THREAT, RISK, AND VULNERABILITY: THE FUTURE OF THE TWIC PROGRAM

HEARING

BEFORE THE

SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JUNE 18, 2013

Serial No. 113–23

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

85–688 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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
JASON CHAFFETZ, Utah
STEVEN M. PALAZZO, Mississippi
LOU BARLETTA, Pennsylvania
CHRIS STEWART, Utah
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana
SUSAN W. BROOKS, Indiana
SCOTT PERRY, Pennsylvania
MARK SANFORD, South Carolina
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
YVETTE D. CLARKE, New York
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
RON BARBER, Arizona
DONDALD M. PAYNE, JR., New Jersey
BETO O'ROURKE, Texas
TULSI GABBARD, Hawaii
FILEMON VELA, Texas
STEVEN A. HORSFORD, Nevada
ERIC SWALWELL, California

GREG HILL, *Chief of Staff*
MICHAEL GEFFROY, *Deputy Chief of Staff/Chief Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

CANDICE S. MILLER, Michigan, *Chairwoman*

JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
STEVEN M. PALAZZO, Mississippi
LOU BARLETTA, Pennsylvania
CHRIS STEWART, Utah
MICHAEL T. MCCAUL, Texas *(Ex Officio)*
SHEILA JACKSON LEE, Texas
LORETTA SANCHEZ, California
BETO O'ROURKE, Texas
TULSI GABBARD, Hawaii
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

PAUL L. ANSTINE, *Subcommittee Staff Director*
DEBORAH JORDAN, *Subcommittee Clerk*
ALISON NORTHROP, *Minority Subcommittee Staff Director*

CONTENTS

THREAT, RISK, AND VULNERABILITY: THE FUTURE OF THE TWIC PROGRAM

Tuesday, June 18, 2013

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 10:09 a.m., in Room 311, Cannon House Office Building, Hon. Candice S. Miller [Chairwoman of the subcommittee] presiding.

Present: Representatives Miller, Duncan, Palazzo, Barletta, Stewart, Jackson Lee, O'Rourke, and Gabbard.

Mrs. MILLER. Good morning. The Committee on Homeland Security, Subcommittee on Border and Maritime Security, will come to order.

The subcommittee is meeting today to examine the future of the TWIC program, and our witnesses today are Rear Admiral Joseph Servidio from the U.S. Coast Guard, Steven Sadler, assistant administrator for the Office of Intelligence and Analysis, Transportation Security Administration, Stephen Lord with the Government Accountability Office, and Marcus Woodring, from the Port of Houston Authority. I will give them a more formal introduction in just a moment.

After 9/11, Congress passed the Maritime Transportation Security Act, or MTSA—it is sort of the acronym—to address several security vulnerabilities within the Nation's maritime and transportation sectors to prevent acts of terrorism that might impact our Nation. Among the provisions of the bill was a requirement from the Department of Homeland Security to develop a secure biometric access credential for individuals who require unescorted access to secure areas of regulated maritime facilities and vessels.

Ports by their very nature may be susceptible to acts of terrorism that could cause loss of life and severe economic disruption. The lack of access control at the Nation's ports was certainly a glaring security vulnerability that MTSA and subsequently the Transportation Worker Identification Credential—we commonly call TWIC—was intended to fix.

However, more than 11 years later, the TWIC card designed to prevent terrorists from gaining access to sensitive parts of the Nation's ports is currently no more than an extensive flash pass that costs workers about $130, principally to run criminal and terrorism background checks on prospective applicants.

Unfortunately, the biometric capabilities on the card are of little use because delays in the pilot program and rulemaking processes

have taken longer than ever intended. Pilot programs as envisioned by the Congress should have been designed to assist the Coast Guard in understanding the impact of proposed regulations on port operations and transportation workers alike, instead have been less than useful in the rulemaking process. Certainly, all of us are looking forward to hearing from our witnesses today on the extent to which the pilot was used to inform the rulemaking process.

Maritime security is not the provenance of the Federal Government alone. Private industry and other stakeholders have an important role to play, but the Government has introduced an unacceptable level of uncertainty when it comes to TWIC. For several years, Members of this committee have been calling on the Department to release the reader rules on—or effective assessment of the program. That strikes me as a very poor way to run this program.

Last Congress, I introduced the SMART Port Act, which passed through this committee and in the House, which would have made a series of reforms to the TWIC program. Included in that bill was a provision which required TSA to change the requirement for TWIC applicants who currently must go to an enrollment center twice and instead would allow for only visit to an enrollment center by allowing cards to be sent through the mail, just as passports and credit cards are today.

Through our efforts, that provision was attached to last year's Coast Guard authorization act and it was signed into law by the President. However, it does appear that TSA will not comply with the 270-day time line in the statute. Making two trips to an enrollment center seems to just be a very onerous burden on transportation workers.

So I will be very interested to hear how TSA will implement this provision, consistent with Congressional intent within that time frame. Millions of dollars of previously allocated and future grant spending are predicated on the TWIC providing a tangible security benefit at the Nation's ports and maritime facilities. We have an obligation to get this done right, and the way this program has been run so far does not give us the confidence that we are on the right course.

Today I hope that we will be able to examine the security purpose of the TWIC card, principally, as well as chart out the future of this program to ensure that we maximize security and minimize the burden on American workers.

With that, I would yield to the gentlelady from Texas, my Ranking Member, Ms. Jackson Lee.

[The statement of Chairwoman Miller follows:]

STATEMENT OF CHAIRWOMAN CANDICE S. MILLER

JUNE 18, 2013

After 9/11, Congress passed the Maritime Transportation Security Act—MTSA—to address several security vulnerabilities within the Nation's maritime and transportation sectors to prevent acts of terrorism that might impact the Nation's economy. Among the provisions of the bill, was a requirement for DHS to develop a secure biometric access credential for individuals who require unescorted access to secure areas of regulated maritime facilities and vessels.

Ports, by their very nature, may be susceptible to acts of terrorism that could cause loss of life and severe economic disruption. The lack of access control at the

Nation's ports was a glaring security vulnerability that MTSA, and subsequently the Transportation Worker Identification Credential (TWIC) was intended to fix.

However, more than 11 years later, the TWIC card, designed to prevent terrorists from gaining access to sensitive parts of the Nation's ports, is currently no more than an expensive flash pass that costs workers $129.75—principally to run criminal and terrorism background checks on prospective applicants.

Unfortunately, the biometric capabilities on the card are of little use because delays in the pilot program and rulemaking processes have taken longer than ever intended. Pilot programs, as envisioned by the Congress, should have been designed to assist the Coast Guard in understanding the impact of proposed regulations on port operations and transportation workers alike, instead have been less than useful in the rulemaking process.

I am looking forward to hearing from our witnesses on the extent to which the pilot was used to inform the rulemaking process.

Maritime security is not the provenance of the Federal Government alone. Private industry and other stakeholders have an important role to play, but the Government has introduced an unacceptable level of uncertainty when it comes to TWIC.

For several years, Members of this committee have been calling on the Department to release the reader rule to provide some certainty to workers and industry. Finally, we have a notice of proposed rulemaking that only requires TWIC readers to be used at the riskiest 5 percent of all TWIC-regulated vessels and facilities, nearly 6 years after workers were first required to pay for and obtain a TWIC card.

The proposed rule and findings of a recent GAO report, leads to some very simple questions about the threat, risk, and vulnerability at our Nation's ports, and how the TWIC program should be used to reduce the risk of a terrorist attack at the handful of facilities and vessels identified in the proposed rule.

I support a smart, risk-based approach to security, because I am convinced that maritime security is maximized through the use of a risk-based methodology. However, we should continue to scrutinize troubled programs by examining the principal reason they exist—in this case, preventing terrorists from doing economic harm to the Nation by disrupting the supply chain.

This hearing will hopefully answer the question of whether or not the TWIC program serves that purpose.

At this point, I believe it is still an open question as to what degree this card enhances maritime security. To that end, I hope to hear answers to the following questions: How many terrorist plots have been stopped by this card? Does TWIC enhance security in a tangible way? Can we address the security challenges at our Nation's ports in a more cost-effective, and balanced way?

Today, we will hear from the Government Accountability Office, which recently reported that, " . . . DHS has not demonstrated how, if at all, TWIC will improve maritime security." An assessment of how TWIC improves maritime security should have been one of the very first things the Department did when it began to implement the program.

It has been more than a decade since the legislation that required TWIC was first enacted, but it is troubling that we have never done a simple security or effectiveness assessment of the program. That strikes me as a poor way to run a program.

Last Congress, I introduced the SMART Port Act which passed through this committee and in the House, and would have made a series of reforms to the TWIC program.

Included in that bill was a provision, originally authored by Mr. Scalise, which required TSA to change the requirement for TWIC applicants who currently must go to an enrollment center twice, and instead would allow for only one visit to an enrollment center by allowing cards to be sent through the mail, just as passports and credit cards are today.

Through our efforts, that provision was attached to last year's Coast Guard Authorization Act and was signed into law by the President. However, it appears that TSA will not comply with the 270-day time line in statute.

Making two trips to an enrollment center is an onerous burden on transportation workers, and I will be very interested to hear how TSA will implement this provision, consistent with Congressional intent within that time frame.

Millions of dollars of previously allocated and future grant spending are predicated on the TWIC providing a tangible security benefit at the Nation's ports and maritime facilities.

We have an obligation to get this right, and the way this program has been run so far does not give me the confidence that we are on the right course.

Today, I hope that we examine the security purpose of the TWIC card, as well as chart out the future of this program to ensure that we maximize security and minimize the burden on American workers.

With that I will yield to the gentlelady from Texas.

Ms. JACKSON LEE. Thank you. Good morning.

I want to thank you, Madam Chairwoman, for holding today's hearing on the Department of Homeland Security's Transportation Worker Identification Credential program, something that many of us who have served on this committee have been dealing with not only with our constituents, but with our individual constituents and our corporate constituents, such as the Houston Port Authority.

We have tried to be responsive to individuals, constituents who simply need to get to work. To our dismay, there have been a number of challenges with this program, though I know that its intentions were well-intentioned. Challenges that I would like to offer for the record are the site locations for individuals, the hours that TWIC offices would be open, the difficulty of those who lived away from ports or places like Louisiana, where they had to secure them places away from their particular home base. So there have been a lot of issues that have arisen with TWIC, and as I indicated, the intentions were good to give this card of identification.

As a Member of Congress representing the port of Houston, the formal Chairwoman and Ranking Member of the Subcommittee on Transportation Security, and now working with this committee and Madam Chairwoman, I have been focused on the TWIC program since its creation.

Early on, I engaged ports, workers, and other stakeholders about the program and heard their concerns about how it was being deployed. Like many of my colleagues, my office has received significant amounts of TWIC casework primarily from workers having difficulty obtaining and renewing their TWIC cards.

While some of the issues with the program have largely been addressed, over time, other concerns have taken their place. I am particularly troubled by the Government Accountability Office report released last month that found serious problems with the TWIC reader pilot, which was intended to serve as the basis for the TWIC reader rulemaking. GAO has found that the pilot results were incomplete, inaccurate, and unreliable for informing Congress and for developing a final reader rule. GAO concluded these issues, calling to question the TWIC program's premise and its effectiveness in enhancing security.

These concerns, coupled with prior unaddressed issues related to security vulnerabilities with the program, prompted GAO to recommend that the Department not move forward until a security assessment of the program is completed. However, DHS, which was made aware of GAO's finding in December 2012, published a notice of proposed rulemaking for the TWIC readers in March of this year.

The NPRM would require readers to be deployed to only the highest-risk facilities and vessels accessed by just 5 percent of TWIC holders. While nothing precludes DHS from expanding the reader requirement in the future, such a limited deployment of biometric readers is not what Congress envisioned when it mandated the TWIC program, and I would encourage DHS to regroup and reassess, take more advice and counsel from stakeholders, more importantly reassess the technology. Technology is good. But it can be

even better, obviously, if we pause for a moment and try to develop the technology that will, in fact, work.

