared that too many workers would be disqualified, and commerce and small businesses would suffer significantly as a result. Thus, TSA balanced a variety of important legal and policy issues in arriving at the current policy.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROGER F. WICKER TO HON. JOHN S. PISTOLE

Question 1. What steps were taken to identify security vulnerabilities in the TWIC program before it was implemented?

Answer. The Transportation Worker Identification Credential (TWIC) program followed the principle of establishing a chain-of-trust from the initial enrollment of an applicant to delivery of their TWIC. Best practices from other credentialing programs were reviewed and adopted as appropriate. Integrating document authenticating scanner technology to assist in identifying counterfeit documents, such as driver licenses and passports, and comparing a new applicant's fingerprints to those of previous applicants, to catch an attempt to enroll more than once, are two examples of adopting best practices from other programs.

The secure card technology and issuance procedures for a TWIC are very similar to the standards developed for government workers and contractors, specified for the Personal Identity Verification (PIV) card. The physical security features on the card meet the highest levels of counterfeit resistance specified by the Government. The procedures for issuing the TWIC ensure that the card is only delivered to its rightful holder.

Question 2. The information encoded in the TWIC cards includes sensitive information about the cardholders, including information that could be used to profile cardholders. What steps are taken to protect this information from being leaked to third parties?

Answer. Protecting personal privacy is a key component of the Transportation Worker Identification Credential (TWIC) program's mission statement. TWIC includes limited personal information contained on the card. The TWIC contains only three elements of personal information: name, facial photograph, and fingerprint templates for two fingerprints. The cardholder's name is printed on the card and encoded on the Integrated Circuit Chip (ICC) so that it may be freely read by a card reader. The facial photograph is also printed on the card and encoded on the ICC. However, it is encoded on the ICC such that it is protected from being viewed by a card reader without a Personal Identification Number (PIN)—selected by, and known only to, the cardholder. The fingerprint templates are stored in two locations on the card to facilitate use by either a TWIC reader or a Personal Identity Verification card reader. In the first case, the algorithm is encrypted to prevent disclosure of the template if an attempt is made to "skim" (*i.e.,* the practice of intercepting information from a smart card using a device without the knowledge of the card holder) the card using radio-frequency technology. To decrypt the algorithm, a cardholder must physically "swipe" or insert his/her card into a reader. Thus, an unencrypted fingerprint template cannot be obtained without the cardholder's action. In the second case, the algorithm is available only after entering a PIN.

Note: A fingerprint template is a compact digital representation of distinct characteristics derived from a fingerprint image. Fingerprint templates are used as the basis for comparison during biometric authentication.

Question 3. After the Agency addresses the problems cited by the GAO report, how will it evaluate those remediation steps to determine that they close the gaps the GAO identified?

Answer. The Transportation Security Administration (TSA) is currently working to initiate the recommended controls assessment of the Transportation Worker Identification Credential (TWIC) program. As part of this assessment, a method will be established for each control enhancement that defines how TSA will monitor the effectiveness of the change. While the evaluation technique will depend on the remediation method, TSA plans to continue unannounced system and operational audits regarding key security areas. In addition, reporting mechanisms will be created that will assist TSA in ensuring that any new security procedures are being followed.

Question 4. Robust and effective cybersecurity and the protection of freight information systems are important elements in port security for the United States. Among other important goals of port security are the ability to reliably and economically detect weapons of mass destruction that may be hidden in containers and cargo. Additionally it is important to verify the trustworthiness of foreign shippers. The compromise of data and information systems that relate to these vulnerabilities would represent critical risks to national security. Has the cybersecurity of port security systems, and related freight information, been addressed?

Answer. Yes. All U.S. Customs and Border Protection (CBP) systems, including port security systems, abide by the Federal Information Security Management Act (FISMA) of 2002. FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. CBP has developed a robust Certification and Accreditation program to align with the goals and objectives of FISMA. Additionally, the Security and Technology Policy Branch ensures that port security systems align with DHS Sensitive Systems Policy Directive 4300A and CBP Information Systems Security Policies and Procedures Handbook 1400–05D.

