FEDERAL GOVERNMENT APPROACHES TO ISSUING BIOMETRIC IDS

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS
OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEETH CONGRESS

FIRST SESSION

MAY 9, 2013

Serial No. 113–25

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

81–281 PDF WASHINGTON : 2013

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
DOC HASTINGS, Washington
CYNTHIA M. LUMMIS, Wyoming
ROB WOODALL, Georgia
THOMAS MASSIE, Kentucky
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
KERRY L. BENTIVOLIO, Michigan
RON DESANTIS, Florida

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
JACKIE SPEIER, California
MATTHEW A. CARTWRIGHT, Pennsylvania
MARK POCAN, Wisconsin
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
DANNY K. DAVIS, Illinois
PETER WELCH, Vermont
TONY CARDENAS, California
STEVEN A. HORSFORD, Nevada
MICHELLE LUJAN GRISHAM, New Mexico

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
STEPHEN CASTOR, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

JOHN L. MICA, Florida, *Chairman*

TIM WALBERG, Michigan
MICHAEL R. TURNER, Ohio
JUSTIN AMASH, Michigan
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
JIM COOPER, Tennessee
MARK POCAN, Wisconsin

CONTENTS

FEDERAL GOVERNMENT APPROACHES TO ISSUING BIOMETRIC IDS

Thursday, May 9, 2013,

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT OPERATIONS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 9:00 a.m., in Room 2154, Rayburn House Office Building, Hon. John Mica [chairman of the subcommittee] presiding.

Present: Representatives Mica, Massie, Meadows, Connolly, and Cummings.

Staff Present: Ali Ahmad, Majority Communications Advisor; Alexia Ardolina, Majority Assistant Clerk; Molly Boyl, Majority Parliamentarian; Sharon Casey, Majority Senior Assistant Clerk; Adam P. Fromm, Majority Director of Member Services and Committee Operations; Linda Good, Majority Chief Clerk; Ryan M. Hambleton, Majority Professional Staff Member; Michael R. Kiko, Majority Staff Assistant; Mitchell S. Kominsky, Majority Counsel; Mark D. Marin, Majority Director of Oversight; Laura L. Rush, Majority Deputy Chief Clerk; Scott Schmidt, Majority Deputy Director of Digital Strategy; Jaron Bourke, Minority Director of Administration; Devon Hill, Minority Research Assistant; Lucinda Lessley, Minority Policy Director; Rory Sheehan, Minority New Media Press Secretary; and Cecelia Thomas, Minority Counsel.

Mr. MICA. Good morning. I would like to call this subcommittee hearing of Government Operations Subcommittee of the House Government Oversight and Reform Committee to order.

Welcome, everyone, this morning. The topic of today's hearing is Federal Government Approaches to Issuing Biometric IDs. It looks like a relatively brief hearing. We have two witnesses that will be participating and I will introduce them shortly.

The order of business today, we will hear members' opening statements, then we will hear from our two witnesses, and then we will have a round or rounds of questioning, as appropriate.

So, with that, let me again welcome everyone. I want to again state on behalf of the committee that we believe we have a very important mission of oversight. This committee exists for a very fundamental purpose, two basic principles. First, the American people have the right to know how their money is spent that Washington has taken from them. We have the fiduciary responsibility of seeing how it is expended and what programs are successful, what are unsuccessful, making certain, first of all, that the American public, our Nation is secure.

And I think, finally, the American public deserves an efficient, effective Government that works for them. We have that important responsibility in this committee and we intend to protect those rights. We want to hold Government accountable for the taxpayers and make certain that we, through these hearings and the proceeding today, that we keep the executive branch and others charged with important responsibilities true to the intent and legislative purpose that Congress has set forth.

So that is our purpose. I look forward to working with Mr. Connolly, our ranking member, and members of the subcommittee to continue this effort, and thank them for their cooperation this morning.

On November 25th, 2002, then—President Bush signed the Maritime Transportation Security Act of 2002. That is more than a decade ago and that legislation set forth the credentialing for individuals that are entering some of our port facilities and regulated facilities that accommodate vessels and maritime traffic.

According to the GAO, from 2002 to 2012, an excess of half a billion dollars has been spent in that effort, some $540 million. About a quarter of a billion dollars raised on fees from some of the workers and other folks, and then about a quarter of a billion dollars in public money and grants.

According to CRS, since we first issued the cards in 2007, about 2,001 cards have been issued. The cost initially was $129.75 for the past number of years and there is a proposal now that some of the workers can extend their cards for a fee of $60. The card was intended from the very beginning, and having participated in that process, to have a biometric component, to be a secure, durable identification that could ensure the identity of those entering, again, those secure areas in our port facilities.

We have had at least four hearings that I know of, some on the Transportation Committee, some on some subcommittees, reviewing the progress of this card. I think if you will look at a poster child for programs that sort of run amok and do not get the job done, that the TWIC card, as it is affectionately known, Transportation Worker Identification Card, is unfortunately the poster child, again, for not producing what I think Congress intended.

Despite all the time that has lapsed, the hearings that have been conducted, GAO continues to find that TSA is failing to properly administer the TWIC program. The latest report we have has just come out. This is March 2013. It cites a whole host of problems with the program. First of all, we wanted the card produced with biometric capability. The card had some capability, fingerprint; it doesn't have iris, as I understand it. The cards were issued. Since 2007 the cards have not had the capability of having a reader. Congress had passed additional legislation trying to get the reader program engaged, and we will hear today that while GAO is testing some of the equipment, that we still do not have readers deployed in a universal manner to read the cards.

So what you have is a farcical system of a card that, and not by my evaluation, but previous GAO studies have shown, is not what we intended; it is tamperable. It has actually been, in testing by GAO, it has been found to be deficient and, again, it is a card that can also be easily reproduced.

So what you have is, again, a card that is produced at great expense to individual workers, great expense to the Government; does not have a guaranty that it is a secure card, that is, tamperable; it has become a joke among transportation workers because at almost every port they are now required to produce a driver's license or some other identification that is used for entry.

So this sort of goes on and on. After, again, spending an incredible amount of money, TSA and the independent tests agent, they found did not even have a clear record of baseline data for comparing operational performance at access points with the TSA readers. This is in the testing. GAO went on to find that TSA and the independent test agent did not collect complete data on malfunctioning TWIC cards.

I know this is a long explanation of where we are, but I think it deserves sort of an update for the record. We again are faced with more than a decade delay in producing what Congress intended. Now years have gone on trying to get a reader that is approved.

The final thing I would just point out to Mr. Connolly and other members is other agencies do have cards. Most recently, here is our TWIC card, a little mockup of it. Again, I think some of you may have seen this before, the TWIC card, again flawed. Here is a clear card which a private company has produced, and it actually has biometric, both fingerprint, and I think it is all five fingers, and iris; and it is in use. We found other agencies that have readers and they also have cards that have both components that Congress was trying to get some years ago.

So this is very frustrating and the purpose of the hearing is to review where TSA is and where we are going to go.

With that, I would like to recognize our ranking member, Mr. Connolly.

Mr. CONNOLLY. Mr. Chairman, thank you, and thank you for your leadership on this issue and for holding this hearing. I can't help but observe there are two lonely members of the press at the press table. Yesterday we had dozens and dozens and dozens.

Mr. MICA. This isn't Benghazi.

Mr. CONNOLLY. And yet the Benghazi hearing basically uncovered nothing. Actually, today's hearing potentially has so much more of an impact in terms of U.S. security, but I guess it is not a particularly sexy subject, at least when it comes to the media. But I think it is very important to our Country's security.

And again I thank you for your leadership, Mr. Chairman. I know you cared about this in your previous capacity at Transportation and Infrastructure as chairman, and I am so glad you bring that sensitivity to this committee as well.

All of us want to make sure that our transportation system is secure. Every day our transportation system moves more than 1.4 million shipments of hazardous materials, any of which could be potentially of harm to Americans. As we all know, securing all of this cargo is very daunting, but we know it is imperative to the safety of the Nation.

The Maritime Transportation Security Act of 2002 requires the Department of Homeland Security to issue a biometric transportation security card, TWIC, to identify individuals who will be al-

lowed unescorted access to the secure areas of ports and vessels. The biometric information contained in the card includes, of course, as the chairman indicated, fingerprints and a digital photograph. TSA is responsible for the issuance of the card, while the United States Coast Guard is responsible for enforcing its use.

TWIC cards are intended to be utilized with an electronic reader that would simply scan the card to determine entry into the respective facility. Under the Safe Port Act of 2006, DHS was required to conduct a pilot program on the efficacy of the TWIC card readers. Unfortunately, the most recent GAO report, which we are going to hear about today, found significant methodological problems with the study.

Specifically, GAO determined that TSA lacked data analysis plans, performance standards, or sampling methodology development prior to selection of participating facilities and vessels in the TWIC reader pilot. In addition, GAO also found that the finalized TWIC cards did not undergo any level of durability testing, which is problematic considering the use of these cards will be in sometimes harsh, wet, maritime environments, which was also cited by the GAO report.

These findings are disappointing and of great concern. I, for one, want to know why the Department has not responded favorably to GAO's serious findings, if in fact they have not. We look forward to hearing about that today.

If the readers and the TWIC cards fail to function properly, not only will maritime workers not be able to perform their jobs adequately on a daily basis, but these facilities are left vulnerable to a potential security breach. Given the volume of cargo coming into the United States, that is of great concern. The United States transportation system of maritime facilities remain a target and a means through which terrorists seek to attack the homeland. We all know that an attack on our Nation's maritime transportation system could have very serious consequences, and it seems to me all of us have got to do everything in our power to make sure that does not happen.

I look forward to hearing from our witnesses this morning and what corrective measures we can take to make TWIC an effective security card.

With that, I yield back, Mr. Chairman.

Mr. MICA. Thank you, Mr. Connolly.

Also, I will just explain for the members of the panel that we attempted to look at IDs across the board, because TSA is at the heart of approval and DHS is at the heart of approval of moving all these ID programs forward. We were not able to get Customs and Border Patrol to participate today, nor Department of State and some others that we wanted; they wanted more time.

So, unfortunately, what we have done is divided this review up. We will, hopefully in a couple of weeks, and with the agreement of the minority, reconstitute the panel and we will look at problems with the pilots' license, there are problems with the various cards that we have for identification. At the airports we have a global entry under the Department of State.

But I think all of these, and it is part of our responsibility. We are the only committee with enough jurisdiction to look at all of

these, and then also TSA's responsibility. So we will follow up on that.

With that, let me recognize Mr. Meadows, then we will go to the ranking member, Mr. Cummings, of the full committee.

Mr. MEADOWS. Thank you, Mr. Chairman, and thank you to the ranking member, Mr. Connolly, who has, over and over again, expressed a willingness to work in a bipartisan way to cut out waste, fraud, and abuse.