I am not advocating for broader deployment of readers at present, but I am concerned that DHS would ask port workers to pay for a biometric card whose biometric capabilities apparently may never be utilized. More broadly, I am concerned that DHS appears to be moving forward with its long-delayed reader rule before addressing the fundamental concerns that the program GAO has identified in its reports.

I was pleased to invite from the port Mr. Marcus Woodring, who we have engaged and over the years has given effective service in the United States Coast Guard and has dealt with the TWIC issue over and over again, to testify before the subcommittee today to offer his port's perspective on the issues facing the TWIC program. Besides being one of the Nation's major ports with a significant presence of petrochemical-related facilities and vessels, the port of Houston has been using TWIC readers voluntarily since 2008. Mr. Woodring currently serves as managing director for health, safety, security, and environment at the Port of Houston Authority, having recently served in the Coast Guard, cumulating with service as captain of the port for the Houston region.

I am especially interested in hearing from him about the port of Houston's experience with TWIC readers and his views on how the TWIC program can be strengthened going forward. I am delighted that he is here along with all the other witnesses, who I welcome. I want to hear from our DHS witnesses about how they plan to address GAO's recommendation, ensure TWIC programs become the maritime security program Congress intended, that ports and facilities can use without undue disruption to their businesses, and that DHS can justify asking maritime workers to continue to pay for.

Finally, I would note that I have previously supported one enrollment process, one fee, and one security threat assessment for transportation workers. Madam Chairwoman, I will tell you, with all the numbers of cards that I have heard workers having to have, it may be well time for us to try and do that.

I would like to hear from witnesses today about how the on-going issues of the TWIC program might affect this effort. Again, we are grateful for the witnesses, and I want to acknowledge Mr. O'Rourke and Ms. Gabbard present here today. Thank you very much, Madam Chairwoman.

I yield back.

[The statement of Ranking Member Jackson Lee follows:]

STATEMENT OF RANKING MEMBER SHEILA JACKSON LEE

JUNE 18, 2013

As a Member of Congress representing the port of Houston, the former Chairwoman and Ranking Member of the Subcommittee on Transportation Security, and current Ranking Member of the Subcommittee on Border and Maritime Security, I have been focused on the TWIC program since its creation.

Early on, I engaged ports, workers, and other stakeholders about the program and heard their concerns about how it was being deployed.

Like many of my colleagues, my office has received significant amounts of TWIC casework, primarily from workers having difficulty obtaining and renewing their TWICs.

While some of the issues with the program have largely been addressed over time, other concerns have taken their place.

I was particularly troubled by the Government Accountability Office (GAO) report released last month that found serious problems with the TWIC reader pilot, which was intended to serve as the basis for the TWIC reader rulemaking.

GAO found that the pilot results were incomplete, inaccurate, and unreliable for informing Congress and for developing a final reader rule.

GAO concluded these issues call into question the TWIC program's premise and its effectiveness in enhancing security.

These concerns, coupled with prior, unaddressed issues related to security vulnerabilities with the program, prompted GAO to recommend that the Department not move forward until a security assessment of the program is completed.

However, DHS, which was made aware of GAO's findings in December 2012, published a Notice of Proposed Rulemaking (NPRM) for the TWIC readers in March of this year.

The NPRM would require readers to be deployed to only to the highest-risk facilities and vessels, accessed by just 5% of TWIC holders.

While nothing precludes DHS from expanding the reader requirement in the future, such a limited deployment of biometric readers is not what Congress envisioned when it mandated the TWIC program.

I am not advocating for broader deployment of readers at present, but am concerned that DHS would ask port workers to pay for a biometric card whose biometric capabilities apparently may never be utilized.

More broadly, I am concerned that DHS appears to be moving forward with its long-delayed reader rule before addressing the fundamental concerns with the program GAO has identified in its reports.

I was pleased to invite a witness from the port of Houston, Mr. Marcus Woodring, to testify before the subcommittee today to offer his port's perspective on the issues facing the TWIC program.

Besides being one of the Nation's major ports with a significant presence of petrochemical-related facilities and vessels, the port of Houston has been using TWIC readers voluntarily since 2008.

Mr. Woodring currently serves Managing Director for Health, Safety, Security, and Environmental (HSSE) at the Port of Houston Authority, having recently served in the Coast Guard culminating with service as captain of the port for the Houston region.

I am especially interested in hearing from him about the port of Houston's experience with TWIC readers and his views on how the TWIC program can be strengthened going forward.

Similarly, I want to hear from our DHS witnesses about how they plan to address GAO's recommendations and ensure TWIC becomes the maritime security program Congress intended, that ports and facilities can use without undue disruption to their businesses, and that DHS can justify asking maritime workers to continue to pay for.

Finally, I will note that I have previously supported one enrollment process, one fee, and one security threat assessment for transportation workers.

I would like to hear from our witnesses today about how the on-going issues with the TWIC program might affect this effort.

Mrs. MILLER. Let me formally introduce our witnesses this morning. Again, we welcome all of you gentlemen. We appreciate you taking the time to be here.

First of all, Rear Admiral Joseph Servidio is the assistant commandant for prevention policy overseeing Coast Guard inspections and compliance, marine transportation systems, and commercial regulations and standards. He is responsible for navigation and boating safety, commercial vessels, ports and facilities, merchant mariner credentialing, and vessel documentation. We welcome you, Admiral.

Mr. Steven Sadler is the assistant administrator for the Office of Intelligence and Analysis at the Transportation Security Administration. In this role, he is responsible for the alignment of intelligence functions with vetting operations. Before joining TSA, Mr.

Sadler spent 25 years in the commercial maritime industry in a number of leadership roles. Welcome.

Mr. Stephen Lord directs the GAO's numerous engagements on aviation and surface transportation security issues and regularly discusses these issues before Congress in various industry forums. He supervised recent reviews of TSA passenger rail security programs and the TWIC program.

I am going to ask my Ranking Member to make the formal introduction of her constituent, who graciously joins us this morning.

Ms. JACKSON LEE. As I indicated, let me welcome all the witnesses, but I am particularly—and thank you, Madam Chairwoman, very much—particularly excited and pleased to be able to welcome Mr. Marcus Woodring, retired from the United States Coast Guard, as captain of the port of Houston-Galveston in 2011. We are delighted that he assumed his new and current position with the port of Houston in July of that year. He is responsible for safety, security, environmental stewardship, and emergency response at eight terminals along the Houston ship channel.

Over the years, I have had the privilege of working with Captain Woodring, and I would tell you, Madam Chairwoman, that he is one of the most engaged public servants and a problem-solver. I am delighted for him to bring that experience to this committee and this hearing that is so very important today. Welcome you and welcome you from Houston, Captain.

Mrs. MILLER. Thank you very much. Other Members are reminded that statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JUNE 18, 2013

This committee has a long history of TWIC oversight, going back almost to its inception. Since that time, DHS has made progress in standing up the program, vetting and enrolling approximately 2.5 million maritime workers.

Certainly, workers have done their part by applying for TWICs, submitting to background investigations, paying for their credentials, filing for waivers and appeals as necessary, and making multiple trips to ultimately receive their cards.

Yet, the program has long been plagued by delays, security vulnerabilities, and other problems.

These problems now have many questioning whether TWIC will ever be the transportation security program Congress envisioned when it enacted the Maritime Transportation Security Act of 2002 and the SAFE Port Act of 2006.

Just last month, the Government Accountability Office issued its latest in a series of troubling reports related to TWIC—this time on the reader pilots.

GAO concluded that the pilots were so severely flawed that they cannot be used to inform DHS' long-delayed rulemaking process for the TWIC readers.

Despite being made aware of GAO's serious concerns about the reliability of the reader pilot data and the TWIC program as a whole, Coast Guard published its Notice of Proposed Rulemaking (NPRM) for the TWIC readers earlier this year.

The NPRM divides ports and facilities into three risk groups, requiring only those in the highest-risk group—Group A—to install biometric readers for admittance to secure areas.

Facilities in Groups B and C can continue to allow TWICs to be used as "flash passes" with only a visual inspection required to gain access.

This means that only 5% of TWIC holders would be using their biometric credentials as Congress intended—with a biometric reader.

The remainder of TWIC holders will continue to use their card as an expensive flash pass.

Let me be clear—I am not advocating for deployment of readers at additional facilities or vessels at this time.

Rather, I believe the limited deployment of readers proposed by the rule raises some hard questions that need to be answered.

For example, what does it say about the security value of the TWIC, and the TWIC program itself, if DHS does not believe the program needs to be fully deployed at all regulated facilities?

And how can we continue requiring workers to pay for a biometric credential when, in the vast majority of cases, the full capability of that card will not be used?

To get answers to these and other vital questions, I strongly support GAO's recommendation for an assessment of the TWIC program prior to its continued deployment.

My staff has done significant stakeholder outreach on the rule, and I plan to file comments based on this outreach and our oversight work outlining my thoughts and concerns.

I look forward to a discussion today about what needs to be done to address the persistent problems facing the TWIC program.

In particular, I hope to hear from GAO in detail about their recommendations for the path forward for the program.

Mrs. MILLER. Again, thank you all for coming. At this time, the Chairwoman recognizes Admiral Servidio.

STATEMENT OF REAR ADMIRAL JOSEPH A. SERVIDIO, ASSISTANT COMMANDANT FOR PREVENTION POLICY, U.S. COAST GUARD

Admiral SERVIDIO. Good morning, Madam Chairwoman, Ranking Member Jackson Lee, distinguished Members of the subcommittee. I am Rear Admiral Joe Servidio, the assistant commandant for prevention policy for the Coast Guard, and I am honored to have this opportunity to speak before you today about the Coast Guard's role in enforcing compliance with the Transportation Worker Identification Credential and update you on the status of the TWIC reader rule.

The Coast Guard views TWIC as a key component of our layered security strategy. By providing a Nationally-recognized vetting standard and a common credential, TWIC promotes both security and economic efficiency. Issued under a uniform standard, TWIC allows facility and vessel operators, as well as law enforcement Nation-wide, to verify the identity of individuals using a single official document. TWIC enables transportation workers the flexibility to potentially move among facilities, vessels, and geographic regions during routine operations and in emergencies, maintaining security and facilitating resiliency.

While TWIC provides a standard baseline to determine suitability to enter the secure area of a facility or vessel regulated under the Maritime Transportation Security Act, it is only half of a two-part process. In addition to possessing a valid TWIC, an individual must also be specifically granted access to a secure area by a vessel or facility security officer.

To re-emphasize, the possession of a valid TWIC alone is not sufficient for the holder of a credential to access secure areas. This two-step process provides an additional layer of security to help protect vital maritime transportation infrastructure from unauthorized access or exploitation.

In addition to facility and vessel operators' significant efforts, Coast Guard inspectors have validated about 280,000 TWICs during planned and unplanned no-notice visits since 2009. The Coast Guard also reviews approximately 3,100 facility and 11,000 vessel security plans each year.

On 22 March 2013, the Coast Guard released the TWIC reader notice of proposed rulemaking, which outlines requirements for certain MTSA-regulated facilities and vessels to use electronic readers as part of their TWIC access control program. This NPRM is an important element of maritime security, as electronic readers allow for biometric confirmation of the TWIC holder's identity.

As with our other security regs, the Coast Guard balanced the expected security benefits of the requirement with the expected costs to industry. Accordingly, the reader rule proposes the use of TWIC readers only at the vessels and facilities where a security incident could pose the greatest consequence and where biometric verification of a TWIC would reduce risk.

Vessels and facilities not required to use electronic readers under this rule will still be required to conduct visual TWIC verifications. The GAO released a report questioning the security benefits of the TWIC and the way the Coast Guard used the results of the pilot program to inform the rule. We indicated to GAO that we were aware of the pilot program's limitations and used pilot data with discretion in developing the NPRM.

Moreover, we are convinced that TWIC, including the use of biometric readers, is an important part of our maritime security system. The GAO report was released while the NPRM common period was open. Given the timing of the report's release, a request by Representative Thompson and to ensure that we captured comments informed by the report, we extended the comment period by 30 days to 20 June 2013.

The Coast Guard hosted four public meetings around the country, providing other outlets for public feedback on the proposed regs. To date, we have received approximately 50 comments on the NPRM.