The National Cyber Security Division (NCSD), within the National Protection and Program Directorate's Office of Cybersecurity and Communications, is working with its public and private sector partners to address industrial control systems security and general cybersecurity at port and shipping facilities. Its Control Systems Security Program (CSSP) provided resources to conduct high-level assessments in Boston, Houston, and Norfolk. The assessment reports are still in development. Using the Cyber Security Evaluation Tool, CSSP will be conducting evaluations at ports

and terminals located at the top ten facilities, based on a ranking by the Department of Transportation's Bureau of Transportation Statistics, as well as Maersk Shipping. In 2009, CSSP conducted several evaluations of freight rail facilities, as well as a port facility in Saipan, Commonwealth of the Northern Mariana Islands.

Question 5. What evaluations, assessments, and tests have been performed to determine whether other port security systems under the agency's purview, such as freight information systems, can be compromised as readily as the GAO was able to with the TWIC program?

Answer. CBP employs a defense-in-depth approach to security. As a component of FISMA, a detailed and thorough Security Test and Evaluation (ST&E) of port security systems is conducted. Testing includes personal interviews, scans of workstations, websites and data bases, and a physical site assessment to find and mitigate potential vulnerabilities. Additionally, CBP site risk assessments are performed to evaluate the site's security posture. Risk assessments are performed continuously throughout the calendar year. Each port security system also has a dedicated Information Systems Security Officer (ISSO) who handles day-to-day security for the system. ISSO duties include daily/weekly log file examination, review of the CBP Security Operations Center monthly enterprise vulnerability scans, and oversight of configuration management.

NCSD's Critical Infrastructure Protection—Cyber Security (CIP–CS) program is in discussions with the Maritime Sector Specific Agency (U.S. Coast Guard) to scope a Maritime Sector-wide cybersecurity risk assessment. This assessment would focus on identifying and assessing risks to categories of cyber critical infrastructure that support Maritime Sector critical functions. CIP-CS is conducting this work in support of the critical infrastructure and key resources cross-sector community to identify cyber critical infrastructure and support sector-wide approaches to cybersecurity risk management.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO REAR ADMIRAL KEVIN COOK

Question 1. The Coast Guard uses a risk analysis model to inform decisions on how best to secure our nation's ports and allocate limited resources. Could the Coast Guard model be applied to TWIC to assess its effectiveness and to enhance security?

Answer. The Coast Guard Maritime Security Risk Analysis Model (MSRAM) is a terrorism risk analysis tool and process used by Coast Guard analysts across the nation to perform detailed risk analysis for their areas of responsibility. The results of this process are used to support a variety of risk management decisions at the strategic, operational, and tactical levels.

During the initial rollout of TWIC, MSRAM data was used as part of a risk analysis approach in developing TWIC reader requirements in the maritime sector, and MSRAM will continue to provide risk analysis support to TWIC. However, since MSRAM is a risk analysis tool and not designed or capable of being used as a measure of effectiveness, it is not an appropriate model to assess the effectiveness of TWIC.

Question 2. It has been more than 9 years since the TWIC program was created, but ports still do not have readers for the cards. Instead, they rely on visual verification, which can be more susceptible to fraud. How much will it cost to install readers at ports across the country and who is expected to pay for it?

Answer. The Department of Homeland Security managed the TWIC pilot through the joint participation of TSA and the Coast Guard. The Coast Guard plans on using data from the TWIC Pilot Program, along with other studies and reader vendor data, to estimate the costs to fully implement the final card reader phase of the TWIC program. The Coast Guard is working on publishing a Notice of Proposed Rulemaking in the *Federal Register* that will present estimates of the costs to install readers at affected port facilities and present the number and types of affected facilities that will need to install readers. The cost of readers, as well as any necessary installation, will be incurred by the affected facilities. The ports may apply for grants to fund installation.