As we are here today obviously looking at some half billion dollars spent on a program that is yet to be implemented, I am reminded of the fact that there are two ways things get done here in Washington, D.C., slow and never, and we are trying to figure out which one of these this particular thing is going to be, because we have heard testimony in this very room of computer systems that we have spent some $1 billion on, then was never implemented.

So is this just another government program where it has great intentions of providing security, but in essence we are going to spend millions and millions, and perhaps billions of dollars only to find out later that the theory or the genesis of this particular security system is one that is not going to be implemented?

The most recent GAO report is troubling from some of the accusations and literally some of the research that it is providing here, so I look forward to really less looking at when are we going to have a system that secures our ports. We have been at this for some 11 years now. So if not next year, then when? If not next year, then are we looking at another 10 years? What is the time line? And from a practical standpoint what are the deficiencies? Would we be better off to just say we made a mistake, let's go back to the drawing board, let's find another area to do it?

I have the privilege of having Google in my particular district, and I can tell you the type of security that is there with those facilities didn't take this long to get implemented in the private sector and, quite frankly, are extremely secure. So if the private sector can do it, certainly we, with all of our resources of the greatest Nation in the world, should be able to figure it out. So I look forward to your testimony.

With that, I yield back, Mr. Chairman. Thank you so much.

Mr. MICA. I thank the gentleman.

Now I am pleased to recognize the ranking member of the full committee, the gentleman from Maryland, Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman and Ranking Member Connolly, for calling this hearing. And I want to thank the witnesses for their testimony.

This is a subject that is of great interest to me because I previously served as the chairman of the Subcommittee on the Coast Guard and Maritime Transportation, and during my tenure in that position I convened two hearings to examine the rollout of the TWIC card, which began, unbelievably, in 2007.

Now, six long years later, 2.5 million transportation workers have been enrolled in the TWIC program and 2.7 million TWIC cards have been printed. These enrollees have paid an estimated $300 million to implement this program. However, those TWIC

cards are nothing more than very expensive flash passes without sophisticated electronic readers to read them. That is sad.

We now know that many vessels and facilities will never use TWIC readers, yet workers there are still being required to obtain the TWIC card. The Coast Guard, which is responsible for enforcing the use of the TWIC cards, has recently issued a Notice of Proposed Rulemaking that would require only vessels and facilities in what are known as Risk Group A classification to utilize TWIC card readers. As a result, far less than 1 percent of regulated vessels and approximately 16 percent of facilities will require a TWIC reader.

So the TWIC card is just a very expensive flash pass for all the mariners and transportation workers working in the 99 percent of vessels and more than 80 percent of facilities without TWIC card readers.

But the problems with the TWIC card program run deeper than that. Where TWIC card readers will be required, they must be able to determine whether a card is valid and matches the biometrics of the individual who seeks access to a restricted area in a port or on a vessel. Unfortunately, we cannot count on that. When the GAO reviewed the TWIC pilot program required by the Safe Port Act, it identified methodological problems with the pilot that are so severe GAO has concluded that the results of the pilot are simply not reliable.

I am stunned by the scope of the shortcomings identified by the GAO, particularly given that as long ago as 2009 GAO identified shortcomings that needed to be addressed to ensure the TWIC pilot program would yield reliable results.

We are all aware that we need to take every effective step to protect our maritime facilities from those who wish to harm us. However, at this time we still have no reliable data proving that the TWIC card is one of those steps.

I can simply say I am disappointed and we are better than that. As my colleague said just a moment ago, if the private sector can do this, we ought to be able to do this, and we need to know exactly why we can't.

When I was chairman of the Coast Guard subcommittee, Mr. Chairman, I constantly talked about, I was really talking about the Coast Guard and its acquisition program, but talked about how we were moving into a culture of mediocrity; and I think this whole fiasco is a step below that. So I am hoping that we will get some answers, that we will get some results soon so that the intended purpose of the TWIC card will be able to carry out the way we wanted it to be done.

With that, I yield back.

Mr. MICA. Well, I thank the ranking member and concur in his very frank statement. We will work together. We have to figure out a way to get this program back on track.

No other members this morning, so I will ask unanimous consent that members have seven days to submit opening statements for the record. Without objection, so ordered.

So now we will turn to our two witnesses this morning. First we have Mr. Steve Sadler, and he is the Assistant Administrator for

Intelligence Analysis for the Transportation Security Administration.

Welcome back, Mr. Steve Lord. He is the Director of Forensic Audits and Investigative Services for GAO, the Government Accountability Office.

Gentlemen, this is an investigative panel of Congress. If you will stand and be sworn. Please raise your right hand.

Do you solemnly swear that the testimony you are about to give before this subcommittee of Congress is the whole truth and nothing but the truth, so help you, God?

[Witnesses respond in the affirmative.]

Mr. MICA. Let the record reflect that both witnesses answered in the affirmative.

We aren't too pressed for time this morning, so we will give you a little bit of leeway. Usually it is a little briefer, but we will recognize first Mr. Sadler, the Assistant Administrator for Intelligence and Analysis at TSA.

Welcome and you are recognized, sir.

STATEMENT OF STEPHEN SADLER

Mr. SADLER. Good morning, Chairman Mica, Ranking Member Connolly, and distinguished members of the subcommittee. Thank you for the opportunity to testify today about TSAs role in the TWIC program.

TWIC is a fee-based program that issues a tamper-resistant biometric credential. Eligible maritime workers use TWIC for unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002. TSAs primary areas of responsibility include conducting security threat assessments, providing customer service at enrollment centers, and engaging industry to develop specifications for TWIC readers.

The full enrollment fee for a transportation worker is $129.75, and an initial TWIC is valid for five years. Under the Extended Expiration Date Initiative, eligible workers may request a three-year extension by paying the $60 card replacement fee.

Currently, the United States Coast Guard requires maritime operators to visually inspect the TWIC prior to granting unescorted access to secure areas. Under MTSA, the Coast Guard currently regulates nearly 14,000 vessels and more than 3200 facilities. With a single uniform credential, facilities, vessel operators, and law enforcement entities can verify an individual's identity and eligibility to enter secure areas with a higher level of confidence than was feasible prior to TWIC. TWIC is an important layer in maritime security as risk-based control requirements and technical capabilities mature.

TWIC readers determine whether a card is authentic and issued by TSA. The readers also check that the card has not expired and has not been revoked or reported lost or stolen. The Coast Guard recently published a proposed Notice of Rulemaking on TWIC readers in which the use of those readers would be required for certain high-risk vessels and facilities.

Recently, several major challenges have converged for the TWIC program. These include the expiration, re-enrollment, and demand

for replacement of 1.5 million TWICs over an 18-month period; modifications to the process to limit enrollment and card issuance to a single visit; and a transition of the program from a current single-provider contract to separate contracts for enrollment services and system operations.

Beginning this summer, the first phase of an initiative to enable individuals to apply for and obtain a TWIC with a single visit to an enrollment center will be tested in Alaska and should expand nationwide in 2014. One visit represents the most significant program change since TWICs inception and will greatly ease the burden on future applicants and individuals needing a replacement card.

Additional customer service improvements include expanding the number of TWIC enrollment centers from 136 to more than 300; increasing call center representatives focused on reducing call wait times; developing a web-based process to apply for extended expiration date TWICs or replacement cards; and increasing mobile enrollment opportunities to facilities wanting to enroll workers onsite.

As a result of the TWIC pilot program, we obtained considerable data and sufficient quantity and quality to support the general findings and conclusions in the pilot report. Our analysis concluded that TWIC readers function properly when they are designed, installed, and operated in a manner consistent with the characteristics and business needs of the facility or vessel operation. The analysis also concluded that reader systems can make access decisions efficiently and effectively.

Thank you for the opportunity today, and I will be glad to answer any of your questions.

[Prepared statement of Mr. Sadler follows:]

Statement of

Steve Sadler

Assistant Administrator for Intelligence & Analysis

Transportation Security Administration

U.S. Department of Homeland Security

Before the

United States House of Representatives

Committee on Oversight and Government Reform

Subcommittee on Government Operations

May 9, 2013

Good morning Chairman Mica, Ranking Member Connolly, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today about the Transportation Security Administration's (TSA) role in the Transportation Worker Identification Credential (TWIC) program.

The security of the maritime environment is complicated, and like our land and air borders, a layered approach offers the best defense. To fulfill a security mission of such scale, DHS leverages the expertise of its components to evaluate the entities that comprise the maritime domain and design security measures to counter potential threats. The fee-based TWIC program is mandated by the Maritime Transportation Security Act of 2002 (MTSA, P.L. 107-295) and administered jointly by TSA and the United States Coast Guard (USCG).

The program requires careful planning and consultation with an array of public and private sector partners in addition to agility in responding to the concerns of workers while

ensuring national security. Under the program, eligible maritime workers are provided a tamper-resistant biometric credential for unescorted access to secure areas of port facilities and vessels regulated under MTSA. This credential is referred to as the "TWIC card," or just the "TWIC." In carrying out the TWIC program, TSA is responsible for enrollment, security threat assessments (STA), and systems operations and maintenance related to TWICs while USCG is responsible for enforcement of regulations governing the use of TWICs at MTSA-regulated facilities and vessels.

As of April 15, 2009, TWICs are required to be presented when requesting unescorted entry to secure areas of MTSA-regulated facilities nationwide, which provides a security benefit by demonstrating to facility and vessel security operators that the TWIC holder has successfully passed the STA. While a TWIC is valid for five years and costs the transportation worker $129.75[1], on August 30, 2012 DHS announced that eligible workers may submit a request to extend the expiration date on their TWIC by three years and pay a $60 card replacement fee under the Extended Expiration Date (EED) initiative through December 31, 2014. The EED is a one-time initiative to allow workers to extend their TWIC until readers are required. While the TWIC is an important step towards improved security, the security benefits of the TWIC are most fully realized when used with readers that can confirm that the person presenting the card is the person to whom it was issued.

The TWIC Program and National Security

TWIC provides a uniform, industry-wide, biometric, tamper-resistant credential that is issued following successful completion of the STA. TSA began the national deployment of the

[1] The fee is reduced to $105.25 if the worker uses a comparable STA to establish TWIC eligibility.

TWIC program on October 16, 2007, with the enrollment of maritime workers at the Port of Wilmington, DE. To date, TSA has conducted comprehensive STAs for over 2.5 million workers and has prevented approximately 50,000 individuals from obtaining a TWIC because they did not meet the required security standards.

Currently, USCG requires maritime operators to visually inspect the TWIC prior to granting unescorted access to secure areas on board regulated vessels and at facilities. Under MTSA, USCG regulates approximately 13,825 vessels and 3,270 facilities. Use of this common credential enables facility and vessel operators, as well as Federal, state, local, tribal, and territorial law enforcement entities, to verify the identity of individuals and their eligibility to enter secure areas with a higher level of confidence than was feasible prior to TWIC. The TWIC program's common credential will be critically important as risk-based access control requirements and technical capabilities mature.