The Coast Guard's focus is to facilitate a secure and efficient maritime transportation system, and TWIC is an important tool in that effort. As part of our layered security strategy, we are committed to establishing and enforcing effective and efficient access control requirements through TWIC. Our reader NPRM solicits public comment, which we recognize as critical to port security success, and we will continue to work with the Department, TSA, industry groups, labor organizations, Congress, and other key stakeholders to find ways to improve service.

We know that we have more work to do, and we will ensure that Congress is informed of our progress. Thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Admiral Servidio follows:]

PREPARED STATEMENT OF REAR ADMIRAL JOSEPH SERVIDIO

JUNE 18, 2013

Good morning Madam Chairwoman and distinguished Members of the subcommittee. Thank you for the opportunity to testify before this committee on the Coast Guard's role in enforcing compliance of the Transportation Worker Identification Credential (TWIC) program within the maritime transportation system.

In previous testimonies, the Coast Guard has described our responsibility for ensuring industry compliance with TWIC regulations, the status of our deployment of handheld readers to field units, and our efforts to publish regulations for electronic TWIC readers in accordance with Congressional requirements as provided in the Security and Accountability For Every (SAFE) Port Act of 2006. This testimony will

provide an update of our on-going efforts to enhance the safety and security of the Nation's ports through the effective implementation of the TWIC program and recent publication of the TWIC Reader Requirements Notice of Proposed Rulemaking (NPRM).

The Coast Guard and the Transportation Security Administration (TSA) have formed a successful partnership in the joint management of the TWIC program and continue to work together to effectively build, manage, and improve it. TSA is responsible for TWIC enrollment, security threat assessment and adjudication, card production, technology, TWIC issuance, conduct of the TWIC appeal and waiver process as it pertains to credential issuance, and management of Government support systems. The Coast Guard is responsible for establishing and enforcing access control requirements at Maritime Transportation Security Act (MTSA) regulated vessels and facilities, which include the requirement for TWIC.

VALUE OF TWIC

TWIC is one part of the layered approach to port security and establishes a minimum, uniform, vetting, and threat assessment for mariners and port workers across the country. It ensures that workers needing routine, unescorted access to secure areas of facilities and vessels are vetted against a specific list of terrorism associations and criminal convictions and it provides a standard baseline for determining an individual's suitability to enter the secure area of a MTSA-regulated vessel or facility. However, it is only the first half of a two-part process. First, vessel and facility security personnel must determine that an individual posseses a valid TWIC.

Second, they must assess the individual's business case for entering a vessel or facility before granting the person unescorted access. The possession of a valid TWIC alone is not sufficient to gain the holder of that credential access to secure areas on vessels or facilities across the country. The TWIC provides a means by which a vessel or facility security officer can determine that an individual has been vetted to an established standard. It helps inform the security officer's decision to grant unescorted access to an individual. The facility owners/operators must maintain control of the access privileges to their respective facilities based on the valid TWIC and business case.

The Nation-wide recognition of TWIC promotes security and standardization. A 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—a step that was not feasible prior to TWIC implementation with potentially thousands of different facility-specific credentials. TWIC also allows transportation workers to move among facilities, vessels, and geographic regions as needed for routine market demands and during emergencies, while still maintaining security.

As required by the SAFE Port Act, the Coast Guard conducts at least two security inspections annually at MTSA-regulated facilities, with one inspection being unannounced. Vessels and facilities in all 42 Coast Guard Captain of the Port Zones are in compliance with TWIC requirements, and have been since the April 15, 2009 implementation date. In addition to the security activities taken by vessel and facility security officers, the Coast Guard conducts regular inspections, spot checks, and TWIC verifications at approximately 3,100 maritime facilities, 14,000 vessels, and 50 outer continental shelf facilities. Our enforcement program also includes the use of hand-held TWIC readers by Coast Guard personnel to conduct spot checks using the biometric capabilities of TWIC.

READER REQUIREMENTS

On March 22, 2013, the Coast Guard issued the TWIC Reader Requirements Notice of Proposed Rulemaking which outlines requirements for certain MTSA-regulated facilities and vessels to use electronic readers in accordance with Congressional requirements as provided in the SAFE Port Act as part of their TWIC access control program. The Notice of Proposed Rulemaking maintain the visual verification requirement for remaining vessels and facilities. Per 33 CFR Parts 104, 105, and 106, this visual inspection must include, at a minimum:

- A match of the photo on the TWIC to the individual presenting it;
- Verification that the TWIC has not expired; and
- A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

This Notice of Proposed Rulemaking is an important element of the Coast Guard's maritime security mission. Electronic readers add an important additional layer of security by providing biometric confirmation of the TWIC holder's identity.

As you are aware, the Government Accountability Office (GAO) recently released a report questioning the security benefits of TWIC, and the way in which the Coast Guard used results of the pilot program to inform the reader rule. As we indicated to GAO in our reply to their report, we were aware of the pilot program's limitations, and used it with discretion in developing the Notice of Proposed Rulemaking. Moreover, we are convinced that TWIC, including the use of biometric readers, can and should be a part of the Nation's maritime security system. In part, because the GAO report came out while the Notice of Proposed Rulemaking public comment period was open, we extended the open period by 30 days to June 20, 2013, to ensure that the public had sufficient opportunity to review and provide feedback on the proposed regulations.

CONCLUSION

TWIC is improving access control at vessels and maritime facilities across the country. Its standard, Nation-wide recognition secures and facilitates a resilient, mobile transportation workforce during routine and emergency situations. The Coast Guard's NPRM will further increase the security value of TWIC to the Nation by focusing on the highest-risk vessels and facilities. We will continue to work with TSA, industry groups, labor organizations, and other stakeholders to find ways to reduce costs, and improve service. As part of that process, we will continue to monitor the costs and benefits of TWIC, as well as the external security environment. In all of these matters, our primary concern is to provide the American people with a secure and efficient marine transportation system. We know we have more work to do, and we will ensure Congress is informed of our progress.

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

Mrs. MILLER. Thank you very much, Admiral.

The Chairwoman now recognizes Mr. Sadler for his testimony.

STATEMENT OF STEVE SADLER, ASSISTANT ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Mr. SADLER. Good morning, Chairman Miller, Ranking Member Jackson Lee, and distinguished Members of the subcommittee. Thank you for the opportunity to speak with you today about TSA's role in the TWIC program.

TWIC provides a uniform biometric tamper-resistant credential that is issued following the successful completion of the security threat assessment. For those with a business need, the credential is required to gain unescorted access to secure areas at port facilities and vessels regulated under the Maritime Transportation Security Act.

TSA is responsible for enrollment and security threat assessments, as well as system operations and maintenance. TSA conducts a comprehensive security threat assessment, and more than 2.3 million transportation workers hold active TWIC cards. These credentials represent a capability that didn't previously exist in the maritime environment.

We have taken the following steps to improve the program and reduce burden on workers while maintaining the security objectives of the program. In August 2012, we announced the Extended Expiration Date TWIC initiative, a one-time effort that runs through December 2014. This initiative allows workers to extend their credential for 3 years at half the cost of a 5-year credential and requires only one visit to an enrollment center.

Last month, TSA processed over 58,000 requests for TWIC cards. Of these, almost 23,000 were for the 3-year credential. This means the travel burden on 39 percent of all current applicants can be cut in half. To reduce wait times for workers, we have added customer

service representatives and refined contractual performance standards.

We have developed a web-based process that allows workers to apply for an Extended Expiration Date TWIC or a replacement card, and we have a plan to increase mobile enrollment opportunities. We are in the process of transitioning our single enrollment and system maintenance contract to two separate contracts. This will give us better oversight capability and allow the contractors to focus on their core functions.

As directed by Congress, we are reforming the program by implementing the one-visit initiative to enable all workers to apply for and obtain a credential with a single visit to an enrollment center. Beginning with a pilot program in Alaska next month, we will expand the initiative Nation-wide in 2014.

With one visit, an applicant will provide identification and biometric information during a single visit to an enrollment center. If approved to receive the credential, TSA will mail the card directly to the applicants, saving the applicant time and travel cost. We are more than doubling the number of enrollment centers from 136 to approximately 300 sites by leveraging existing assets that will allow transportation workers to apply for a TWIC or hazardous material endorsement at the same location.

The SAFE Port Act directed DHS to conduct a reader pilot to test the viability of biometric card readers. Seventeen sites participated on a voluntary basis. These facilities started using readers in August 2008, and despite numerous challenges identified in our report to Congress submitted in February 2012, the pilot generated considerable data that proved helpful in evaluating reader performance and assessing the impact of readers at maritime facilities.

We concluded that the reader system functions properly when designed, installed, and operated in a manner consistent with the business requirements of the facility or vessel operation. When TWIC readers are deployed, it will determine whether a card is authentic, valid, and issued by TSA. They will also facilitate access control decisions made by port facilities and vessels. In the biometric mode, readers confirm through a fingerprint match that the person using the card is the rightful owner of the card.

Prior to the TWIC program, there was no standard identity verification or background check policy for entrance to a port facility or vessel. Today, facility and vessel owners and operators can look for one identification document based on an extensive background check.

The use of readers and biometric verification will enhance security at MTSA-regulated port facilities and vessels. Thank you for the opportunity to be here today. I look forward to taking your questions.

[The prepared statement of Mr. Sadler follows:]

PREPARED STATEMENT OF STEVE SADLER

JUNE 18, 2013

Good morning Chairman Miller, Ranking Member Jackson Lee, 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.

To fulfill a security mission of such scale, the Department of Homeland Security (DHS) leverages the expertise of its components to evaluate the entities that comprise the maritime domain and design security measures to counter potential threats. TWIC provides a uniform, industry-wide, biometric, tamper-resistant credential that is issued following successful completion of a security threat assessment (STA). Following successful completion of the STA and payment of relevant fees, eligible maritime workers are provided a tamper-resistant biometric credential that permits unescorted access to secure areas of port facilities and vessels regulated by the USCG under MTSA. These security benefits are most fully realized when the credential is used in conjunction with readers that can provide electronic verification.

TSA and the United States Coast Guard (USCG) jointly administer the fee-based TWIC program, which was established under Section 102 of the Maritime Transportation Security Act (MTSA) of 2002. The Act required the Secretary (at the time the Secretary of the Department of Transportation) to issue biometric transportation security cards to prevent unauthorized individuals from entering an area of a vessel or facility designated as a secure area. Currently, TSA is responsible for enrollment, STAs, and systems operations and maintenance related to TWICs while the USCG is responsible for establishing and enforcing access control standards including requirements for TWIC readers at MTSA-regulated facilities and vessels.

TSA began National deployment of the TWIC program on October 16, 2007, with the enrollment of maritime workers at the Port of Wilmington, DE. Since that time, TSA has conducted comprehensive STAs and issued TWIC credentials to over 2.5 million workers while identifying and preventing approximately 50,000 TWIC applicants who did not meet the required security standards from receiving a TWIC.

TWIC: MEETING INDUSTRY NEEDS AND SECURITY REQUIREMENTS

The TWIC program represents an important maritime security measure by allowing facility and vessel security operators to verify that the holder has successfully passed the STA, through possession and visual inspection of the TWIC credential. Workers at the approximately 13,825 vessels and 3,270 maritime facilities that the USCG regulates under MTSA have been required to present their TWIC for unescorted entry to secure areas of those facilities since mid-April 2009. Until TWIC readers are in place, security access personnel are required to visually inspect the TWIC prior to granting unescorted access to secure areas on-board regulated vessels and at facilities.

TWIC reader systems are designed to 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 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.

A TWIC is valid for 5 years. The cost is $129.75, unless a worker has a comparable STA and uses it to establish TWIC eligibility, in which case the cost is $105.25. In late August 2012, DHS announced the Extended Expiration Date (EED) initiative under which eligible workers have been able to submit a request to extend the expiration date on their TWIC by 3 years and pay a $60 card replacement fee. The EED is a one-time initiative through December 31, 2014. The TWIC reader requirements have been proposed by USCG in a Notice of Proposed Rulemaking published on March 22, 2013. The NPRM proposals, if finalized as published, would require TWIC readers for certain high-risk vessels and facilities. Use of readers at these sites would enhance security by verifying the validity of the TWIC card as well as the identity of the card owner.