TWIC Projects are eligible for funding under the FEMA Port Security Grant Program (PSGP). TWIC related projects have been specifically funded since FY06 or earlier and identified as a PSGP priority since FY07. TWIC Readers and associated equipment have been specifically identified as the major component of over $88M of PSGP funded projects since FY06. Project size, scope, and costs vary greatly among ports, and TWIC projects may typically include readers, cameras, fencing, gates, lighting, and associated installation costs as part of the overall project.

Question 3. According to the FBI, New Jersey is home to the most at-risk area for a terrorist Answer. attack in the U.S. This area has targets ranging from the port to airports to chlorine gas plants. An attack in this area could impact 12 million people who live nearby. Shouldn't TSA prioritize these high-risk areas for TWIC funding and implementation?

Answer. It is essential that the prioritization for TWIC funding and reader implementation be consistent across the Nation. Those facilities and vessels that present the highest risk, or are in high-risk areas, will be prioritized accordingly, as they were in the initial TWIC implementation.

Question 4. GAO investigators were able to fraudulently obtain TWIC cards and then use them to access secure facilities. TWIC cards can be used to access literally thousands of facilities nationwide. What is being done to prevent fraudulently obtained cards from being used to access airports, military bases, and other secure facilities?

Answer. Each port establishes the requirements for access to its secure facilities. Possession of a TWIC, while a necessary element for access, does not guarantee its holder the right of access absent meeting the business case that individual port authorities establish for entering their secure facilities. The Coast Guard works with the ports to ensure the enforcement of security practices for access to secure facilities.

Another important enhancement will be the use of card readers to verify TWICs electronically and ensure that the cards have not been revoked. The Coast Guard is currently developing an upcoming rulemaking that will include requirements for TWIC readers at Maritime Transportation Security Act (MTSA) regulated facilities and vessels. Once the final card reader phase of the program is implemented for electronic verification of TWICs, it will significantly enhance protection against counterfeit, tampered, or expired TWICs being used to gain access to MTSA-regulated facilities and vessels.

Finally, TSA is conducting a review of internal controls for TWIC enrollment to identify ways to enhance the program's ability to prevent people from obtaining a TWIC using fraudulent identity documents. Almost all credentialing programs at all levels of government and the private sector face this challenge. TSA follows best practices by requiring the use of document authentication technology as a safeguard against TWIC applicants using counterfeit or altered identity documents at enrollment. DHS will continue to seek out best practices and new technologies to ensure that TWIC takes every reasonable precaution against fraud.

UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE
Washington, DC, July 6, 2011

Hon. FRANK R. LAUTENBERG,
Hon. BILL NELSON,
Committee on Commerce, Science, and Transportation,
U.S. Senate.

Subject: Transportation Worker Identification Credential: Responses to Posthearing Questions for the Record

On May 10, 2011, I testified before the Committee on Commerce, Science, and Transportation on the Department of Homeland Security's (DHS) credentialing program known as the Transportation Worker Identification Credential (TWIC). This letter responds to the three questions for the record that you posed. The responses are based on work associated with previously issued GAO products.[1] Your questions and my responses follow.

Question 1. Through your covert testing, you were able to obtain fraudulent TWIC cards and access secure facilities using fraudulent and counterfeit cards. What potential security threats are our ports and other secure facilities exposed to because of the problems with the TWIC program?

Answer. We reported in May 2011 that internal control weaknesses in TWIC enrollment, background checking, and use could have contributed to the breach of Maritime Transportation Security Act (MTSA)-regulated ports during covert tests

[1] See GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, GAO–11–657 (Washington, D.C.: May 10, 2011); *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, GAO–11–648T (Washington, D.C.: May 10, 2011); and *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO–10–43 (Washington, D.C.: Nov. 18, 2009).

conducted by our investigators.[2] We had our investigators conduct covert testing at TWIC enrollment center(s) to identify whether individuals providing fraudulent information could acquire an authentic TWIC. Further, during covert tests of TWIC use at several selected ports, our investigators were successful in accessing ports using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases (*i.e.,* reasons for requesting access). Our records show that operations at the ports our investigators breached included cargo, containers, and fuel, among others.[3] Our investigators reported that throughout the testing, security officers did not question the authenticity of TWICs presented for acquiring access.