TWIC readers determine whether a card is authentic, valid, and issued by TSA. The readers also check that the card has not expired and, by accessing the cancelled card list, can determine if the card has been revoked or reported lost or stolen. When used in the biometric mode, readers confirm through a biometric fingerprint match that the person using the card is the rightful owner of the card. The TWIC card and reader system can perform these checks virtually anywhere with portable or fixed readers because connectivity to an external database is not required. On March 22, 2013, USCG published a notice of proposed rulemaking (NPRM) which would require TWIC readers for certain high-risk vessels and facilities. This is expected to further enhance security at those sites by providing verification of the validity of the TWIC card and of the identity of the owner.

TWIC and Hazardous Materials Endorsement STA Comparability

TWIC is an example of a strategic security partnership among the USCG, TSA, and the private sector. TWIC is one layer, within the array of maritime security measures mentioned above, that enhances port facility and vessel security. Since the beginning of the TWIC program, truck drivers holding a Hazardous Materials Endorsement (HME) have been able to obtain a TWIC based on their HME STA and pay a reduced fee $105.25. Also, beginning in February 2012, TSA made it possible for truck drivers to apply for an HME based on an existing TWIC STA. Through this effort, drivers with valid TWICs in those states that have systems and procedures in place to offer comparability do not have to re-submit fingerprints and can pay a reduced fee for HME enrollment. To date, 24 states have implemented comparability for their HME applicants.[2]

Instituting New Policies to Meet Ongoing Challenges

TSA and USCG have addressed a number of challenges in implementing the TWIC program over the past year. This included 1) the expiration of 1.5 million TWICs over an 18-month period with the resultant demand for re-enrollments and replacement cards; 2) realignment of the TWIC system to comply with the new congressional mandate to limit enrollment and card issuance to one visit; and 3) transition of the program from the current single-provider contract to separate contracts for enrollment services and system operation. Departmental leadership conducted an analysis of the TWIC program, including port operations, in considering reader requirements and identifying customer service improvements. DHS also initiated a formal DHS Acquisition Review Board (ARB) that met in March 2013. DHS

[2] Other states have not been able to offer comparability due to state regulatory and/or system constraints.

leadership prioritized the program to focus on enhancing customer service and successful transition among contractors.

The ARB will continue to meet periodically to gather additional information on challenges facing the TWIC enterprise and to find solutions to those challenges. In addition, an Executive Steering Committee, co-chaired by the TSA and USCG leadership, has been established to address TWIC concerns and issues.

Customer Service Improvements Include "OneVisit"

TSA will soon implement the "OneVisit" initiative designed to ease the burden on eligible applicants and individuals needing a replacement TWIC. The first phase of the initiative to enable individuals to apply for and obtain a TWIC with one visit to an enrollment center will begin with a test in Alaska this summer and is expected to expand nationwide in 2014. Under OneVisit, applicants will visit an enrollment center to enroll and, upon completion of a satisfactory security threat assessment, a card will be produced and mailed directly to the applicant. OneVisit will ease crowding at enrollment centers by eliminating the visit currently required to activate the card and select a PIN.

In addition to OneVisit, we are planning additional customer service improvements including expanding the number of TWIC enrollment centers from 136 to over 300 sites. We are also implementing a robust oversight effort to gauge sustained customer service at our enrollment centers and will be increasing call center representatives in order to reduce call wait times. DHS is developing a web-based process to apply for EED TWICs or replacement cards to increase convenience for TWIC holders and also plans to increase mobile enrollment opportunities.

The Qualified Technology List Process

TSA is committed to partnerships with stakeholders, including the private sector, to carry out its mission. To meet the demands of the TWIC program, TSA will soon provide MTSA-regulated facility owners and operators with a list of TWIC readers that meet current TWIC specifications. TSA established the Qualified Technology List (QTL) process on November 1, 2012, with the announcement that three National Voluntary Laboratory Accreditation Program laboratories were accredited to accept readers for compliance testing.

Prior to the announcement, TSA worked with the National Institute of Standards and Technology as well as independent laboratories and industry to provide QTL workshops and test cards to all interested parties. The QTL process also provides industry with a formal, repeatable, and standardized approach for certifying readers and reporting the results to TSA. Once each reader is certified, TSA will update the publicly available QTL with information on the new reader.

The TWIC Reader Pilot Program

In October 2006, Congress mandated that DHS conduct a TWIC reader pilot to inform its approach to implementing reader requirements. The Department delegated responsibility for conducting the pilot to TSA. The TWIC reader pilot obtained considerable data that has been helpful in evaluating reader performance and assessing the impact of using readers at maritime facilities. TSA's analysis concludes that TWIC reader systems function properly when they are designed, installed, and operated in a manner consistent with the characteristics and business needs of the facility or vessel operation. The analysis also finds that reader systems can facilitate access decisions efficiently and effectively, though there were operational and technological

difficulties that affected performance at some pilot locations. These conclusions and other information in the pilot report are some of the many sources used by the USCG in drafting the aforementioned TWIC reader NPRM. Additionally, the USCG will use pertinent information received during the rulemaking process from affected parties to further evaluate the use and performance of the reader program.

Conclusion

Prior to the TWIC Program, there was no standard identity verification or background check policy for entrance to a port facility or vessel. This created vast opportunities for fraud and risk. Today, facility and vessel owners and operators look for one standard identification document that confirms the holder's identity, and verifies that he or she successfully completed an STA. TWIC cards contain security features that make the card highly resistant to counterfeiting. When biometric verification becomes a requirement and readers are in use, we expect this will further enhance security at port facilities and vessels regulated by MTSA.

TSA and its partners have taken significant steps to add layers of security to protect our nation's port facilities and vessels. These steps link together information sharing, security, and law enforcement from across TSA, USCG, DHS and a multitude of partnerships. Each security layer builds upon and complements the others. TWIC is one of those layers. Thank you for the opportunity to discuss the TWIC program. I am available to answer any questions.

Mr. MICA. Thank you.

We will turn now to Mr. Steve Lord, the Director of Forensic Audits and Investigative Services for GAO. Welcome back.

STATEMENT OF STEPHEN A. LORD

Mr. LORD. Thank you very much, Mr. Chairman, Ranking Member Connolly, and Representative Meadows. I am really pleased to be here today to discuss the results of our recent TWIC report issued just recently. I should point out this is not the only report we have issued on this subject. We have work going back several years, including a very significant study we issued in 2009 on the design of the pilot, as well as a May 2011 report on the internal controls in the program.

The overall message that I wanted to convey today, I think it is a very important message, that the pilot results should not be used to inform future decisions regarding the TWIC reader rule or the future deployment of card readers. This is where we disagree with TSA and DHS. I am also surprised to see that the Coast Guard went ahead and issued their March 22nd Notice of Proposed Rulemaking, because it incorporated the results of the pilot even though we found major issues in the pilot data, which we had previously shared with them.

I would like to briefly touch on some of the key challenges we identified in the pilot. They fall into three major buckets. The first one is planning. Bottom line is DHS did not address the pilot planning weaknesses we identified in our 2009 report. Although it took some initial steps to address them, it did not develop a full evaluation plan or the performance standards we called for to help guide the pilot as it unfolded.

The second key issue we identified was related to data collection. We identified eight separate weaknesses in how the pilot participants collected data. I am not going to discuss all eight today, but I would like to briefly highlight three.

First, TSA and the independent test agent did not record clear baseline data. If you don't have a clear baseline, you really have nothing to compare the collected data to.

They also did not collect complete data on reasons for card failures or the reasons people were denied access to facilities. Obviously, they collected some, but we scrutinized the data they did collect and we found several significant discrepancies and anomalies in the data.

The third key data collection issue we identified was the operational impact of using TWICs with readers was not consistently documented. And this is a really important issue because this was one of the major reasons they ran a pilot, to measure the business impact on the private sector. Yet, when we looked at how they measured that, they didn't do a good job and they essentially did not collect the data needed to assess that issue.

As a result of all the challenges we identified, we think it is really difficult to assess whether the problems experienced were due to the cards themselves, to the readers, or to the way the users were using them. So it could have been a combination of all three, and that is something we highlight in our report.

We also scrutinized DHS's report to Congress. I should mention we just didn't evaluate the report; we looked at what went into the preparation of the report. We pulled all available data sets that were used to support the February 2012 report to Congress.

And one notable issue we identified was the assessments of the entry times at ports, again, the throughput times. This is a really important issue that was looked at, where these measures were mixed up with reader response times, which is the time it takes a card to be read in a laboratory setting. So obviously they weren't really measuring throughput, which is a key objective of the pilot, but basically how much time it took a card to be read in a laboratory setting.

Given all the issues we identified, we do not believe using TWICs with readers would provide a critical layer of port security. We think that has yet to be demonstrated, and that is why we called for the agency to implement our prior recommendation on that point, to do a security assessment, to try to identify the value added of using TWICs with readers. Is it better than the regimes used in the past or not? We think that is a really important issue. So that is why, again, we called for that in our 2011 report.

But we do acknowledge some of the many challenges that DHS experienced in the pilot. They were dealing with 17 different sites; they participated on a voluntary basis, they couldn't compel them to participate or collect data in a certain way. And we recognize that, yet we still think some of those risks could have been mitigated by perhaps having more personnel involved at the sites or providing additional resources.

In closing, given the many issues we identified, as we highlight in our report, we think Congress should consider repealing the requirement that the final regulations for the card readers be consistent with the pilot findings. Essentially, we think those two issues should be de-linked given the issues we identified in the pilot. Instead, we believe Congress should require DHS to complete a security assessment, as we originally called for in our May 2011 report. Again, the security assessment will help demonstrate the value of the program.

And the assessment should also include a comparison of alternative credentialing approaches. There are different options they could have considered. For example, the Government can conduct a security assessment and have the credentials be provided at the local level. That was an option that was never considered in the early analysis of alternatives, and we think that has possible merit that should be studied further.

Thank you, Mr. Mica, Ranking Member Connolly, Representative Meadows. This concludes my prepared statement and I look forward to answering any questions.