TSA is committed to partnerships with stakeholders, including the private sector, to carry out its mission. To meet the demands of the TWIC program, the TSA will provide MTSA-regulated facility owners and operators with a list of TWIC readers that meet current TWIC specifications as outlined in current guidance. 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.

"ONEVISIT" INITIATIVE AND OTHER PLANS TO ENHANCE CUSTOMER SERVICE

TSA will soon implement the "OneVisit" initiative to facilitate card issuance to eligible applicants and individuals needing a replacement TWIC. The initiative will enable individuals to apply for and obtain a TWIC with a single visit to an enroll-

ment center and will begin with a pilot in Alaska this summer and expand Nationwide in 2014 after TSA carefully evaluates the pilot results. Under "OneVisit," an applicant will visit an enrollment center to provide identification and biometric information. Upon successful completion of an STA, TSA will directly mail a card to the applicant. "OneVisit" will eliminate the need for the transportation worker to make a follow-up visit to an enrollment center to activate the card and select a Personal Identification Number (PIN). Eliminating this second visit saves the applicant time and travel costs, as well as easing crowding at enrollment centers.

The Coast Guard and Maritime Transportation Act of 2012 mandates that, within 270 days from the date of enactment, DHS reform the process for TWIC enrollment, activation, issuance, and renewal to require no more than one in-person visit to a designated enrollment center, except in cases where extenuating circumstances exist requiring more than one visit. DHS made clear that, while a plan would be initiated within 270 days to reform the process, it would likely take additional time to fully implement the provision in a manner that preserved the security of the credential.

In addition to "OneVisit," TSA is committed to providing enhanced customer service in a variety of ways. TSA will expand the number of TWIC enrollment centers from 136 to approximately 300 sites by transitioning Hazardous Materials Endorsement (HME)/TWIC enrollments sites to Universal Enrollment Service Centers. This will permit individuals to apply for a TWIC or HME at the same location, and shorten travel distances for many applicants. TSA is also increasing its oversight of customer service at our enrollment centers and has added call center representatives to reduce call wait times.

THE TWIC READER PILOT

In October 2006, pursuant to the SAFE Port Act, Congress mandated that DHS conduct a TWIC reader pilot to inform reader requirements prior to Nation-wide implementation and test the viability of selected biometric card readers while examining the technical aspects of connecting TWIC readers to access control systems. Seventeen sites participated in the reader pilot on a voluntary basis. These facilities used readers in conjunction with TWICs starting in August 2008. The pilot faced several constraints, including extreme differences in the nature of operations at participating sites. Additionally, the participating sites had to ensure that the use of the new readers and test protocols did not interfere with the security and daily operations of the facilities. Notwithstanding these challenges, the TWIC reader pilot generated considerable data that proved helpful in evaluating reader performance and assessing the impact of using readers at maritime facilities.

Following analysis of the pilot results, TSA concluded 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. TSA also found that reader systems can facilitate access decisions efficiently and effectively despite the operational and technological difficulties that affected performance at some pilot locations. While a recent Government Accountability Office (GAO) report evaluating the results of the TWIC reader pilot program concluded that that DHS should not use the analysis of the pilot program as basis for developing the final TWIC reader regulation, the pilot did produce valuable information concerning the environmental, operational, and fiscal impacts of the use of TWIC readers.

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 opportunities for fraud as well as security risks. 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. The use of readers and biometric verification will enhance security at MTSA-regulated port facilities and vessels.

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.

Mrs. MILLER. Thank you very much.

The Chairwoman now recognizes Mr. Lord.

STATEMENT OF STEPHEN M. LORD, DIRECTOR, FORENSIC AUDITS AND INVESTIGATIVE SERVICES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. LORD. Good morning, Chairwoman Miller, Ranking Member Jackson Lee, and other distinguished Members of the committee. I am really pleased to be here today to discuss our recent work on the TWIC pilot. As context, I would like to note that GAO has conducted an extensive body of work on a TWIC program spanning several years, which I believe gives me some unique insights to come in on the program today.

The overall message that I wanted to convey today—I think this is a very important message—is that the pilot results reported to Congress in February 2012 should not be used as a basis to inform the current rulemaking or to inform decision-making. Why is that? As we noted in our May 2000 report, we identified a number of planning, data collection, and reporting challenges that we believe made the pilot results unreliable.

I am a little surprised to see on the March 22 NPRM that the Coast Guard concluded that the cards function properly and enhance security, as we found this very difficult to extrapolate from the pilot results.

In terms of planning, we think it is notable that DHS did take some important initial steps to address the pilot planning issues we identified in our 2009 report. At the same time, it did not develop an evaluation plan or performance standards as we recommended. In terms of data collection, we identified several limitations in the way data was collected during the pilot. For example, TSA and the independent test agent did not always record clear baseline data for comparing reader performance. They also did not collect complete data on card failures or the reasons an individual was denied access to a facility.

Also, the operational impact of using TWICs, that was one of the key purposes of the pilot, with readers was not consistently documented across pilot sites. As a result of these challenges, this made it really difficult to determine whether the problems encountered at the pilot sites were due to the card itself, the card reader, or the way the users were using them or a combination of all three.

In terms of the report to Congress, we found that some of the information in the report was not always supported by the pilot data. For example, assessments of entry times at ports—this is really important piece of data—the throughput times were—seem to have been mixed up with the reader response time, which is calculated in a controlled laboratory setting.

DHS's report also stated that the TWIC readers can enhance security, even though that type of data was not collected during the pilot, nor was it a purpose of the pilot. Thus, it is still unclear how TWICs—using TWICs with readers will improve security even though we recommended that the Department assess this in our May 2011 report.

To be fair, DHS officials, TSA officials did note that several challenges affected their ability to collect reliable data. For example, TSA noted that pilot participation was voluntary and, in some cases, it was analogous to herding cats. It is difficult to ensure consistency.

TSA and the Coast Guard also said the independent test agent did not always collect and record key data consistently. We spoke to the independent test agent. He identified some resource constraints. Basically, they didn't have the physical presence in all locations to really figure out why the cards weren't working. However, we believe these risks could have been mitigated through better pilot planning and implementation.

In closing, given the many issues we identified, we believe Congress should consider repealing the requirement that the final regulations for the card readers be consistent with the findings of the pilot. Essentially, we think those two events should be de-linked.

Instead, we still believe Congress should require DHS to complete a security assessment to clearly show how using TWICs with readers will actually improve security over and above the systems that are already in place. This is something we recommended in our May 2011 report, which is still an open recommendation. As part of this assessment, we believe they should consider alternative credentialing approaches, including consideration of a more decentralized approach. We think it is really important to look at other approaches for achieving the same goal.

Madam Chairwoman, other Members of the committee, this concludes my prepared statement. I look forward to your questions. Thank you.

[The prepared statement of Mr. Lord follows:]

PREPARED STATEMENT OF STEPHEN M. LORD

JUNE 18, 2013

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL.—CARD READER PILOT RESULTS ARE UNRELIABLE; SECURITY BENEFITS SHOULD BE REASSESSED

GAO–13–695T

Chairman Miller, Ranking Member Jackson Lee, 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

[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).

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 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. USCG published the TWIC card reader notice of proposed rulemaking (NPRM) on March 22, 2013, and has since extended the public comment period to June 20, 2013.[6]

To help inform this rulemaking and to fulfill the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) requirement,[7] 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.[8] Among other things, the SAFE Port Act required that DHS submit a report on the findings of the pilot program to Congress.[9] DHS submitted its report to Congress on the findings of the TWIC reader pilot on February 27, 2012.[10] The Coast Guard Authorization Act of 2010 required that, among other things, GAO conduct an assessment of the report's findings and recommendations.[11]

We have been reporting on TWIC progress and challenges since September 2003.[12] Among other issues, we highlighted steps that TSA 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.[13] 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.[14] 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.[15]

My statement today highlights the key findings of our May 8, 2013, report on the TWIC program, which 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.[16] 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

---

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

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

[6] 78 Fed. Reg. 17,782 (Mar. 22, 2013); 78 Fed. Reg. 27,335 (May 10, 2013).

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

[8] 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).

[9] 46 U.S.C. § 70105(k)(4).

[10] 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, Pub. L. 109–347 (SAFE Port Act) Final Report. Feb. 17, 2012.

[11] Pub. L. No. 111–281, § 802, 124 Stat. 2905, 2989.

[12] GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain,* GAO–03–1155T (Washington, DC: Sept. 9, 2003).

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

[14] 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, DC: Nov. 18, 2009).

[15] GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives,* GAO–11–657 (Washington, DC: May 10, 2011).

[16] GAO, *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed,* GAO–13–198 (Washington, DC: May 8, 2013).

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 (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.[17] 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 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 did not utilize the data analysis plan.[18] 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

[17] GAO–10–43.

[18] 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.

thus it was unable to determine whether errors encountered were due to TWIC cards, readers, or users, or some combination thereof.

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 contact-less interface) the reader used to communicate with the TWIC card during data collection.[19] 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 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

[19] As used in this statement, "contact-less 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.

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 NPRM, which included results from the TWIC card reader pilot.[20] We subsequently removed the recommendation from our final report, given that USCG had moved forward with issuing the NPRM 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 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,[21] 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 2011 report. 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 Miller, Ranking Member Jackson Lee, and Members of the subcommittee, this concludes my prepared statement. I would be happy to respond to any questions that you may have.

---

[20] 78 Fed. Reg. 17,782 (Mar. 22, 2013).
[21] 46 U.S.C. § 70105(k)(3).

Mrs. MILLER. I thank the gentleman. The Chairwoman now recognizes Captain Woodring.

STATEMENT OF CAPTAIN MARCUS WOODRING, USCG (RET), MANAGING DIRECTOR, HEALTH, SAFETY, SECURITY, AND ENVIRONMENTAL, PORT OF HOUSTON AUTHORITY

Captain WOODRING. Good morning, Chairman Miller, Ranking Member Jackson Lee, and distinguished Members of the subcommittee. We would like to thank Chairman Miller for holding this important hearing today. I must also recognize Ranking Member Jackson Lee for inviting the Port of Houston Authority as the industry witness. As you know, the port of Houston is in the Ranking Member's district, and we have benefited from both her leadership and advocacy on behalf of the port.

The port of Houston is comprised of the Port Authority's eight public terminals, along with more than 150 private terminals. The port is consistently ranked first in the United States in foreign waterborne tonnage, first in imports, second in export tonnage, and second in total tonnage. The port of Houston is also home to the largest petrochemical complex in the Nation.

Results of a recent economic impact study show that ship channel-related businesses at the port of Houston are responsible for more than 2.1 million jobs and annually generate $499 billion in economic activity, contributing over $52 billion in tax revenue Nationally.

The Port of Houston Authority was not part of the TWIC reader pilot program but has been utilizing installed TWIC readers since 2008, so we speak from real-world experience. The Port of Houston Authority started very early, with the installation of access point hardware, which could utilize the features of the TWIC card. The initial infrastructure was purchased with close to $10 million in port security grant funding.

The Port of Houston Authority currently has over 350 access points that can read the TWIC card, of which 73 are biometric. Not all access points used the biometric or coded access technology due to the tremendous flow of commerce through our gates. Our Bayport container terminal, for example, handles close to 19,000 vehicles a week. To facilitate commerce, we currently use the TWIC as a flash pass in our vehicle entrance lanes in conjunction with our visitor management system.

Let me expand on that point for just one moment. Having a TWIC is just one part of the regulated access control. I have a TWIC, but that does not give me unfettered access to any restricted port in the country. I must also have a valid business reason to be there. Management of that validation is left to terminal operators.

For repeat visitors, we issue a Port of Houston Authority ID card. For occasional visitors, we have designated certain trusted agents to enter names into our visitor management system. On any given day, we average over 3,000 names in that system, all that have a valid business reason for being on-board our facilities and overall have more than 35,000 TWIC cards registered with our credentialing office. The key takeaway is the possession of a TWIC itself is just a piece of the overall security process.

During my time as captain of the port for the U.S. Coast Guard, the TWIC was first being introduced and issued in Houston. It took me several months to obtain my initial TWIC card. I recently applied for the 3-year extension and witnessed some process improvements.