According to the Coast Guard's January 2008 National Maritime Terrorism Threat Assessment, al Qaeda leaders and supporters have identified western maritime assets as legitimate targets.[4] Moreover, according to the Coast Guard assessment, al Qaeda-inspired operatives are most likely to use vehicle bombs to strike U.S. cargo vessels, tankers, and fixed coastal facilities such as ports. If an individual presents an authentic TWIC acquired through fraudulent means when requesting unescorted access to the secure areas of a MTSA-regulated facility or vessel, the cardholder is deemed not to be a security threat to the maritime environment because the cardholder is presumed to have met TWIC-related qualifications during a background check. In such cases, individuals who wish to do harm to the maritime transportation system could better position themselves to inappropriately gain unescorted access to secure areas of a MTSA-regulated facility or vessel.[5]

As we recently reported in May 2011, while one of the goals of the TWIC program was to improve security by reducing risks associated with fraudulent or altered credentials by using biometrics to positively match an individual to the credential, as our covert tests demonstrated, an authentic TWIC and a legitimate business case were not always required in practice.[6] As detailed in our report, inspection of TWICs with biometric readers is not currently required. Rather, TWICs are primarily used as visual identity cards—known as a flashpass—where a card is to be visually inspected before a cardholder is allowed unescorted access to a secure area of a MTSAregulated port or facility. The investigators' possession of TWICs provided them with the appearance of legitimacy and facilitated their unescorted entry into secure areas of MTSA-regulated ports at multiple locations across the country. If individuals are able to acquire authentic TWICs fraudulently, verifying the authenticity of these cards with a biometric reader will not necessarily reduce the risk of undesired individuals gaining unescorted access to the secure areas of MTSA-regulated facilities and vessels. Our report noted that, unlike prior access control approaches, which allowed access to a specific facility, the TWIC potentially facilitates access to thousands of facilities once the Federal Government attests that the TWIC holder has been positively identified and is deemed not to be a security threat.

Question 2. According to the FBI, New Jersey is home to the most at-risk area for a terrorist attack in the U.S. This area has targets ranging from the port to airports to chlorine gas plants. An attack in this area could impact 12 million people who live nearby. Shouldn't TSA prioritize these high-risk areas for TWIC funding and implementation?

Answer. Funding for the TWIC program is a shared responsibility between the Federal Government and the private sector. TSA's efforts to issue the TWIC are to be funded by enrollment fees collected from TWIC applicants.[7] Additional resources, however, would be required if TWIC is to be implemented with biometric card readers. For instance, MTSA-regulated facility operators could be required to expend resources on TWIC readers and infrastructure to support TWIC-related operations, such as installing fiber optic cables and investing in computing system(s) capable of managing and recording TWIC-related access control efforts. While funding for such efforts is anticipated to be the responsibility of facility operators, limited Federal funding is expected to be available through Federal grant programs, such as

---

[2] GAO–11–657.

[3] The details related to the means used by the investigators in the tests could not be described here because they were deemed sensitive security information by TSA.

[4] U.S. Coast Guard Intelligence Coordination Center, *National Maritime Terrorism Threat Assessment* (Washington, D.C.: Jan. 7, 2008).

[5] The TWIC program requires individuals to both hold a TWIC and be authorized to be in the secure area by the owner/operator to gain unescorted access to secure areas of MTSA-regulated facilities and vessels. A regulation on the use of TWICs with card readers is currently under development and expected to address how the access control technologies, such as biometric card readers, are to be used for confirming the identity of the TWIC holder against the biometric information on the TWIC.

[6] GAO–11–657.