[Prepared statement of Mr. Lord follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 9:00 a.m. EST
Thursday, May 9, 2013

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Card Reader Pilot Results Are Unreliable; Security Benefits Should Be Reassessed

Statement of Stephen M. Lord, Director
Homeland Security and Justice

Chairman Mica, Ranking Member Connolly, and Members of the Subcommittee:

I am pleased to be here today to discuss our work examining the Department of Homeland Security's (DHS) Transportation Worker Identification Credential (TWIC) program. Ports, waterways, and vessels handle billions of dollars in cargo annually, and an attack on our nation's maritime transportation system could have serious consequences. Maritime workers, including longshoremen, mechanics, truck drivers, and merchant mariners, access secure areas of the nation's estimated 16,400 maritime-related transportation facilities and vessels, such as cargo container and cruise ship terminals, each day while performing their jobs.[1]

The TWIC program is intended to provide a tamper-resistant biometric credential[2] to maritime workers who require unescorted access to secure areas of facilities and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA).[3] TWIC is to enhance the ability of MTSA-regulated facility and vessel owners and operators to control access to their facilities and verify workers' identities. Under current statute and regulation, maritime workers requiring unescorted access to secure areas of MTSA-regulated facilities or vessels are required to obtain a TWIC,[4] and facility and vessel operators are required by regulation to visually inspect each worker's TWIC before granting unescorted access.[5] Prior to being granted a TWIC, maritime workers are

[1]For the purposes of this statement, the term "maritime-related transportation facilities" refers to seaports, inland ports, offshore facilities, and facilities located on the grounds of ports.

[2]A biometric access control system consists of technology that determines an individual's identity by detecting and matching unique physical or behavioral characteristics, such as fingerprint or voice patterns, as a means of verifying personal identity.

[3]Pub. L. No. 107-295,116 Stat. 2064. According to Coast Guard regulations, a secure area is an area that has security measures in place for access control. 33 C.F.R. § 101.105. 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 offshore petroleum or gas production facilities, the secure area is generally the whole vessel or facility. A restricted area is a part of a secure area that needs more limited access and higher security. Under Coast Guard regulations, an owner/operator must designate certain specified types of areas as restricted. For example, storage areas for cargo are restricted areas under Coast Guard regulations. 33 C.F.R. § 105.260(b)(7).

[4]46 U.S.C. § 70105(a); 33 C.F.R. § 101.514.

[5]33 C.F.R. §§ 104.265(c), 105.255(c).

required to undergo a background check, known as a security threat assessment.

Within DHS, the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG) jointly administer the TWIC program. USCG is leading efforts to develop a new TWIC regulation (rule) regarding the use of TWIC cards with readers (known as the TWIC card reader rule). The TWIC card reader rule is expected to define if and under what circumstances facility and vessel owners and operators are to use electronic card readers to verify that a TWIC card is valid. To help inform this rulemaking and to fulfill the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) requirement,[6] TSA conducted a TWIC reader pilot from August 2008 through May 2011 to test a variety of biometric readers, as well as the credential authentication and validation process. The TWIC reader pilot, implemented with the voluntary participation of maritime port, facility, and vessel operators, was to test the technology, business processes, and operational impacts of deploying card readers at maritime facilities and vessels prior to issuing a final rule.[7] Among other things, the SAFE Port Act required that DHS submit a report on the findings of the pilot program to Congress.[8] DHS submitted its report to Congress on the findings of the TWIC reader pilot on February 27, 2012.[9] The Coast Guard Authorization Act of 2010 required that, among other things, GAO conduct an assessment of the report's findings and recommendations.[10]

We have been reporting on TWIC progress and challenges since September 2003.[11] Among other issues, we highlighted steps that TSA

[6]Pub. L. No 109-347, § 104(a), 120 Stat. 1884, 1888 (codified at 46 U.S.C. § 70105(k)).

[7]The SAFE Port Act required the Secretary of Homeland Security to conduct a pilot program to test the business processes, technology, and operational impacts required to deploy transportation security card readers at secure areas of the maritime transportation system. 46 U.S.C. § 70105(k)(1)(A).

[8]46 U.S.C. § 70105(k)(4).

[9]Department of Homeland Security, *Transportation Worker Identification Credential Reader Pilot Program: In accordance with Section 104 of the Security and Accountability For Every Port Act of 2006, P.L. 109-347 (SAFE Port Act) Final Report.* Feb. 17, 2012.

[10]Pub. L. No. 111-281, § 802, 124 Stat. 2905, 2989.

[11]GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*, GAO-03-1155T (Washington, D.C.: Sept. 9, 2003).

and USCG were taking to meet an expected surge in initial enrollment as well as various challenges experienced in the TWIC testing conducted by a contractor for TSA and USCG from August 2004 through June 2005. We also identified challenges related to ensuring that the TWIC technology works effectively in the harsh maritime environment.[12] In November 2009, we reported on the design and approach of a pilot initiated in August 2008 to test TWIC readers, and found that DHS did not have a sound evaluation methodology to ensure information collected through the TWIC reader pilot would be complete and accurate.[13] Moreover, in May 2011, we reported that 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.[14]

My statement today highlights the key findings of a report we released yesterday on the TWIC program that addressed the extent to which the results from the TWIC reader pilot were sufficiently complete, accurate, and reliable for informing Congress and the TWIC card reader rule.[15] For the report, among other things, we assessed the methods used to collect and analyze pilot data since the inception of the pilot in August 2008. We analyzed and compared the pilot data with the TWIC reader pilot report submitted to Congress to determine whether the findings in the report are based on sufficiently complete, accurate, and reliable data. Additionally, we interviewed officials at DHS, TSA, and USCG with responsibilities for overseeing the TWIC program, as well as pilot officials responsible for coordinating pilot efforts with TSA and the independent test agent

[12]GAO, *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO-06-982 (Washington, D.C.: Sept. 29, 2006). TWIC readers and related technologies operated outdoors in the harsh maritime environment can be affected by dirt, salt, wind, and rain.

[13]*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).

[14]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).

[15]GAO, *Transportation Worker Identity Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed*, GAO-13-198 (Washington, D.C.: May 8, 2013).

(responsible for planning, evaluating, and reporting on all test events), about TWIC reader pilot testing approaches, results, and challenges. Our investigators also conducted limited covert testing of TWIC program internal controls for acquiring and using TWIC cards at four maritime ports to update our understanding of the effectiveness of TWIC at enhancing maritime security since we reported on these issues in May 2011. Our May 2013 report includes additional details on our scope and methodology. We conducted this work in accordance with generally accepted government auditing standards, and conducted the related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

TWIC Reader Pilot Results Are Not Sufficiently Complete, Accurate, and Reliable for Informing Congress and the TWIC Card Reader Rule

Our review of the pilot test identified several challenges related to pilot planning, data collection, and reporting, which affected the completeness, accuracy, and reliability of the results.

Pilot Planning

DHS did not correct planning shortfalls that we identified in our November 2009 report.[16] We determined that these weaknesses presented a challenge in ensuring that the pilot would yield information needed to inform Congress and the card reader rule and recommended that DHS components implementing the pilot—TSA and USCG—develop an evaluation plan to guide the remainder of the pilot and identify how it would compensate for areas where the TWIC reader pilot would not provide the information needed. DHS agreed with the recommendations; however, while TSA developed a data analysis plan, TSA and USCG reported that they did not develop an evaluation plan with an evaluation methodology or performance standards, as we recommended. The data analysis plan was a positive step because it identified specific data

[16]GAO-10-43.

elements to be captured from the pilot for comparison across pilot sites. If accurate data had been collected, adherence to the data analysis plan could have helped yield valid results. However, TSA and the independent test agent[17] did not utilize the data analysis plan. According to officials from the independent test agent, they started to use the data analysis plan but stopped using the plan because they were experiencing difficulty in collecting the required data and TSA directed them to change the reporting approach. TSA officials stated that they directed the independent test agent to change its collection and reporting approach because of TSA's inability to require or control data collection to the extent required to execute the plan.

Data Collection

We identified eight areas where TWIC reader pilot data collection, supporting documentation, and recording weaknesses affected the completeness, accuracy, and reliability of the pilot data

1. **Installed TWIC readers and access control systems could not collect required data on TWIC reader use, and TSA and the independent test agent did not employ effective compensating data collection measures.** The TWIC reader pilot test and evaluation master plan recognizes that in some cases, readers or related access control systems at pilot sites may not collect the required test data, potentially requiring additional resources, such as on-site personnel, to monitor and log TWIC card reader use issues. Moreover, such instances were to be addressed as part of the test planning. However, the independent test agent reported challenges in sufficiently documenting reader and system errors. For example, the independent test agent reported that the logs from the TWIC readers and related access control systems were not detailed enough to determine the reason for errors, such as biometric match failure, an expired TWIC card, or that the TWIC was identified as being on the list of revoked credentials. The independent test agent further reported that the inability to determine the reason for errors limited its ability to understand why readers were failing, and thus it was unable to determine whether errors encountered were due to TWIC cards, readers, or users, or some combination thereof.

[17]To conduct the TWIC reader pilot, TSA contracted with the Navy's Space and Naval Warfare Systems Command (SPAWAR) to serve as the independent test agent to plan, analyze, evaluate, and report on all test events.

2. **Reported transaction data did not match underlying documentation.** A total of 34 pilot site reports were issued by the independent test agent. According to TSA, the pilot site reports were used as the basis for DHS's report to Congress. We separately requested copies of the 34 pilot site reports from both TSA and the independent test agent. In comparing the reports provided, we found that 31 of the 34 pilot site reports provided to us by TSA did not contain the same information as those provided by the independent test agent. Differences for 27 of the 31 pilot site reports pertained to how pilot site data were characterized, such as the baseline throughput time used to compare against throughput times observed during two phases of testing. However, at two pilot sites, Brownsville and Staten Island Ferry, transaction data reported by the independent test agent did not match the data included in TSA's reports. Moreover, data in the pilot site reports did not always match data collected by the independent test agent during the pilot.
3. **Pilot documentation did not contain complete TWIC reader and access control system characteristics.** Pilot documentation did not always identify which TWIC readers or which interface (e.g., contact or contactless interface) the reader used to communicate with the TWIC card during data collection.[18] For example, at one pilot site, two different readers were tested. However, the pilot site report did not identify which data were collected using which reader.
4. **TSA and the independent test agent did not record clear baseline data for comparing operational performance at access points with TWIC readers.** Baseline data, which were to be collected prior to piloting the use of TWIC with readers, were to be a measure of throughput time, that is, the time required to inspect a TWIC card and complete access-related processes prior to granting entry. However, it is unclear from the documentation whether acquired data were sufficient to reliably identify throughput times at truck, other vehicle, and pedestrian access points, which may vary.
5. **TSA and the independent test agent did not collect complete data on malfunctioning TWIC cards.** TSA officials observed malfunctioning TWIC cards during the pilot, largely because of broken antennas. If a TWIC with a broken antenna was presented for a

[18]As used in this statement, "contactless mode" refers to the use of TWIC readers for reading TWIC cards without requiring that a TWIC card be inserted into or make physical contact with a TWIC reader.

contactless read, the reader would not identify that a TWIC had been presented, as the broken antenna would not communicate TWIC information to a contactless reader. In such instances, the reader would not log that an access attempt had been made and failed.