I would also like to note that when I was with the U.S. Coast Guard, I had the pleasure of accompanying the Ranking Member Jackson Lee to the TWIC office in Houston to activate her card in August 2008. Ma'am, I would like to take this opportunity to remind you that your card expires in 60 days.

[Laughter.]

Captain WOODRING. The benefits of the TWIC reader program are clear. Individuals have a Federally-issued tamper-proof credential that can be used Nation-wide. The program ensures that individuals have been screened against the terrorism database, something I cannot do. The threat of a transportation security incident is reduced at the macro level, but there are still gaps in the system.

Most ports issue their own credentials in addition to the TWIC card. I personally carry a port of Houston ID and my TWIC card on a daily basis. Secondly, the background check is only conducted at a very high level for very serious crimes. As a facility owner and operator, we strive to prevent any crime on our docks and still conduct our own local background checks on our employees for lesser crimes, such as driving while intoxicated, theft, or assault. These lesser crimes are just as important to us.

Finally, the TWIC background check is a snapshot in time. Unless self-reported, there does not appear to be a constant and ongoing linkage between the TWIC issuance and local criminal databases. Currently, the background check of the TWIC program is only as good as the day it was conducted.

I would like to leave the subcommittee with two thoughts today. The Port of Houston Authority has received over $60 million in port security grant funding, and it continues to be vital to our security posture. We are in the process of making application for the 2013 port security grants, one of which will request handheld TWIC readers. It is critical to our National security that the port security grant program remain independent of other grant programs and that the erosion of the funding level ceases.

Second, the initial intent of the Transportation Worker Identification Credential program was to credential all transportation workers in all transportation modes. It was envisioned as a Nationwide solution to be used at airports, seaports, rail, pipeline, trucking, and other mass transit. Someday this program will theoretically expand to all those modes of transportation, and what comes out of hearings such as this will more broadly impact the future of the TWIC program.

Thank you, and I look forward to your questions.

[The prepared statement of Captain Woodring follows:]

PREPARED STATEMENT OF CAPTAIN MARCUS WOODRING

JUNE 18, 2013

Chairman Miller, Ranking Member Jackson Lee, and Members of the subcommittee, I am Marcus Woodring. I serve as the managing director for health, safety, security, and environmental (HSSE) at the Port of Houston Authority.

We would like to thank Chairman Miller for holding this important and vital hearing today. I must also recognize Ranking Member Jackson Lee for inviting the Port of Houston Authority as the industry witness. As you may know, the port of Houston is in the Ranking Member's district and we have benefitted from her leadership and advocacy on behalf of the port.

Security of our Nation's borders, both land and maritime, is a vexing problem with many different components and concerns. While I certainly do not have the solutions to all the challenges, I can tell you about our maritime port facilities, how we operate, and the impact of the TWIC program.

First, let me begin by giving you a short background about myself. I earned an undergraduate degree at Brown University, and a Masters degree at Cornell University. I'm fairly new at the Port of Houston Authority, having been hired in 2011 after "retiring" from a 27-plus year career in the U.S. Coast Guard. My U.S. Coast Guard service culminated as the Captain of the Port for the Houston region.

There is a saying that if you've seen one port, you've seen one port—every port in the country is organized differently. But let me tell you about ours. The port of Houston is comprised of the Port Authority's eight public terminals along with 150-plus private industrial terminals along the 25-mile long upper Houston Ship Channel.

Each year, more than 229 million tons of cargo moves through the port of Houston, with more than 8,100 vessel calls and 200,000 barge transits, trading with over 200 countries around the globe. The port is consistently ranked first in the United States in foreign waterborne tonnage, first in U.S. imports, and second in U.S. export tonnage, and it is also ranked second in the United States in total tonnage.

The port of Houston is the largest importer and exporter of petroleum and petroleum products in the United States, which is no surprise, as it is home to the largest petrochemical complex in the United States, and is the second-largest petrochemical complex in the world.

As one of the world's busiest ports, the port of Houston is a large and vibrant component of the regional economy. Results of a recent economic impact study show that ship channel-related businesses at the port of Houston were responsible for more than 1 million jobs throughout Texas. This activity helped generate more than $178.5 billion in State-wide economic impact and more than $4.5 billion in annual State and local tax revenues. For the United States, the port's impact is even greater, with 2.1 million jobs, $499 billion in economic activity and $52.1 billion in tax revenue.

Considering this economic impact and the volume of cargo traveling the waterways of the port of Houston, there are potentially significant National implications should a Transportation Security Incident occur within our maritime domain. Now I will get more specific in answering the questions on today's agenda.

(1) CURRENT USE OF TWIC READERS

I have read the recent GAO report, but the Port of Houston Authority was not part of the TWIC Reader Pilot Program. Instead, we have been utilizing installed TWIC readers since 2008, so I will speak from that experience. In an attempt to meet the "spirit of the regulations", the Port of Houston Authority started very early with the installation of access point hardware which could utilize the features of the TWIC card. The initial phases of the TWIC reader installation project was funded close to $10 million dollars in Port Security Grant funding ($6.3 million in Round 5, $1.7 million in Round 7, and $1.2 million in Round 8). The Port of Houston Authority currently has over 350 access points which can read the TWIC card, of which 73 are biometric.

Not all access points use the biometric or coded access technology due to the tremendous flow of commerce through our gates. For example, the Bayport Container Terminal handles close to 19,000 vehicles a week. That equates to an average of almost two trucks per minute, around the clock, at just one of our three major terminals. To facilitate commerce, we currently use the TWIC as a "flash pass" in our vehicle entrance lanes, in conjunction with our Visitor Management System (VMS).

Let me expand on that point for a moment, having a TWIC is just one part of regulated access control. I have a TWIC, but that does not give me unfettered access to any restricted port in the country. I must also have "a valid business reason" to

access the restricted or secure area. Management of the validation of that "business reason" is left to terminal operators, and managed at the Port of Houston Authority by our Credentialing Office. For our repeat visitors, we issue a Port of Houston Authority ID card. For occasional visitors, we have designated certain "trusted agents" to enter names into our Visitor Management System. On any given day, we average over 3,000 names in our system that all have a "valid business reason" for being on-board our facilities, and overall have 35,000 TWIC cards registered with our Credentialing Office. The key "take-away" is that possession of a TWIC itself is just a piece of the overall security process.

(2) ENROLLMENT AND ISSUANCE OF TWIC

In 2008, during my time as Captain of the Port for the U.S. Coast Guard, the TWIC was first being introduced and issued in Houston. I heard many stories about the issuance process and while not required by law to obtain a TWIC (my military ID and status as a member of the U.S. Coast Guard precluded the requirement), I chose to personally apply and pay for a card so that I could witness the process first-hand, desiring to validate the stories I was hearing. The initial call to schedule an appointment took over 3 hours on the phone. After several months, I was able to determine my card was ready for pick-up. I made an appointment for 0630 and was told my card could not be located. After revealing my position with the U.S. Coast Guard, another search quickly located my card. The activation was fairly easy.

Knowing that my card was due to expire in early 2013, I recently applied for the 3-year extension option. Again, the phone call took over 2 hours. The turn-around time was much quicker, and I was notified within several weeks that my new card was ready for activation. My appointment time had five other people, and we all lined up in front of computers and activated our new cards in less than 30 minutes, a vast improvement in the processing.

(3) SECURITY BENEFITS OR PROBLEMS WITH TWIC PROGRAM

The benefits are clear, individuals have a Federally-issued, tamper-proof credential that can be used Nation-wide. The program ensures that individuals have been screened against a terrorism database (aka the Security Threat Assessment), which I cannot do. The threat of a Transportation Security Incident is reduced at the macro level. It also allows facilities to automate access by coding the TWIC to activate unmanned entrance points.

But there are still gaps in the system.

- Most ports still issue their own credentials in addition to requiring a TWIC; I personally carry a Port of Houston Authority ID and my TWIC on a daily basis. The Port of Houston Authority ID is required to prove that I have a "valid business reason" for being on the docks.
- Second, the background check is only conducted at a very high level, for serious crimes. As a facility owner and operator, we strive to prevent any crime on our docks and still conduct our own local background checks on our employees for lesser crimes, such as driving while intoxicated, theft, or assault. These "lesser crimes" are just as important to me in keeping our facilities safe and secure.
- Finally, the TWIC background check is a "snapshot" in time. Unless self-reported, there does not appear to be a constant and on-going linkage between the TWIC issuance and local criminal databases. Again, I have over 35,000 TWIC cards registered in my access system, and the background check of the TWIC program is only as good as the day it was conducted.

(4) THOUGHTS CONCERNING THE TWIC READER NPRM

The Port of Houston Authority has already submitted "comments for the docket" concerning the TWIC Reader NPRM. I will briefly summarize those comments as they are available for public viewing on the docket website and included as an attachment to my prepared testimony.

As I mentioned earlier, the TWIC is just a piece of the overall security process. The TWIC Reader Rule emphasizes the need to ensure the TWIC is valid, thereby simply ensuring the "Security Threat Assessment" is valid. There is enormous cost involved to ensure this sense of security. The background check associated with the TWIC card isn't the risk point, the risk point is when the "valid business reason to be in the secure area" is accepted by the individual facilities, allowing access to the waterfront. That part of the process is more critical than obtaining the TWIC card itself, but unregulated and left to individual facility security officers.

We also asked for clarification of several items:

- The process for reporting inoperable readers to the U.S. Coast Guard, and associated waiver process, is problematic if it stops the flow of commerce while awaiting permission.
- The definition of "CDC in bulk" is vital to which determining which level of TWIC compliance a facility must obtain, and we asked for the term to be better defined.
- Recordkeeping requirements at a cruise terminal also need clarification as the Facility Security Plans are often "shared" between the cruise line and facility owner.
- Finally, we requested that the "recurring unescorted access" waiver be better defined to accommodate workers such as porters, who may be required to enter and exit a cruise terminal up to 30 times each, per day.

I would like to leave the subcommittee with two thoughts today—the Port of Houston Authority alone has received over $60 million dollars in Port Security Grant funding to date, and it continues to be vital to our security posture. We are in the process of making our applications for the fiscal year 2013 Port Security Grants, one of which will request handheld TWIC readers for our remote access points and for use during heightened levels of MARSEC. It is critical to our National security for the Port Security Program to remain independent of other grant programs, and that the erosion of the funding level cease.

Second, the initial intent of the Transportation Worker Identification Credential program was to credential all transportation workers in all transportation modes. It was envisioned as a Nation-wide solution to be used at airports, seaports, rail, pipeline, trucking, and other mass transit facilities. Someday, this program will theoretically expand to all those modes of transportation, and what comes out of hearings such as this will more broadly impact the future of the TWIC program.

This concludes my prepared statement. I would be pleased to respond to any questions that you may have. Thank you.

ATTACHMENT.—PORT OF HOUSTON AUTHORITY'S COMMENTS FOR DOCKET RE: TWIC READER NPRM

We appreciate the effort being put forth with the TWIC program to ensure each potential port worker has been screened with a background check. Unfortunately, the background check doesn't go deep enough to ensure we are protected from crime. The TWIC Reader Rule wrongly emphasizes the need to ensure the TWIC is valid, thereby simply ensuring the very broad background check is valid. There is enormous cost involved to ensure this small sense of security. The background check associated with the TWIC card isn't the risk point, the risk point is when the "valid business reason to be in the secure area" is accepted by the individual facilities, allowing access to the waterfront. That part of the process is more critical than the TWIC card itself, which is easy to obtain, yet totally unregulated and left to individual facility security officers. This TWIC Reader Rule does not address the true risk decision point.

The process for reporting inoperable readers to the USCG, and the associated waiver process, needs to be clarified. Are facilities allowed to switch methods, so as to not impede commerce, and then notify the U.S. Coast Guard? Or must commerce stop until the U.S. Coast Guard is notified and permission received to deviate from the TWIC Reader Rule? We suggest that facilities take prudent actions required to maintain their level of security, and simply notify the U.S. Coast Guard of the deviation within a set time frame (say 30 minutes). To pause, and await permission, will impact the movement of cargo.