[7] TSA was authorized to fund the program's operations by collecting $196.8 million in enrollment fees from TWIC applicants from Fiscal Years 2008 through 2010.

the Federal Emergency Management Agency's (FEMA) Port Security Grant Program and the Transit Security Grant Program.[8] As we previously reported, issuance of such grants is, in part, based on available risk information.[9]

Funding and implementing TWIC in a risk-informed manner would be consistent with our prior work.[10] The purported benefit of making risk-informed investments is that Federal funds are to be directed at those programs that are most effective at reducing risk given available resources. However, as we reported in May 2011, DHS had not assessed the effectiveness of TWIC at enhancing security or reducing risk for MTSAregulated facilities and vessels.[11] Further, DHS had not demonstrated that TWIC, as currently implemented and planned with readers, is more effective than prior approaches used to limit access to ports and facilities, such as using facility-specific identity credentials with business cases. Moreover, our May 2011 report found that enrollment and background checking processes were not designed to provide reasonable assurance that only qualified individuals could acquire TWICs, or that once issued a TWIC, TWIC-holders had maintained their eligibility. These weaknesses, coupled with the results of our covert tests on TWIC use, raise questions about the effectiveness of the TWIC program. As such, we recommended that the Secretary of Homeland Security evaluate the costs, benefits, security risks, and corrective actions needed to implement the TWIC program in a manner that will mitigate existing security risks. Completing these steps will facilitate efforts to identify high-risk areas for TWIC funding and implementation.

Question 3. We have four of the highest volume U.S. ports in Florida, which are involved in tens of billions of dollars in trade each year. Did your investigators turn anything up unique about the efforts made by the folks running the TWIC program in Florida?

Answer. Prior to being amended, previous Florida state law required workers accessing the state's 12 active deepwater public ports to undergo a state criminal history records check, and Florida's ports required workers to obtain a local port identification card. In doing so, Florida had implemented background check and identification requirements that extended beyond those of the TWIC program. First, prior to being repealed on May 24, 2011, a Florida statutory provision required that all applicants undergo a State of Florida fingerprint-based criminal history records check to identify certain specified state criminal offenses, such as theft and burglary, separately from those specifically required to be identified or considered by the criminal history records check conducted by the TWIC program. Second, Florida denied access to individuals who had obtained their TWIC through the TWIC-waiver process, whereby individuals with disqualifying offenses could be granted a TWIC. Third, Florida maintained a database that retained the fingerprints and eligibility status of all seaport workers accessing its ports, and provided ports with an ongoing notification of the workers' criminal histories. While Florida has repealed its background check requirements, various Florida ports still require that individuals attempting to gain access to a port or facility provide a port-specific identification card in addition to the TWIC to gain access to ports in Florida.

As we reported in May 2011, our investigators were successful in accessing ports using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases (*i.e.,* reasons for requesting access) during covert tests of TWIC use at several selected ports.[12] Information on the specific ports and locations that our investigators were unable to access during covert testing was deemed sensitive security information by TSA. However, our report states that our investigators did not gain unescorted access to a port where a secondary port specific identification was required in addition to the TWIC.

---

[8] From Fiscal Years 2006 through 2010, $111.7 million had been made available to maritime facilities implementing TWIC from FEMA grant programs—the Port Security Grant Program and the Transit Security Grant Program.

[9] See GAO, *Transit Security Grant Program: DHS Allocates Grants Based on Risk, but Its Risk Methodology, Management Controls, and Grant Oversight Can Be Strengthened*, GAO–09–491 (Washington, D.C.: June 8, 2009); and *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO–06–91 (Washington, D.C.: Dec. 15, 2005).

[10] See GAO, *Homeland Security: Applying Risk Management Principles to Guide Federal Investments*, GAO–07–386T (Washington, D.C.: Feb. 7, 2007); and GAO–06–91.

[11] GAO–11–657.

[12] GAO–11–657.

If you have any questions about this letter or need additional information, please contact me at (202) 512–4379 or *lords@gao.gov*.

STEPHEN M. LORD,
Director, Homeland Security and Justice Issues.

○