6. **Pilot participants did not document instances of denied access.** Incomplete data resulted from challenges documenting how to manage individuals with a denied TWIC across pilot sites. Specifically, TSA and the independent test agent did not require pilot participants to document when individuals were granted access based on a visual inspection of the TWIC, or deny the individual access as may be required under future regulation. This is contrary to the TWIC reader pilot test and evaluation master plan, which calls for documenting the number of entrants "rejected" with the TWIC card reader system operational as part of assessing the economic impact. Without such documentation, the pilot sites were not completely measuring the operational impact of using TWIC with readers.
7. **TSA and the independent test agent did not collect consistent data on the operational impact of using TWIC cards with readers.** TWIC reader pilot testing scenarios included having each individual present his or her TWIC for verification; however, it is unclear whether this actually occurred in practice. For example, at one pilot site, officials noted that during testing, approximately 1 in 10 individuals was required to have his or her TWIC checked while entering the facility because of concerns about causing a traffic backup. Despite noted deviations in test protocols, the reports for these pilot sites do not note that these deviations occurred. Noting deviations in each pilot site report would have provided important perspective by identifying the limitations of the data collected at the pilot site and providing context when comparing the pilot site data with data from other pilot sites.
8. **Pilot site records did not contain complete information about installed TWIC readers' and access control systems' design.** TSA and the independent test agent tested the TWIC readers at each pilot site to ensure they worked before individuals began presenting their TWIC cards to the readers during the pilot. However, the data gathered during the testing were incomplete. For example, 10 of 15 sites tested readers for which no record of system design characteristics were recorded. In addition, pilot reader information was identified for 4 pilot sites but did not identify the specific readers or associated software tested.

According to TSA, a variety of challenges prevented TSA and the independent test agent from collecting pilot data in a complete and

consistent fashion. Among the challenges noted by TSA, (1) pilot participation was voluntary, which allowed pilot sites to stop participation at any time or not adhere to established testing and data collection protocols; (2) the independent test agent did not correctly and completely collect and record pilot data; (3) systems in place during the pilot did not record all required data, including information on failed TWIC card reads and the reasons for the failure; and (4) prior to pilot testing, officials did not expect to confront problems with nonfunctioning TWIC cards. Additionally, TSA noted that it lacked the authority to compel pilot sites to collect data in a way that would have been in compliance with federal standards. In addition to these challenges, the independent test agent identified the lack of a database to track and analyze all pilot data in a consistent manner as an additional challenge to data collection and reporting. The independent test agent, however, noted that all data collection plans and resulting data representation were ultimately approved by TSA and USCG.

Reporting

As required by the SAFE Port Act and the Coast Guard Authorization Act of 2010, DHS's report to Congress on the TWIC reader pilot presented several findings with respect to technical and operational aspects of implementing TWIC technologies in the maritime environment. However, DHS's reported findings were not always supported by the pilot data, or were based on incomplete or unreliable data, thus limiting the report's usefulness in informing Congress about the results of the TWIC reader pilot. For example, reported entry times into facilities were not based on data collected at pilot sites as intended. Further, the report concluded that TWIC cards and readers provide a critical layer of port security, but data were not collected to support this conclusion.

Because of the number of concerns that we identified with the TWIC pilot, in our March 13, 2013, draft report to DHS, we recommended that DHS not use the pilot data to inform the upcoming TWIC card reader rule. However, after receiving the draft that we sent to DHS for comment, on March 22, 2013, USCG published the TWIC card reader notice of proposed rulemaking (NPRM), which included results from the TWIC card reader pilot.[19] We subsequently removed the recommendation from our final report, given that USCG had moved forward with issuing the NPRM

[19]78 Fed. Reg. 17,782 (Mar. 22, 2013).

and had incorporated the pilot results into the proposed rulemaking. In its official comments on our report, DHS asserted that some of the perceived data anomalies we cited were not significant to the conclusions TSA reached during the pilot and that the pilot report was only one of multiple sources of information available to USCG in drafting the TWIC reader NPRM. We recognize that USCG had multiple sources of information available to it when drafting the proposed rule; however, the pilot was used as an important basis for informing the development of the NPRM, and the issues and concerns that we identified remain valid.

Given that the results of the pilot are unreliable for informing the TWIC card reader rule on the technology and operational impacts of using TWIC cards with readers, we recommended that Congress should consider repealing the requirement that the Secretary of Homeland Security promulgate final regulations that require the deployment of card readers that are consistent with the findings of the pilot program; and that Congress should consider requiring that the Secretary of Homeland Security complete an assessment that evaluates the effectiveness of using TWIC with readers for enhancing port security. This would be consistent with the recommendation that we made in our May 2011report. These results could then be used to promulgate a final regulation as appropriate. Given DHS's challenges in implementing TWIC over the past decade, at a minimum, the assessment should include a comprehensive comparison of alternative credentialing approaches, which might include a more decentralized approach, for achieving TWIC program goals.

Chairman Mica, Ranking Member Connolly, and members of the subcommittee, this concludes my prepared statement. I would be happy to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Steve Lord at (202) 512-4379 or lords@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Dave Bruno, Assistant Director; Joseph P. Cruz; and James Lawson. Key contributors for the previous work that this testimony is based on are listed within each individual product.

Mr. MICA. Thank you. We will start questions. I will start with a round.

First, Mr. Sadler, have you ever had the opportunity see the movie Groundhog Day?

Mr. SADLER. Yes, I did, sir.

Mr. MICA. In that movie, doesn't the character keep repeating the same day over and over again and sort of the same thing over and over?

Mr. SADLER. I believe he does, sir.

Mr. MICA. I feel a little bit like that character, Mr. Connolly and Mr. Meadows. From 2002, 2005, 2006, 2009, to 2011. Last I checked, this is 2013. And we still do not have a viable TWIC program. I just heard Mr. Lord go through his analysis of these reader tests experiences. We have his report here. It is very frustrating.

I guess you did 17 sites?

Mr. SADLER. That is right, sir.

Mr. MICA. And we don't really know how many people went through. DHS's report to Congress shows a total population of 33,111. However, final pilot site test systems showed a population of 79,000. There is a discrepancy even in the number of participants. Mr. Lord said that you couldn't get some to participate.

The report says pilot participants did not document instances of denied access. TSA and the independent test agent did not collect complete data on malfunctioning TWIC cards. I mean, the report just goes on and on about, again, what is supposed to be pilot testing to develop a card that we can use and have some basic knowledge about what is effective and how all this can be utilized. How do you respond to GAO?

Mr. SADLER. I would say that GAO, in their opening statement, pointed out some of the challenges that we faced when we started this pilot program, and that is a key point. This is a pilot program that we implemented in the commercial maritime environment. No one has done that before. And I know you have heard that before, but that is the crux of the issue.

Mr. MICA. In a maritime environment?

Mr. SADLER. No one has done this type of pilot, that I know of, in this type of environment. So we got voluntary participation from the facilities. We were very happy that these facilities stepped forward and participated, but we did this pilot under the condition of an operational maritime port facility. So we couldn't put readers at every access point; whether it was for a vehicle, whether it was for a pedestrian.

So those were some of the challenges that we faced. It was a voluntary pilot; it was in an maritime operational environment; not all access points had readers. If we could have locked the place down and put a reader at every access point, possibly——

Mr. MICA. So you are saying it is not practical to have a reader with a TWIC program?

Mr. SADLER. No, I am not saying that, sir. What I am saying is under the conditions we had to test, we faced challenges; and we stated those in our report to Congress as well.

Mr. MICA. Now, let me ask you a question. You have issued, what, 1.8 million of these?

Mr. SADLER. About 2.5 million, sir.

Mr. MICA. But is there 1.8 million coming due or something?

Mr. SADLER. Well, there are about 1.5 million cards that are set to expire over the next 18 months.

Mr. MICA. I am sorry, I messed up the figures. So in the next 18 months you have 1.5 million. Do you have a card now that has a biometric component that would recognize both fingerprints and iris?

Mr. SADLER. Sir, we use the fingerprint template only because that is the only federal standard that is in existence today, and it was the most robust biometric.

Mr. MICA. And you are working with the folks that set the standards, and they have told us at several previous hearings that the standard was just around the corner for iris. What are they telling you now?

Mr. SADLER. As I understand it, they are in their second iteration of the iris standard out for comment, and I don't know what their schedule is for final publication of that standard. I would have to defer to them.

Mr. MICA. Well, TSA, you also oversee entry programs, for example, the CLEAR program. I am told that the CLEAR program has an iris and also I think all five fingers are incorporated, and this is in use in the airports, is that correct?

Mr. SADLER. It may be, sir. I am not aware that we are overseeing that program at this point.

Mr. MICA. TSA just lets anybody put a program in place?

Mr. SADLER. It is not about TSA allowing the program; it is about a relationship between the contractor or that company and the airport.

Mr. MICA. So do you accept these cards? These aren't accepted?

Mr. SADLER. I don't know if they are accepted or not. I would have to get back to you on that answer. As far as boarding an aircraft?

Mr. MICA. Yes.

Mr. SADLER. I would have to get back to you on that answer. What I would say about that is we use a fingerprint template; we do not use an image for privacy purposes. We have to encrypt our biometric. I don't know if they encrypt their biometric.

Also, if an individual comes up to a kiosk in an airport, that is much different than an individual who is in a tractor trailer or a truck going through a gate trying to use an iris scan. If I could set every person going into a port coming up to a kiosk and take the time I needed to take that iris scan and embed that in the card, then we would do that, but that is not the way the port operates. Now, if the port wanted to use an iris, they can use an iris and they can use a TWIC card as a pointer to get back to that biometric.

Mr. MICA. So basically you are going to be issuing more than a million cards, reissuing the cards that have expired, without an iris component and I guess somewhat limited fingerprint component. I think one of the previous studies that Mr. Lord did was some of the flaws with the card that they could be tampered with.

And, actually, I think on several occasions you thwarted the system, is that correct, Mr. Lord?

Mr. LORD. Yes. We did some covert testing as part of our 2011 report and this report as well. We dispatched covert testers to basically conduct two types of tests. We presented fraudulent identification documents. We were able to obtain an authentic TWIC and we also manufactured a TWIC, we basically made a fake TWIC; and we were able to access facilities using both types of credentials.

Mr. MICA. Did you use any of the fake TWICs to thwart the pilot?

Mr. LORD. At one site they were using a reader, but it is my understanding they had some problems with false positives, so our undercover investigators were waved in. Even after the entry guard tried to swipe it and it wasn't working, she still provided them access to the facility.

Mr. MICA. Very good.

Let me go to Mr. Connolly. I want to be fair with the members that are here.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Mr. Sadler, do you think the pilot program was successful?

Mr. SADLER. I think the pilot program showed what we asked it to do.