The term "CDC in bulk" is used several times in the NPRM. According to 33CFR160.204, carried in bulk means "a commodity that is loaded or carried on board a vessel without containers or labels and received and handled without mark or count". We assume this is the same definition being used in the NPRM. As a large container facility, with several hundred CDC iso-tanks present in a fairly confined area at any given time, we would like to ensure that we are not handling "CDC in bulk". Request the definition being used in the NPRM be clarified in the final rule for vessel and facility grouping purposes.

As a facility that does not "handle CDC in bulk", are we allowed to provide a layberth for a vessel that carries CDC in bulk, but that we have no capability of handling? If the ship is in Group A, does the facility have to match that Group? Conversely, can a Cruise Ship Terminal (a Group A facility) act as a Group B layberth for a bulk ship when not operating as a Cruise Terminal?

The record-keeping requirement also requires clarification. As a Port Authority, we maintain the FSP for our cruise terminal. When a cruise ship is in port, the cruise line security operates under their own FSP. Who maintains the records? We

assume the Port Authority would continue to maintain the records and provide them to the U.S. Coast Guard should they desire to inspect the cruise line security operation. Request clarification in the rule making.

At a cruise terminal, porters are required to enter and exit the secure area up to 25 times a day each. With 35 porters (for example) working, that is hundreds of verifications in a single day. Please clarify the process for seeking relief from this apparently cumbersome process.

With the TWIC Reader Rule coming to fruition, the QTL should be expanded to include not just the authorized TWIC readers but also any supporting software, particularly for record-keeping requirements.

Mrs. MILLER. Thank you very much, all of you. Excuse me.

I think I am going to just start with you, Captain. I appreciate your testimony. I was taking a couple notes as you were talking, and what you just said at the end there, that someday this would be a much more comprehensive kind of a program that could be utilized intermodally for all the various types of transportation. Well, actually, that probably was the original vision, I think, of Congress with this program, but what has happened has become rather unrecognizable from what our original vision was, because—excuse me—you have got the airports that do their own thing now, really, and even on our highways and that, with hazardous material endorsements, the way that those are handled through the States as an add-on to a commercial driver license, et cetera.

You also mentioned that in your observation that the TWIC card currently is sort of a flash pass. It is something that we say here, a very expensive flash pass, and whether or not it actually works. Just listening to your testimony about how you have your own ID cards in the port of Houston, and most ports do, have their own—sort of a layered approach, I suppose, at all of these individual ports of what they have.

Let me just ask you. Do you think the TWIC is really a critical component of security at your port?

Captain WOODRING. The TWIC card gives me comfort that a background check or a threat assessment has been done against the terrorism database which I cannot do. That is at the macro level. As Admiral Servidio said, it is a piece of the process of the layers that come with it. We have two reasons for issuing our own Port of Houston Authority ID card. One is to validate that business reason for being on the docks, which speeds up commerce going through the gates. You don't have to check in the computer to see if they are on the list for today. I simply show them that, and it speeds commerce through. But that card also allows me to code that card with other things.

The TWIC card can be coded in our credentialing office to beep at the gate and do those kinds of things. Our Port of Houston Authority ID card can also be coded up to do other things. So we have split purposes. The TWIC card will get you into the restricted area. The port of Houston ID card has a flash pass, will show you a valid business reason, but it will also beep on the doors in the executive building and get us in there.

Mrs. MILLER. I see. Admiral, really, the proposed rulemaking for the reader really only includes the highest-risk facilities. Without going into details of what those all are, it has been the one-digit numerals apparently of what the high-risk facilities actually are.

So you still have—who are required to have a TWIC card, so you still have 90-some percent of those who needed a TWIC card. I am

just wondering, what is the rationale for requiring the entire universe of everyone to be having these TWIC cards if you are only—there is such a small percentage that you are really looking at.

Admiral SERVIDIO. Madam Chairwoman, we do see that the TWIC is an enabler for the future, in addition to allowing a migratory worker population to move between various facilities. As Captain Woodring said, the port of Houston is the port authority. When I was in St. Petersburg, there were about 80 different facilities, and over half of those were not part of that port authority terminal. So technically, you could have a worker that would need to have 30 to 40 to 80 different identification credentials to get around the port environment. It is a very different environment than an airport environment.

So having a single credential, I have seen how that has increased security in that the gate guards can look at one credential and try to figure out, what are the security measures on that card, and to verify it.

Also, we see biometrically that this is the direction we need to go. The Coast Guard has approximately 300 biometric hand-held readers that we use every time we do an inspection, either a regular inspection or a no-notice inspection. We know that there are 75 to 100 facilities that have already used the TWIC as their one access credential to that port. Some of them could potentially biometrically validate those people when they come in during high-risk.

We see—this is the direction that we need to have in the future, is a biometrically-enabled, risk-based methodology moving forward. At the present time, our cost-benefit analysis clearly identified for risk group A that the benefits far outweigh the costs, which are about $26 million, I think, annualized. We see in the future that there might be changes in cost, and we would expand that population.

Mrs. MILLER. Thank you, Admiral.

Just one other question, Mr. Sadler. I mentioned in my opening statement that last year we passed a SMART Port Act, where we are trying to assist the customer group, I suppose, and obviously security is the marquee issue always, so that they didn't have to go to more than one place to access the TWIC card. We gave the—we said that we needed to have that done, gave the Department 270 days, actually, I think in statute, but you were just mentioning that at this point you hope to have a pilot program or you will have a pilot program in Alaska next month.

I just mentioned that sort of like, what is the hold-up? I think you—the frustration that the Congress always has—although I have to tell you the truth that sort of what is happening—what you just testified to—is indicative of this entire program, it seems, during a number of years. So why is there such a lag in what the Congress's intent was and the application of that?

Mr. SADLER. Thank you, Chairwoman. We think that the One-Visit is the right way to go, and we appreciate Congress's direction on the One-Visit program. To put it in some context, currently we are transitioning one system, which I will call the legacy system, which was used to enroll TWIC workers, to a new system, a more

modernized system. That is going to allow us to roll an individual once and use that enrollment for multiple credentials.

So, for instance, if you get a person who is enrolling for a TWIC card or an HME background check, we will be able to enroll that person once. We will be able to use that background check for both of those programs. So when we looked at the 270-day time line, we determined that we would have to make significant changes, very costly changes to the legacy system that may or may not be able to be carried over to the modernized system. That was one of the first things that happened.

Then doing that, you would have to modify a number of contracts, as well, on the legacy side, as well as the contracts on the system for modernization. So when we looked at the overall risks and did our rough order of magnitudes for cost estimates, we determined that in order to get this right, because we obviously are fully aware of the work the GAO has done with us—and we appreciate their work, as well—in order to get this right and make such a significant change in the program, because this is one of the most significant changes we have made, we are going from two enrollments to one enrollment, we determined that the best course of action would be to implement a pilot, get some lessons learned, particularly in an area like Alaska, which is similar to Hawaii. You have an upper peninsula of Michigan. You have a lot of challenges for people traveling.

Let's do it in Alaska. Let's get some lessons learned. Let's start building those requirements into the new system and then take a—go to another location late this year or early calendar year of 2014, and then from there move into Nation-wide enrollment—or, excuse me, deployment, once we get the new system in place next spring. That was our thought process for this, ma'am.

Mrs. MILLER. Thank you. I appreciate that. At this time, I will recognize the Ranking Member.

Ms. JACKSON LEE. Thank you very much, Madam Chairwoman, and I think the testimony of all the witnesses have been contributing. Hearings by Members are to be part of problem-solving. So I would indicate to all the witnesses, and particularly to you, Admiral, that you are really working with the cards that you are dealt, and I appreciate you rising to the occasion to do the best that you can, but I am not comfortable that we are where we should be and that we are at our best.

I do, Captain Woodring, thank you very much, and it is good to get a personal notice of expiration, and so I will look forward to doing it again timely. Thanks for giving me the 60-day notice. It will be up to me now, after being told, to rush quickly to get it done.

But I want to—you said one—a number of things that I think are important that I would like to pursue. First of all, the enormity, the largeness of the size of the Houston port is a very good prototype because of the numbers of vehicles, Bayport, 19,000 vehicles, and I didn't hear whether it is 19,000 a week, a month. I didn't hear the number.

Captain WOODRING. Yes, ma'am, 19,000 vehicles per week at just the Bayport container terminal.

Ms. JACKSON LEE. I think—let me take a point of personal privilege to invite my colleagues and the Chair to join me for a site visit at the Houston port, Madam Chairwoman. I would love to host you there and the committee, as well. So that nod is on the record, and it was a nodding yes.

[Laughter.]

Mrs. MILLER. I would be delighted to do that.

Ms. JACKSON LEE. It is on the record now. Captain is writing it down.

But in any event, you said something about you having the ability to access the terrorist lists. Could you just expand on that, how important that is for you? Then could you expand on your renewal? You said the phone call was 2 hours. Frankly, I believe that is too long. Is there something we can do to expedite that?

Captain WOODRING. Yes, ma'am. First, on my renewal, when the cards first came out, I got my initial card. I was on the phone for about 3 hours, made the appointment, went to the TWIC center. They couldn't find my card initially, and I revealed who I was with the Coast Guard at the time, and they did another search in the back room and found it. So that was my——

Ms. JACKSON LEE. What center did you go to?

Captain WOODRING. I went to the one up by the Turning Basin, ma'am.

Ms. JACKSON LEE. Yes, thank you.

Captain WOODRING. You know the one. But that was 5 years ago. When I renewed this time for the 3-year extension, the phone call took me about an hour-and-a-half, and I understand they have now a web-based ability to do that, or at least I heard that in the testimony this morning. Then when I went, it was very easy. There were five of us at a long table, and they were able to activate all those cards simultaneously. So the process had greatly improved over time.

Ms. JACKSON LEE. But there was—and then, could you just expand quickly on the value of being able to access the terrorist list that the TWIC card provides?

Captain WOODRING. Yes, ma'am. I personally cannot run a—I can run a background check through our police department through different databases. I cannot access the terrorism database at the National level, and that is what the TWIC card brings to the table for me.

Ms. JACKSON LEE. So if we could—if we formulated something else that was more responsive, moved more quickly, but still gave access to the terrorist card, you could be open to that?

Captain WOODRING. I believe in the beginning there was some discussion of allowing law enforcement to somehow vet people against that list. I am not sure where that went, but we have the system we do today, and we appreciate the ability to have that.

Ms. JACKSON LEE. Yes, and I wouldn't offer the law enforcement. I would just say something more effective than where we are with the TWIC card. You would be open to it as long as we had—that whatever the new substitute would be would have access to that list?

Captain WOODRING. Absolutely, yes, ma'am.

Ms. JACKSON LEE. Let me go to Admiral and Mr. Sadler. I just want to have a pointed question. The GAO reported last month that not all TWIC reader cards underwent both the environmental and functional tests in a laboratory prior to use in the pilot. Instead, an initial evaluation was enhanced by TSA, and 30 TWIC card readers were approved for use by a pilot participant. However, none of the 30 readers underwent and passed all tests. Why were the readers deployed if they had not passed the proper test? What effect did this have on the pilot and the resulting data?

I am going to ask two questions back-to-back, because I want to get Mr. Lord, and your report is quite thought-provoking, if I might say. I do want to go back to your point about asking us to repeal a requirement, I guess, to rely upon the data and to go in another direction. If I am going to ask Mr. Sadler and then, Mr. Lord, would you follow with your recommendation, expand on that recommendation?

But, gentlemen, could you both answer that? Mr. Admiral, do you want to go first, or Mr. Sadler?

Mr. SADLER. I will go first, ma'am, because we were in charge of the pilot, and that was our responsibility. So as we started to move forward on the pilot, we did a number of tests on the readers that were available at the time. We did some initial tests in a lab. We did an environmental test. Then we did operational tests in the field prior to the implementation of the pilot program.

So all the readers that were put into the field passed an operational test prior to starting the pilot program at that particular location. The situation we got into was, because of the time it was taking to send all the readers and the cost—all the readers through these testings—or these different tests, we made a determination that we would do a test on a certain number of readers and then we would allow the other readers to be used in the marketplace. That is how we got to that decision, ma'am.