Mr. CONNOLLY. Whoa. Time out. The pilot is the predicate for moving forward. It is kind of a critical question. Was it successful? Because GAO says that not only was it not successful; they are recommending the Congress decouple future regulations and standards from the pilot. Do you disagree with that?

Mr. SADLER. I think it was successful in what we intended to do, which was show that if that reader was installed properly, if the operator was trained properly, if the individuals were trained properly in the use of the card and that reader was put in place based on the business requirements of that port, then the reader did its job with the TWIC card.

Mr. CONNOLLY. Mr. Sadler, we just heard testimony, and there is more in the report, you didn't test for durability. Durability of the card actually could be very important in terms of long-term security. The wet conditions are a problem in terms of accurate reading. You just heard Mr. Lord say they actually manufactured a fake card and, sadly, that fake card passed muster that all too often the differentiation between the fake card and the TWIC card failed in the readers.

Now, you think that is just a matter of fine-tuning? And, by the way, another aspect of the GAO report is the cost figures were so flawed as to not be reliable, and they caution Congress don't read too much into that because the methodology, frankly, is not really an accurate picture of what it cost.

What aspect, pray tell, of this pilot could be considered successful such that we could have confidence in moving forward?

Mr. SADLER. If someone uses a card that is fraudulent, and I think it was shown in this case that the reader would not read that card, so that individual who came up with that fraudulent card did not get a positive read off the reader, from what I understand. And if the individual was allowed into that facility, the person should not have been let into that facility without a business need.

Mr. CONNOLLY. Time out.

Mr. Lord, tell us how it worked.

Mr. LORD. The card reader rejected the card; the person was allowed to enter the facility based on what they referred to as social engineering, some discussion with the guard, the security guard.

Mr. CONNOLLY. So they were able to bypass the card system entirely.

Mr. LORD. Yes. They were able to basically talk their way in.

Mr. CONNOLLY. So you are saying that is not really a failure of TWIC; that is a breach of security protocols in general.

Mr. SADLER. What I am saying is in that case it appears that the card and reader did their job; they didn't have a positive identification for that individual. And then the individual talked to the security guard, apparently.

Mr. CONNOLLY. So a separate issue.

Mr. SADLER. That is a different issue completely than the card itself or the reader. If that person didn't have a business need to get into that port, that person should not have been let in.

Mr. CONNOLLY. But how do you respond, Mr. Sadler, to Mr. Lord's and GAO's recommendation to the Congress that the lack of efficacy of the pilot is such we should pass legislation to decouple it from moving forward? That is a pretty rare recommendation coming out of GAO.

Mr. SADLER. I think that the TWIC card and reader, when installed properly, provides security value at the port. It is not a silver bullet; it is part of our layered security, and I think it provides value when it is used properly and installed properly.

Mr. CONNOLLY. Can you point to a place where it has been installed properly and it works and, therefore, we should have confidence in it?

Mr. SADLER. In some of the pilot locations it has been installed properly.

Mr. CONNOLLY. For example?

Mr. SADLER. In a Long Beach Port there was one single gate through the back, and I believe it was Long Beach, it might have been Los Angeles; I would have to go back and check. There was one single gate where, if you came into that back gate you had to use the card, you had to use the reader. It worked and we didn't see any appreciable backup in the flow of traffic. And I will go back and confirm that.

Mr. CONNOLLY. All right. Yes, I wish you would. You know, I spent 20 years, before I came here to Congress, in the private sector, and in two organizations that do a lot of security work, including port security, I might add. I spent 14 years in local government. The practice in both local government and in the private sector, when we were looking at a challenge, was to first look at best practices. We benchmarked ourselves against the competition.

I will use local government rather than the private sector. I represented Fairfax County, a pretty advanced county government, big local government. So we would compare ourselves to DuPage in Illinois and Los Angeles County, and depending on the subject matter, how are they doing it? What are they doing? How does it work? What can we learn from their lessons?

Did we do that before we decided to embrace TWIC as the answer to port security going forward? Because the chairman pointed out that there are other examples, seemingly, of cards that do seem

to work and processes that do seem to work. What have we learned from those that we are trying to apply to what seems to be a flawed process here?

Mr. SADLER. Well, we were required by Congress to issue the biometric credential, and we are doing that.

Mr. CONNOLLY. Excuse me, Mr. Sadler. If I may interrupt just one second. We take that point; the chairman addressed that. The cards he gave you as an example that seemed to work also include biometric data. This is not unique to TWIC.

Mr. SADLER. Those cards are not working in the same environment we are working in.

Mr. CONNOLLY. Your argument is that the port environment, the maritime environment is unique and has special requirements?

Mr. SADLER. Yes. The port environment is unique. And as far as durability of the card goes, some of the analysis that we saw, the use of the card was equivalent to use by DOD, use by park rangers. So this is a very tough environment. It is not the same as coming up to a kiosk in an airport, which is inside, which is a controlled environment. So I would say, yes, it is unique.

Mr. CONNOLLY. All right, my time is almost up, but if I could just add one last question on that.

Mr. Lord, could you respond to that? What about that? This is a unique environment and some of your criticisms might be more applicable if we were talking about access to an office environment in a commercial office building, but you are not being cognizant of the unique attributes of the maritime environment.

Mr. LORD. I think we are. We fully recognize the harsh maritime conditions the card is used within. The analogy we drew in our report was to the DOD CAC card. That card, in contrast to the TWIC card, is durability tested after it is personalized, which tends to introduce some vulnerabilities in the card when you add the little unique features; and that was, to me, an important distinction between the TSA approach and the DOD approach.

As you know, if you have ever been abroad, Iraq, Afghanistan, that is the common access card they use in those types of environments, which we think are pretty harsh environments as well, and those cards are considered a success because they are considered more durable.

Mr. CONNOLLY. Thank you.

Mr. MICA. Thank you, Mr. Connolly.

Mr. Meadows?

Mr. MEADOWS. Thank you, Mr. Chairman. I am going to pick up on some of the line of questioning that the ranking member brought up with regards to the pilot program and the existence, why we have a pilot program is hopefully to make determinations on whether we should proceed.

You are saying that it is a congressional thing and, Mr. Sadler, I am sorry to point all these questions to you. This is not a personal thing and obviously I am looking to you for guidance on what we need to go forward with, because we have had, according to my research, six or seven studies already by GAO in terms of recommendations on this particular thing. Is that correct?

Mr. SADLER. I don't know the exact number, sir, but there have been quite a few.

Mr. MEADOWS. A number of them?

Mr. SADLER. Yes, sir.

Mr. MEADOWS. And each time, from what I understand, you have agreed, or your agency has agreed to the recommendations that the GAO has made, is that correct?

Mr. SADLER. Yes, sir, I believe that is correct.

Mr. MEADOWS. And so I guess my question is why have those not been followed up on or really, truly implemented? Is it because of the weather conditions that you are talking about?

Mr. SADLER. I think that is part of it. It is not necessarily the weather conditions. I think the weather conditions are a part of it.

Mr. MEADOWS. Well, I know that maritime constitutes salt water, generally; not always, but many times salt water. And I know that salt just eats the hell out of anything. So when we have this technology, is this something that could be viable long-term, or are we going to be spending another $3.2 billion five years from now to replace readers?

Mr. SADLER. No, I think what we found in the pilot was that if the reader was installed properly and covered properly, that cut down on a lot of the issues.

Mr. MEADOWS. Okay. And you have installed those readers at 17 ports, is that correct?

Mr. SADLER. Seventeen ports, 100 access points.

Mr. MEADOWS. For the cost of $500 million?

Mr. SADLER. No, the total cost of the pilot that we conducted to the ports was $15 million, and to the Government approximately $8 million. So the total amount of money expended for this pilot was $23 million.

Mr. MEADOWS. All right, so we are talking about $23 million there for the pilot, is that correct?

Mr. SADLER. That is correct.

Mr. MEADOWS. Okay. And you have issued about 2.5 million cards, is that correct?

Mr. SADLER. That is correct also.

Mr. MEADOWS. So how many of those cards have been lost or stolen?

Mr. SADLER. I would have to get back to you, sir, with that number; I don't have that off the top of my head.

Mr. MEADOWS. Do you think you know exactly the number of cards that have been lost or stolen at your agency at this point?

Mr. SADLER. I think we would have a pretty good idea. I don't know if we would know the exact number.

Mr. MEADOWS. So everybody that loses a card or has one stolen, with the transient nature of employment, would call you and let you know?

Mr. SADLER. They would have to call and get a replacement card, yes.

Mr. MEADOWS. Only if they were trying to get back in.

Mr. SADLER. Yes, sir.

Mr. MEADOWS. But if they lost it and they were unemployed, would they call you?

Mr. SADLER. If they needed the card, they would call us.

Mr. MEADOWS. But only if they needed it. My point is when we have this and we are looking at this biometric there, if these cards

are transient and you have no kind of iris screening that would connect them, for a million bucks maybe I give my card to somebody else. So does it actually provide a more secure environment, with the transient nature of this and with nothing that is actually tied to the person that you issue it to?

Mr. SADLER. We can't eliminate that risk, sir; we can try to mitigate it. And that is why I would say we need the readers.

Mr. MEADOWS. All right.

Mr. SADLER. Just as the GAO mentioned, when they tried the card where a reader was positioned, it didn't acknowledge that card. It was social engineering that got it through, not a fraudulent TWIC.

Mr. MEADOWS. So if you were to come back before Congress and say, well, we are doing this because Congress told us we had to do it, if we were to put forth a piece of legislation today that says Congress changed its mind because this is not a wise investment of hardworking American taxpayers' dollars, would you endorse that?

Mr. SADLER. Well, we would try our best to comply with whatever statute Congress passed.

Mr. MEADOWS. But if you were in my shoes, would you put forth a piece of legislation, knowing what you know over the last 11 years, that we have spent over $500 million and we are still yet to have secure ports, would you make that recommendation? If you were going back home and people were going to say, well, it is my money, are you being responsible, is that the kind of decision you would make?

Mr. SADLER. What I would tell my constituents, I would say TWIC is a valuable security tool.

Mr. MEADOWS. It is a valuable security tool.

Mr. SADLER. Yes. And I believe that.

Mr. MEADOWS. And you make that based on 17 installations out of 360?

Mr. SADLER. Seventeen installations, 100 access points, 156 readers, 400,000 pieces of data.

Mr. MEADOWS. Okay. How sure are you that we are only going to spend $3.2 billion to implement this? On the level of 10 being the highest that you are absolutely confident, how sure are you, Mr. Sadler?

Mr. SADLER. Well, the life cycle cost estimate that was conducted, I believe, in 2005 had a limit of $694 million up to $3.2 billion.

Mr. MEADOWS. During the pilot have you had cost overruns?

Mr. SADLER. No, sir.

Mr. MEADOWS. Because there was no budget. So it is hard to go over or under a budget.

Mr. SADLER. No, there was a budget.

Mr. MEADOWS. Okay.

Mr. SADLER. There was $23 million in grants that were let to the facilities, there was $8 million let to TSA, and it is a fee-funded program. So if you have a fee-funded program, you cannot go over budget.

Mr. MEADOWS. So as long as they are paying for it, you don't go over budget. Because I am reading in the GAO there were some concerns with regard to some of the issues in how we implement

this, and we have, obviously, a Government-centric focus here. Do you think we ought to reevaluate that and go with something that is not Government-centric? Or is the Government the best place to provide security here?

Mr. SADLER. I don't know exactly what you mean, sir.

Mr. MEADOWS. Well, it is all about calling into a Government call center to provide these particular cards, and as we look at that it is all about the Government providing it. Could a private agency do a better job than we are doing?

Mr. SADLER. I don't think so, sir, because a private agency is not going to have access to the information we have access to to make those decisions.

Mr. MEADOWS. So there is no private security that could provide that. So you are saying basically because of the information with regards to the matrix with fingerprinting, etcetera?

Mr. SADLER. In my opinion, I think that is correct.

Mr. MEADOWS. So your recommendation is to continue to go forward with this plan?

Mr. SADLER. My recommendation is to implement readers in the maritime environment.

Mr. MEADOWS. I can see my time is up, so let me finish up with this line of questioning. We have been here for 11 years. We have yet to have really new port security. In fact, you even mentioned that we have issues. The GAO report mentions that we have issues. So we don't have a more secure environment in 11 years.

At what point can I tell my folks back home that we are going to have more secure ports, is it five years, six years? You have $3.2 billion to spend, so at what point do we have a more secure environment?

Mr. SADLER. You can tell them that today, sir.

Mr. MEADOWS. So it will be more secure today?

Mr. SADLER. It is already more secure. You have a common credential; you have a consistent security threat assessment that nobody has done before.

Mr. MEADOWS. So you have reached your objective?

Mr. SADLER. No, sir, we have not.

Mr. MEADOWS. So my question, you know what I am meaning, at what point do we reach our objective, Mr. Sadler?

Mr. SADLER. We reach our objective when we get readers installed.

Mr. MEADOWS. All right, which will be when?

Mr. SADLER. I defer to the Coast Guard and their time schedule. They have an MPR out now; they are taking comments. They are going to adjudicate the comments and get a final rule.

Mr. MEADOWS. So we needed to have the Coast Guard here. And you are saying that they can implement it with the pilot results that you have right now?

Mr. SADLER. I am going to defer to the Coast Guard on which results from that pilot program they use and which they don't use.

Mr. MEADOWS. So if it fails, whose fault will it be, yours, TSAs because of the pilot, or the Coast Guard for implementation?

Mr. SADLER. That is a hard question to answer, sir. I am the responsible executive at TSA for this program, so I don't think failure is an option. I know failure isn't an option, but that is a difficult

question to answer because I am presupposing that I know why it failed, if it does, and I don't believe that it will.

Mr. MEADOWS. Well, the pilot should have told us that. But I am way over time.

I appreciate our indulgence, Mr. Chairman, and I yield back.

Mr. MICA. Well, let me just follow up on that.

Now, wait a second. You are shifting the responsibility to the Coast Guard, but you provided the Coast Guard the data on which they are going to evaluate their response to you, is that correct?

Mr. SADLER. Sir, I am not shifting responsibility to the Coast Guard. What I said was we provided data to the Coast Guard.

Mr. MICA. But Mr. Lord said that the data you provide, I mean, his whole report shows the data is flawed and the test results can't, you didn't even have clear baseline data from which you started.

Mr. Connolly and I, Mr. Cummings and the others that were here, our investigators did not go after this; we rely on GAO to evaluate what you are doing with the pilot program, and they came back with one of the most critical reports I have seen. So, again, you are telling us that you are giving the data and the Coast Guard is going to evaluate it based on the data, which is flawed, according to the GAO.

Mr. SADLER. Well, we believe there is meaningful data in that pilot report, and we provided that to the Coast Guard.

Mr. MICA. You cited one place where you thought this worked at some back gate, and you weren't sure if——

Mr. SADLER. Well, you asked me for an example, sir, and I gave you that example.

Mr. MICA. But that is at one back gate.

Mr. SADLER. And the reason I gave you that example was because that was a controlled gate; that wasn't an area where you might have eight gates with only two readers.

Mr. MICA. How much have we spent on the pilot project?

Mr. SADLER. Twenty-three million dollars.

Mr. MICA. Twenty-three million dollars.

Pretty good, Mr. Connolly. We got that one back gate secure. All this data that was collected without reliability.

Mr. Lord, I thought you said that others could do this, and in harsh conditions.

Mr. LORD. Chair, before I respond to that, I think I would like to address one point Mr. Sadler raised. I think there is broad agreement among most stakeholders that there is some value in the program, and that is the background check that is conducted.

Mr. MICA. Yes. And, you know, he didn't do a very good job on that. If I were him, I would have said, well, we stopped 50,000 people from actually getting the cards.

Mr. LORD. But I agree with Mr. Sadler. He did mention that was one of the values of the program. But beyond that, I think that is where, to us, it gets a little fuzzy, because that was one option that wasn't really considered at the start of the program. What if the Government did the background checks and we left the issuance of the credential to the local ports? That is essentially what they do with the CITA model with the airports.

Mr. MICA. Actually, this became an issue. I forgot Mr. Connolly and I were discussing it. I was telling him, in South Florida, about

25 percent of our port workers had criminal backgrounds, and this actually came into Congress, I think, Mr. Connolly, as to what we could consider in background checks. What do you consider now? I thought we set the standard because I know it became a big brouhaha.

Mr. LORD. They do criminal record checks.

Mr. MICA. How far back? You couldn't do State checks versus Federal or something. What is the status of what?

Mr. LORD. It depends on the disqualifying crime. Some crime, such as murder, is an unlimited look back; other crimes are seven years or five years from release of incarceration.

Mr. MICA. I think that is what we got into, yes.

Mr. LORD. Well, we do use State records. We receive State records from 40 States now that we utilize in the background check.

Mr. MICA. Well, again, we spent $23 million just on the pilot program. We are 11 years away from when we passed the initial legislation. We don't have a reader. We are going to issue, again, another million-plus cards, and they don't have the capability that Congress originally intended because, again, you say another agency has not set the standard for iris.

Any hope of when, again, we could actually see this happen if we go through the Coast Guard process, any processes that you have? And then when would you pick a reader, guesstimate? And then when would they be deployed; will it be in the next decade?

Mr. SADLER. Well, sir, I would have to defer to the Coast Guard on the time line as they are promulgating the rule. I can't answer that question.

Mr. MICA. Who actually issues the TWIC card, the Coast Guard?

Mr. SADLER. No, we issue. That is our responsibility, to issue the TWIC.

Mr. MICA. I thought the Coast Guard was sort of the enforcement agency.

Mr. SADLER. They are.

Mr. MICA. They do a great job. Thank God for the Coast Guard, because they are there 24/7, low pay, and guarding the ports at entry points far beyond these gates, also making certain that our maritime facilities are secure.

Okay, let's work this out. Remember my Groundhog Day? I want to know how many more times we are going to do this. So you have the Coast Guard, now this rulemaking. Is that an open-ended thing or is there a time frame?

Mr. SADLER. Ninety-day comment period from March 22nd.

Mr. MICA. Okay. And then you expect them to digest this? Are they going to get back with you? What is the process? Explain it.

Mr. SADLER. The process is that they have public meetings.

Mr. MICA. After the rulemaking or during the rulemaking?

Mr. SADLER. During this 90-day period.

Mr. MICA. We got to that.

Mr. SADLER. Then they receive written comments.

Mr. MICA. I got to 90 days.

Mr. SADLER. Ninety days.

Mr. MICA. Then what is going to happen?

Mr. SADLER. Then they take the written comments, they take the verbal comments from their public meetings, they adjudicate those comments, and then they start to develop the final rule.

Mr. MICA. And any guess as to?

Mr. SADLER. No, sir, I don't.

Mr. MICA. No guess?

Mr. SADLER. No, sir.

Mr. MICA. Mr. Lord?

Mr. LORD. Yes. I think it is worth noting the Coast Guard recently extended the comment period by 30 days. It may be beneficial, given all the issues we discussed at today's hearing, to perhaps extend it another 30 days to get additional stakeholder comments. I imagine there are going to be a lot of comments generated in the next few weeks.

Mr. MICA. Mr. Sadler, how long have you been with TSA?

Mr. SADLER. Since September 22nd, 2003.

Mr. MICA. From the beginning. So you have been there to see that this is something we have tried to put into place for more than a decade, and we seem to, at every turn, not make the progress that Congress originally intended. We don't, again, have a card, I think, that is adequate and we don't have readers or a program really to get a reader in place, so it is very frustrating. We have spent half a billion dollars on this and we have a card now that is flawed; and not by my definition, but by GAO's evaluation.

Mr. Lord, have you got any idea how this will all end?

Mr. LORD. I really don't, sir. That is more a matter for Congress and the executive agencies. Our role is simply to respond to the mandate and the Coast Guard Authorization Act to study the results of the pilot and provide the report to Congress, so that is what we did. On the other hand, we have reported extensively on other TWIC-related issues in the past. It will be interesting to see how it progresses after today.

Mr. MICA. Well, I believe there have been enough models out there and enough opportunities to adopt a better system. It may not be flawless, but, for the money we have spent and the results we have gotten, this is a pitiful commentary to be here May 2013 and still in this situation.

Mr. Connolly?

Mr. CONNOLLY. Thank you, Mr. Chairman.

I guess in addition to just the facts here, I am bothered by two Federal agencies coming to two different conclusions based on the data available. Mr. Lord and GAO have taken the position, if I understand it correctly, that the efficacy of the pilot is flawed such that we should not rely on it. It should not be a guide as we move forward, or something that can be adhered to as a guide because it is so flawed in its methodology in almost all respects, except there are some ancillary things that produced positive externalities, but not by design, you know, background checks or whatever.

Mr. Sadler, if I understood your testimony correctly, you believe that is not correct; that there is reliable data, at least sufficiently reliable that you and the Coast Guard can go forward in expanding the pilot to other facilities. Is that accurate?

Mr. SADLER. What I said, sir, was I think there is enough reliable data to support the conclusions of the pilot itself, which are that the reader, when installed properly, operated properly, and when the individuals are trained properly, whether it is the operator or the individual with the TWIC card, that the reader works properly.

Mr. CONNOLLY. And you say that the GAO report and evident lack of confidence in same notwithstanding.