Ms. JACKSON LEE. That is how you got to some of the errors, because you tested some and didn't test others?

Mr. SADLER. I am not sure that is the reason, ma'am, because all the readers worked. They were operationally tested in the locations prior to the start of the pilot program. There were a number of different reasons that you couldn't get a read on the card. There may have been reader issues; there may have been card issues. One of the challenges that we had is it is difficult to get error information from these readers because they are not designed to do that. They are designed to facilitate access control decisions.

Ms. JACKSON LEE. Admiral, do you quickly want to have a comment so I can hear from Mr. Lord? Thank you for your service.

Admiral SERVIDIO. Thank you, Ranking Member. I would like to point out that, again, when the pilot first started, the systems are more robust than what they were at that time. We are looking to have a QTL, a qualified technology list, that would show that these readers have been tested and that they work properly.

Our NPRM is soliciting comments from industry specifically on whether this is a good rule or bad rule, and we have seen in the past that the comments we received will make a better rule than what we initially proposed. We intentionally have not included some of those high-throughput facilities, like container terminals or

row-row terminals, because we feel that we will get better data initially from the cost-benefit analysis and how we are proposing the NPRM.

Ms. JACKSON LEE. Mr. Lord.

Mr. LORD. Did you want me to respond to the recommendation to de-link those two events? Well, obviously, we found some limitations in the pilot, and TSA and the Coast Guard were directed to use the pilot to help develop the rule. Given the importance of the rule, we believe some of the limitations we noted we are suggesting, well, they should be relieved of that requirement.

Ms. JACKSON LEE. So what should they base the rule on?

Mr. LORD. Well, as the agencies noted in the rule, they used other sources of information to inform the rulemaking. Obviously, that is not the only source of information, although we view it as a key source, but just to ensure the integrity of the process, if the data is no good, we don't believe people should be asked to use it.

Ms. JACKSON LEE. Thank you, Madam Chairwoman. I yield back.

Mrs. MILLER. At this time, the Chairwoman recognizes the gentleman from South Carolina, Mr. Duncan.

Mr. DUNCAN. Thank you, Madam Chairwoman.

First off, let me just say that, after 11 years, this program should be a lot further along than it is. I was reading some of the notes, and it said there are disqualifying factors that can be waived with proper authority, and they include transportation security crimes, improper transportation of hazardous material, unlawful handling of explosive devices, murder, any threat or purposely false information concerning an explosive device in a public or Government facility. That is abysmal, the fact that we are going to waive entry for folks that have committed those type of crimes. So that needs to be addressed, and that is not where I am going to go today, but I would throw that out there for future hearings and conversation.

I was contacted by a constituent from South Carolina, and I would just like to read some of his e-mail to me, because he is a contractor providing some of the hand-held scanners, I think, that the admiral talked about. But he said just yesterday, he spent nearly half-an-hour on the phone with the vice president of SSA, one of the Nation's largest container terminal operators. During that conversation, he told me that TWIC was dead and suggested I look for another market. We have had a team of consultants that work for us in the Texas market, and they are hearing much the same thing from many of their contacts. This was on June 5.

He said that the notice of proposed rulemaking is under the comment period, which will close the 20th of this month. The NPRM was very disappointing, as it only requires Class A facilities to electronically validated TWIC cards and biometrically identify the holder. All Class B and Class C facilities will be allowed to continue to use the TWIC as a flash pass.

Even though this was never the intent, I have spent the last several months on ports and private terminal operators' location and can tell you that the word flash really is the appropriate term. The drivers never take their TWIC out of its plastic protective case, which is typically on a lanyard around their neck, and hold it up for a security guard to see.

For the most part, the name is not even readable from the distance they are viewing it from, certainly not the expiration date. My understanding of the current role and the new NPRM is that it is the responsibility of the security staff to accomplish three things when allowing a visitor on the port facility. One is to get the authenticity of the TWIC. The second is to verify the expiration date. The third is to positively identify the holder by comparing the picture on the TWIC with the face of the individual presenting the TWIC.

This process should take approximately 15 to 20 seconds if it is done correctly. We all experience similar things at TSA, as we see airline personnel and TSA personnel and other clear people go through TSA screening. However, this is never done. In addition, we spend the time and money to publish a CCL so that we make sure we are not allowing an individual on the ports that has caused their name and number to be placed on the list. However, no Class B or Class C port or private terminal facility has the ability to check against a certain list. I think we heard some of that earlier.

Even if such a list were made available to them, it would disrupt the entire operation and to take the necessary time to check the list. No one seems to be able to publish a document that clearly states that TWIC is not dead, but moving forward.

It is concerning to me that I am hearing from someone and from my State that is involved. This is real life. This was an e-mail. I didn't make this up. So this is the real-life example of where we are failing America in this process of making sure that our port facilities are safe.

I agree with the admiral. I think we can have the hand-held scanners that you are using. I think that is a very verifiable way to identify and make sure that that cardholder is holding a valid TWIC, that it is that person that is holding it, it is not fraudulent, and it doesn't take that long to validate that.

Now, I know there are costs involved. But I would be willing to bet that over the past 11 years, the money that has been spent developing this program that is so far behind schedule that we could have probably paid for those type items.

So the question I have for the witnesses is: Do you believe that the TWIC program is dead? Or should it be continued? When do you believe we will see some clarity on that issue? I will just start and go down the list. Admiral?

Admiral SERVIDIO. Thank you, sir, and thank you for the question. I strongly feel that TWIC is not dead. We, the Coast Guard, see great value in having a single credential with the background and the biometrically enabled. I think what is important is not just to look at the past, but to look at the future, and we do need something in the environment we are going to be going in that will allow real-time biometric enabling to verify a person is who they are when they are going in there.

Mr. DUNCAN. I agree with you. Thank you.

I will go down the list. Is TWIC dead? Should it continue? When do you think we will see some clarity?

Mr. SADLER. TWIC is not dead. It should continue. I think we will see some clarity when the Coast Guard finishes getting its comments for the NPRM and adjudicates those comments and

comes out with a good reader rule, because that is the key to this. The TWIC card is one element in the process. The reader is the key to using that card.

Mr. DUNCAN. Do you agree with me that it is being used as a flash pass now, Class B and Class C terminals?

Mr. SADLER. Currently, in many terminals, it is being used as a flash pass. That is why the reader rule is so important to get the readers out there.

Mr. DUNCAN. Let's go down the list. Is it dead? Or should it continue? Some clarity?

Mr. LORD. Obviously, it is not dead. It is—I think we need to rethink the approach, perhaps focus on more higher—use at higher-risk facilities, more selective use. That would help address some of the issues we have identified in our past work, but, again, that is up for Congress.

Mr. DUNCAN. You are a class A terminal in Houston?

Captain WOODRING. Right now, we are not classified, because the NPRM is what groups you or classifies you right now. We currently use the card as a flash pass.

Mr. DUNCAN. Flash pass?

Captain WOODRING. In the new rule, we would be a Group B, which means we would not have to have the biometrics unless the MARSEC level changed, in which case we would have to biometrically check.

Mr. DUNCAN. Thank you, gentlemen. My time is up. I will yield back.

Mrs. MILLER. The Chairwoman now recognizes the gentleman from Texas, Mr. O'Rourke.

Mr. O'ROURKE. Thank you, Madam Chairwoman.

I wanted to start with a statement that I believe I heard Mr. Lord make, which is that you were unable to determine how using TWIC has improved security. I just want to make sure I heard you correctly.

Mr. LORD. Yes, the assumption is—and I know the Coast Guard and TSA strongly believe that is the case—but we—in terms of an analytical perspective or analysis, we have yet to see anything comparing TWIC before and after. That is what we essentially were asked—calling for in our so-called effectiveness study back in 2011.

So the presumption is it would enhance security, but don't forget, a lot of these facilities already have access control systems in place. They are already using local credentials, as the gentleman to my left just explained, so we would like to—I guess we are slightly skeptical and just need to see the analysis, and that is why we made that recommendation in 2011.

Mr. O'ROURKE. You know, I think it is important for us to move forward with objective, verifiable data. If we have spent—as I understand it—more than $500 million so far on this program that we know, it is objective, hard data, if we are going to be asked to spend anywhere from $700 million to more than $3 billion going forward in the future, I think we need to know how and to what degree this improves security.

So because the GAO and Mr. Lord were not able to determine that from the information that you provided, Admiral or Mr. Sadler, do you have anything that you could add now at this hear-

ing that would give us some comfort in moving forward with this program?

Admiral SERVIDIO. Yes, sir. The Coast Guard does an assessment every year—at minimum annually—through what we call the MSRAM, which is the Maritime Security Risk Assessment Model, and we take a look at the whole—all of the components of port security. Access control is part of it, and TWIC is just part of that access control. So doing an assessment on just a subcomponent of one of the components is quite difficult at this time. We do agree that we should be doing assessments, we should have better measures. We feel that when there is a reader rule out there, we can look at the effectiveness of having those biometrics and other types of things. We are looking internally in how we are using the hand-held readers and what the effectiveness of using those hand-held readers are to biometrically verify people.

Mr. O'ROURKE. But without any data, without you being able to give me hard numbers, how could I support authorizing another dime for this program? If we do authorize another dime, how do we decide whether it is $3 billion or $10 billion or $1 trillion if you are not going to give us any reliable cost-benefit analysis to this?

We don't have unlimited money to spend on security, and we have some troubling lack of evidence as to whether or not this is improved security at all so far, and yet we are being asked to spend more and perhaps expand this to other modes of transportation and other frontiers in National security.

I also heard Mr. Lord say that in the data that you made available, throughput times were mixed up with reader response times. That is of particular concern to me in El Paso, Texas, a big trade corridor, more than $90 billion in U.S.-Mexico trade moving through there. If we slow down already long wait times even further, with a system that doesn't work or with a system whose effect on throughput we cannot ascertain, that to me is troubling, as well.

Do you have a response to the statement he made about throughput times?

Admiral SERVIDIO. Okay, sir, if I could answer the first part with regards to the assessment, I guess there are two different answers. I can give you hard numbers on how we have reduced risks in our ports using the MSRAM data each and every year as a result of the actions we have taken in implementing the Maritime Transportation Security Act and the international ship and port facility security code.

We do have numbers saying that we have reduced vulnerabilities and we have reduced risks in our ports. Anecdotally, I have been the captain of the port at three different locations, sir, and I can tell you that we have come a long way in accepting any credential and what the guards would look at to where we are today in TWIC. Are we where we need to be? No, sir, but I think we are moving in that right direction.

Mr. O'ROURKE. Was it worth $500 million? Is it worth an additional $3.2 billion, what you have seen so far? If you can't give us the numbers here, can you tell us in your best judgment whether that is good value for the taxpayer?

Admiral SERVIDIO. I can you tell, sir, that our NPRM has an annualized cost of $26 million for the implementation of TWIC

readers at Group A facilities. That is a good investment in money, sir. As we end up maturing the technology, I believe that we will be able to justify why we should roll this out to Group B facilities and potentially to other facilities, sir.

Mr. SADLER. Yes, sir, I would like to add a couple of things. On the transaction times, that was our responsibility in the reader pilot. We made a determination as we were going through the pilot to use transaction times from the card itself, because we were having difficulty collecting the information on throughput times through these access points. That is one of the challenges that we faced.

So if you think about throughput, whether it is a pedestrian coming up to a gate and presenting the card, or whether it is a truck coming up to a gate and presenting a card, it got to the point that if a truck comes up to the gate, for instance, and the individual has the card on a lanyard and has to back up or move closer to the reader, is that part of the throughput time that is affected by the TWIC?

For us, that throughput time would be standard, no matter who was going through that gate. For us, we were concerned with the transaction time of the card. When the person actually put the card up to the reader, put the fingerprint down or finger down to check the fingerprint, and collect that transaction time, because that was going to determine, you know, how we affected the actual throughput of an individual or a vehicle.

On the card itself—and as far as security is concerned—we believe that the card does improve security. Having gone through ports and facilities for over 20 years myself, I know that you can get through gates or used to be able to get through gates with multiple credentials. I never had to go through a gate with one common credential. I never had to go through a gate with a biometric credential.