Mr. SADLER. I am sorry, sir, could you repeat that?

Mr. CONNOLLY. You are saying that you are fully aware of GAO's findings and reports that come to a very different conclusion.

Mr. SADLER. Well, that was our conclusion when we wrote the pilot report that we sent to Congress, so, yes, that is what I am saying. So we agree in many areas with GAO, and we have to agree because our pilot report itself pointed out many of the same challenges that GAO pointed out as well. So we admitted to those and we know it is a challenge.

Mr. CONNOLLY. But here is the fundamental difference, Mr. Sadler. GAO has come to the conclusion that those flaws, deficiencies, problems, and lack of accurate data because of methodology flaws are of sufficient gravity that Congress should not rely on the pilot. You, in your position on behalf of TSA, are saying quite the opposite. You are saying we are going to rely on it; we don't agree that it is so flawed that it can't be relied upon. And that is what I mean. Their findings notwithstanding, you intend to go forward based on the pilot, even though GAO is saying to Congress we actually think you ought to decouple it from the pilot, it is that flawed.

Mr. SADLER. Well, sir, we have to go forward. We have been directed to issue the credential; we have been directed to install readers. And unless Congress gives us other direction, then we are going to go forward.

But we still stand by the fact that there was enough information gleaned from the pilot to support our conclusions in the pilot report. Then we take that information, we give it to the Coast Guard, and that is why I defer to the Coast Guard, because the Coast Guard takes that information and they use it based on how they think they need it, how they weight it, if they shouldn't use it. So I am not shifting responsibility to the Coast Guard, it is just the fact that they are writing the rule.

Mr. CONNOLLY. Surely, Mr. Sadler, you can sympathize, though, with a taxpayer concern that if we have such a flawed entity in the pilot, why not acknowledge that and find another paradigm with which we are more comfortable, and there are other models that seem to work in harsh environments, albeit maybe not a maritime one, as opposed to slavishly sticking to the pilot because statute cites it?

I mean, you are here to give advice today, as well as to be accountable to Congress, and if it is your studied judgment that we did our college best, but the pilot failed, or it is sufficiently flawed that, in good conscience, if you asked my opinion, I would find something else as a model to base going forward on rather than the pilot.

And I don't want to mischaracterize, but what I am hearing you saying is you don't, that is not your opinion; your opinion is the pilot, flaws and all, is going to give us sufficient data and is sufficiently efficacious that I have confidence that we can move forward based on what we learned from that pilot.

Mr. SADLER. And I want to be careful how I say this because I do have to defer to the Coast Guard, but the pilot data is one of many sources that the Coast Guard used in promulgating their rule. So what I said, and what I will say again, is that we believe we got sufficient data in sufficient quantity, in sufficient quality, to support the conclusions of that pilot itself, which was that if the readers are installed properly, people are trained properly, and they were purchased and installed based on the requirements of that particular port, then they work properly and they can be used to help make access decisions. Those were the conclusions of the pilot.

Mr. CONNOLLY. Okay. The record will show that is in distinct contrast to the GAO point of view. Okay.

Final set of questions, Mr. Chairman, if I may.

Mr. Lord, you cited in our previous round of questioning harsh conditions in Afghanistan and Iraq, war conditions, and lots of weather challenges too, I might add. I have been to both. But they use an access card that includes biometric information, is that correct?

Mr. LORD. Yes. It is called the common access card, the CAC card.

Mr. CONNOLLY. CAC card. And how many CAC cards have been issued?

Mr. LORD. That is a good question. I am not the subject matter expert on that. I know just from personal experience. I was deployed to Iraq for GAO for three months and I had one and it seemed to work and I never had an issue with it.

Mr. CONNOLLY. Hundreds of thousands of contractors?

Mr. LORD. Absolutely. And the servicemen themselves.

Mr. CONNOLLY. And the servicemen. Well, when you look at the total number that have come through Afghanistan and Iraq, it is well over a million, probably, right?

Mr. LORD. Yes.

Mr. CONNOLLY. So we have had a lot of these cards issued. I don't know if it approaches the TWIC, but it would be fairly comparable, is that correct?

Mr. LORD. I believe so. I don't have the exact numbers. But again I cited it as a success. That is an example where the Government was able to issue——

Mr. CONNOLLY. Yes. I am back to my benchmarking. We actually have an example, and the security challenge is paramount. That is why we issued these CAC cards, to make sure bad guys don't get into sensitive facilities or, for that matter, even canteens, where lots of our servicemen and women are congregating, assuming it is a safe harbor; and it works. And it has been working for how long?

Mr. LORD. For how long? That is a good question. I don't know the answer.

Mr. CONNOLLY. Well, we have been at war for 12 years, so presumably most of the duration of that 12 years. Almost paralleling

the same time frame that the chairman cited in his frustration, understandable frustration, where we have been trying to work this out in the ports. And I guess I just wonder what is the likelihood we could perhaps learn from a successful lesson and try to apply it to TSA.

Mr. LORD. Well, that is obviously an option. You know, there is another option. It is not, obviously, my call, but they could rerun the pilot on a limited scale and resource it and oversee it correctly. That is obviously one option. Or you could pursue a different model, as you suggested, you know, have the Government do the background checks and have the local ports provide the credential. That is what I call a hybrid option. But, again, that is not my call, that is the Congress's call.

Mr. CONNOLLY. I know it is the chairman's intention, perhaps, and I would join him in this if that is what he wishes to pursue, where we are going to hear from different examples of Federal agencies using these kinds of access cards, and undoubtedly we will have TSA back, but it will be most instructive to hear more about how the DOD has successfully managed to create and deploy a card that seems to work.

Mr. LORD. In harsh conditions. Actually, they would probably be a very good witness to have at your upcoming hearing.

Mr. CONNOLLY. Thank you very much.

Mr. Chairman, I yield back and I thank you for holding this hearing. It is most illuminating.

Mr. MICA. Well, thank you, Mr. Connolly. We will work with you.

I think, again, our intent is to sort of end this Groundhog Day and not have another one of these hearings. Again, there are just so many of them. I just was reminded by the staff, Mr. Connolly, that we had a one-year pilot program testing the readers back in 2006 at the Port of New York and New Jersey, and we had collected data on fingerprints at that juncture. But we have done that pilot program, we have done these pilot programs. Now we are at this stage and Mr. Lord said it might be valuable to go back and do another pilot program again with some data that is reliable.

Mr. Sadler, you said we spent $23 million on this pilot. Is there any money left?

Mr. SADLER. I believe there is some grant money. And out of the $23 million, as I understand it, the ports expended $15 million of the grant money.

And I would like to make a comment on the DOD, and maybe Mr. Lord can answer this. The DOD may be using a contact mode only, and I don't know if that is accurate or not.

Mr. MICA. But, you know, it is amazing. Are you the head of this program for TSA?

Mr. SADLER. I am the senior responsible executive.

Mr. MICA. And you don't know about the other programs?

Mr. SADLER. If they are using a CAC card, that is a contact biometric, sir.

Mr. MICA. I think the first thing I would do, if I were the head of this, Mr. Connolly, find out what works, is somebody doing it. Are we reinventing the wheel?

Mr. SADLER. Well, I will tell you, sir, contact is not going to work in the maritime environment. And if the CAC card is using a con-

tact biometric, where you have to put the card into a reader and put a PIN in, you are not going to get trucks and individuals through those gates using a contact mode.

Now, to fix that problem, we actually developed a specification with industry to wirelessly transmit an encrypted biometric. There is no standard in the Federal Government for that today. So if we compare models, we need to compare similar models.

Mr. CONNOLLY. Mr. Sadler?

Mr. Chairman?

Mr. MICA. Go ahead.

Mr. CONNOLLY. If I could just follow up on the chairman's point, Mr. Sadler. I am not trying to put you on the spot, but instead of theorizing about what CAC does or does not do, or whether it is applicable or it is not applicable, how about finding out? Would it be worth it? Would you be willing to commit that TSA is going to actually look at how CAC works?

Mr. MICA. Not just CAC, Mr. Connolly, but others. There are programs that do work.

Mr. CONNOLLY. And let's see if we can't fold that into our experience with our own pilot and see if we can't make a better product. Our interest here is success, it is not laying blame; and we would like to partner with you, but if we have a model that is successful, and you may be absolutely right, it may not fully be applicable, it may not be applicable at all, but trucks have to go to remote locations in Afghanistan, and previously Iraq, long convoys, so there may be comparable aspects of this that we could benefit from.

So I wonder if you would be willing to make that commitment, that you are going to look at that to see if there are aspects of it that could be relevant as we fold in lessons learned in the pilot.

Mr. SADLER. We will look at anything, sir, to make this pilot better and to make the result better.

Mr. CONNOLLY. I thank you for that commitment.

Mr. SADLER. And my comment was not meant to infer otherwise.

Mr. MICA. And maybe we will give him about 60 days or something like that, Mr. Connolly; call him back and see what he has learned that is out there that may be applicable, get an evaluation of where they are. Again, maybe you could come back to the committee with a better time line. We have this 90-day review in place.

And then maybe, if there is money left over, Mr. Lord and this report says that some of the basis by which you are proceeding is flawed. Even the data that is given to Coast Guard by which you are making a further evaluation isn't up to date. But, my God, this thing is going on forever. We do not have readers.

The other thing, too, what is the agency that sets the standard for the high risk?

Mr. SADLER. NIST.

Mr. MICA. Yes. Could you write them and ask them when they think they will have that standard? I have had them before Congress several times. I would just be curious if you would write them, and then I will ask the committee staff, we will sign a letter together, when they will have this ready. It was coming some years ago in the summer, and then it was coming in the fall, and then it was coming in mid-January. We still don't have this. And then

maybe if we don't, we can find some standards that Congress could adopt or something.

But to issue cards that do not have a biometric component that is reliable, cards that can be thwarted, which GAO has done in covert testing, and to have this system in place at great expense both to the truckers and the transportation workers, and maybe 129 doesn't sound like a lot to us, but to again have this whole thing not working and not as it was set out to provide us with some firm identification.

Now, we are just looking at TWIC. We are going to look at global entry, we are going to look at the CLEAR card, we are going to look at the pilot's license, all these IDs that TSA and Homeland Security have some say in, and try to see what we can do to ensure that we have better identification, because we are putting ourselves at risk. We are not knowing who we are dealing with. And if we can know that, you can speed up the process, the inconveniences to passengers, to business, truckers, to port personnel.

So that is our intent. I want to thank, again, Mr. Connolly for his involvement, Mr. Cummings, Mr. Meadows, and others. We have a small panel, so we can have this nice exchange. We will be back.

There being, I guess, no further business before the subcommittee, I thank the witnesses for being with us. I thank you and the committee stands adjourned.

[Whereupon, at 10:29 a.m., the subcommittee was adjourned.]