I don't think there was a background check at that time. We have got a standard background check. We have got an adjudication process. There are a lot of things that we have done with this card that were never done before in this maritime environment.

Then last thing, if I could just finish, sir, on the cost estimate, the numbers you are referring to, the $3.2 billion, that is our lifecycle cost estimate for the program through a 10-year estimate. We did that, if I remember correctly, in 2007–2008. I would have to check that number.

So to date, we have spent $394 million on the program—this is in the GAO report—approximately $100 million on appropriations, and $294 million in fees, because it is a fee-funded program.

Mr. O'ROURKE. Madam Chairwoman, I know my time is up. I just want to say that I appreciate your belief that this makes us more secure. The concept is a good one. But we need facts if we are to make informed decisions going forward. Thank you.

Mrs. MILLER. Thank you.

The Chairwoman now recognizes the gentleman from Utah, Mr. Stewart.

Mr. STEWART. Thank you, Madam Chairwoman.

To the witnesses, thank you all. Thanks for your service. Thanks for your expertise and being with us today. I know that you have

a difficult task. The challenges confronting us as a Nation and as a people that you have been involved with over the last 10 or 12 years are in some cases enormous, and we appreciate that.

I think one thing that—an observation, if I could—and I would like to keep my comments and then my specific questions to you very big picture—being kind of new to this, I was a military officer for 14 years. I understand some of the security concerns. I also understand a little bit about how Government bureaucracies work.

I think one of the things—an observation that many of us would agree with, and that is that Government sometimes creates bad legislation when that legislation is created in a time of perceived crisis. When there is a great urgency like we experienced after 9/11 and there was this cry to do something, and we did something, and some of that has been very effective and very important, but some of it has been less so, because it was perhaps not as thoughtful as we would have done had we not been under this—again, this sense of urgency, this sense of crisis.

There were many who warned at the creation of the Department that it would become a big bureaucracy, that it would become unyielding and unresponsive to some of the needs of the people. I think that that is a fair observation. I think—I don't know anyone who would disagree with that, that like any Government agency, that there are some issues with the Department of Homeland Security that could be made better. I think, frankly, this is a pretty good example of that. What the Department has done is good, and there are many great success stories, but, again, I think that there is criticism there that we can take and probably try to apply.

Again, I think the TWIC program is—as you have indicated, I think all of you—and as has been indicated in the questions—it has been troubled from the very beginning. Since its initiation in 2002, DHS has failed to meet every time requirement, essentially. We are, what, 5 years behind what our goal was and where we wanted to be?

So, Mr. Sadler, maybe I will ask you, but then, Admiral, I would like to come to you, as well. Help me understand the big picture. If you can, answer this question not in a couple paragraphs, but answer it in a sentence or two sentences, if you will. What is the greatest challenge we have had? What is the one thing that we can—you know, that you would say this is the problem or this is the most important problem, and then how do we fix that one problem?

Mr. Sadler.

Mr. SADLER. Well, thank you, sir. This is important to understand, so I can put some context around it. We started with nothing in the beginning of the program. So what I mean by that is, there was no common credential. There was no common background check. There was no adjudication process. There was no appeals process or waiver process or administrative law judge review. There was no waiver process. There were no disqualifiers. I will try and keep my answer short, but this is very important. When we started this program, the program as it exists today did not exist then.

Mr. STEWART. So then are you alluding that that is the great challenge, because we started from zero?

Mr. SADLER. I think that is one of the challenges. That is a challenge, because we had to design all these things to get to this point. Another challenge is that we are taking this security and we are applying it across the maritime environment. I know Captain Woodring or Admiral Servidio would say, if you have seen one port, you have seen one port. There are different throughputs. There are trucks. There are vehicles. There are pedestrians. There are service workers. There are tremendous challenges in this program.

Mr. STEWART. Okay.

Mr. SADLER. So I think that is the answer. I think we had to design something that didn't exist. Although there were other cards and credentials and programs out there, it didn't exist in the maritime environment, and just the maritime environment itself is very challenging.

Mr. STEWART. Okay, and I appreciate that, and I know you are not trying to evade the question or the answer, but when you say it is difficult and we had to start from zero, it has still been a long time, and we have still spent a lot of money. I am not sure any of us are satisfied with the result of where we are now.

I was hoping that you would be able to say—and maybe you can't—I was hoping you would be able to say, this is the challenge we have. This is the one thing that if we did this or these two things, if we did this, this would be better, this would be—we would be able to make progress now. We wouldn't get this sense that we are just kind of spinning our wheels. Admiral, do you have any comments on this? Can you help me understand, you know, the one or two things that we could fix that would help this process?

Admiral SERVIDIO. Yes, sir. I believe the two issues are, we have one single credential now, one background credential, the TWIC card, and getting the socialization of that concept, getting the implementation of that has been a challenge. But we have done that.

I think the greatest concern going forward is customer service, and I think we need to decouple customer service issues to trips and other types of issues, being on the phone for 3 hours or 2 hours, from the value in having a single credential with a common background and making it easier for our ports to implement.

I really think we have made progress on going to the single credential. I think we still have work to do on the customer service, and we are working actively with TSA and the Department on addressing those concerns.

Mr. STEWART. All right. Thank you. I am out of time, Madam Chairwoman.

Mrs. MILLER. I thank the gentleman very much.

The Chairwoman now recognizes the gentlelady from Hawaii, Ms. Gabbard.

Ms. GABBARD. Thank you, Madam Chairwoman.

Thank you, gentlemen, for your time, your service, and your work here. Like my colleagues, of course, we are concerned about—at the bottom line, how are we addressing potential threats and alleviating threats that we see today, as well as going forward along our borders and at our maritime ports?

As you can imagine in Hawaii, this is something that is particularly of interest to us, as we receive close to 95 percent of all of our goods coming through our ports. I have a few questions regard-

ing the actual TWIC card. I know you have said that this is just one component of the overall maritime security plan, but looking at the level of threat that we see coming through our containers, coming through the cargo that is coming in, I am curious about how many either specifically or a ballpark figure, maritime figures you have found using this National terrorism database—have found to be on that list?

Mr. SADLER. Well, ma'am, if I could speak to you outside of public forum, I would be happy to give you those numbers, but I am just not comfortable discussing it in this forum.

Ms. GABBARD. Have you seen that this is a prevalent issue?

Mr. SADLER. It is an issue, but, frankly, I would like to discuss it outside of the open forum.

Ms. GABBARD. The reason I ask is because I have had conversations with many of our maritime workers that I have seen in our States. I have visited our various harbors and ports and have seen, more often than not, frustration at a basic level of dysfunction. Not only—you have talked about the readers and the other issues that have been there, but with folks who have been working at our ports for 12, 15, even 20 years, erroneously being flagged as they go through the screening process and then are put out of work for 1 month, 6 months, 8 months, which creates a tremendous hardship on their families and our workers, and to have to undergo this screening not only on an annual basis, you are saying that there is a 3-year plan now that people can apply for, but also the hardship, as we see in Hawaii, of having to travel to the mainland for this screening.

How do you reduce these erroneous disqualifications that are occurring?

Mr. SADLER. Well, we are required to adjudicate the backgrounds against certain disqualifying criminal issues. There are approximately 27 crimes that we look at. Some of them we look back for an unlimited period of time. Some are 5 years from conviction or 7 years from a release from incarceration. That is a statutory requirement.

So one of the things that we do is, we have a robust appeals, waivers, and review process, and as soon as an individual is flagged for having some type of issue, we immediately get a letter out to that person once we have identified that person or that issue, and then we try and get them into this review process, so we can clear up whatever that issue is.

One of the challenges that we have with that type of background check is, the States need to upload their information into the database that we use from the FBI, all right? At this point, we are getting State records from approximately 40 States. They may be more complete than the Federal database. They may not be. They may be more extensive. If we got the records from all the States, that would help us a lot.

It—I am sorry. What were your other questions, ma'am? Oh, on the travel. So, for instance, on the travel, we are doing a couple of things. We are increasing our enrollment sites from 136 to over 300, so if you have a TWIC enrollment site or a hazardous material enrollment site, you will be able to apply for both of those back-

ground checks at the same place, and you can get a discount on the background check if you choose to get both of them.

We are also extending the One-Visit pilot program to Nationwide in 2014, which will only require one visit for all individuals. Then currently, we have the extended expiration date TWIC, the 3-year card, that only requires one visit. So we are taking positive steps to try and reduce that burden, whether it is through an adjudication process or whether it is through the actual visits to an enrollment center.

Ms. GABBARD. Admiral, maybe you could answer this question. How does this background check that our maritime workers are undergoing compare to a background check that a brand-new enlistee in the uniformed services undergoes? I am not talking about a secret clearance. I am just talking about walking in the door.

Admiral SERVIDIO. I am not sure exactly what background check we do when someone comes in, so I am going to have to get back to you on the record. I can tell you that the background check we do for TWIC is different than what we require for a merchant mariner, because of just the interaction with the public and other types of things. So we do tailor some of those background checks to what we are looking for with that part of the industry.

Ms. GABBARD. The reason I ask is because I am wondering if in some ways you are saying we are starting from ground zero, there has been nothing like this put in place before, but when you look at our U.S. military, for example, I know some of the branches have different and higher levels of requirement, but at a baseline level, you have a criminal background check much like the States already provide at the local level.

Without a secret clearance, that is kind of it. There are different requirements there that they are undergone, but you have an ID card with the biometric system that is accessible at military bases around the world, that it is rugged, it is supposed to be durable, and it seems like this is a system that has already been in place and it has worked, and I am not sure why we are investing in something that has now already been done.

Mr. SADLER. Well, our credential—the TWIC card is accepted at DOD facilities. It is—the basic card is the same card as the CAC card, the DOD card. It is a card that we get from the GSA schedule. So it is tested to the same standards, and we believe it probably has about the same failure rate, because it has similar use.

I think the main difference outside of the card itself is the fact that this is a commercial environment, it is all about high volume and throughput and speed. So that is where our challenge comes in, but the card itself is the same card stock that any Federal agency would buy off the GSA schedule.

Ms. GABBARD. Thank you very much. Thank you, Madam Chairwoman.

Mrs. MILLER. I thank the gentlelady.

I certainly thank all the witnesses. You can see by the level of frustration, some of the questions that we are asking, I am sure you all share that. We will see what happens here with this TWIC card, but it is a very important issue. We appreciate all of your attendance here today.

Ms. JACKSON LEE. Madam Chairwoman——

Mrs. MILLER. I would—yes, the Ranking Member?

Ms. JACKSON LEE. Yes, before we end, might I ask to put in the record three things? One, the letter from the American Association of Port Authorities on this very issue, I ask unanimous consent.

Mrs. MILLER. Without objection.

[The information follows:]

LETTER FROM THE AMERICAN ASSOCIATION OF PORT AUTHORITIES

JUNE 13, 2013.

U.S. Department of Transportation,
Docket Management Facility (M–30), West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue, S.E., Washington, DC 20590.

RE: Comments of the American Association of Port Authorities on the NPRM, Transportation Worker Identification Credential (TWIC) Reader Requirements Docket: USCG–2007–28915.

DEAR SIR/MADAM: Seaports deliver prosperity by serving as critical links for access to the global marketplace. Safe and secure seaport facilities are fundamental to both protecting our borders and moving goods. The American Association of Port Authorities (AAPA), on behalf of its U.S. members, welcomes this opportunity to comment on the Coast Guard's (USCG) Notice of Proposed Rulemaking (NPRM) related to the Transportation Worker Identification Credential (TWIC) Reader Requirements. Our U.S. members handle containers, auto and ro/ro cargo, cruise passengers, as well as many bulk and breakbulk cargos, all of which would be impacted by this rule.

While the comments below address specific issues raised in the NPRM, AAPA is concerned about the findings in the recent Government Accountability Office (GAO) May 8, 2013 report, *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed* GAO–13–198. GAO recommended that Congress halt DHS's efforts to promulgate a final regulation until the successful completion of a security assessment of the effectiveness of using TWIC readers. While we understand that there may be some disagreements over these findings, we do ask the Department to consider delaying the implementation date of the rule, and we stand ready to assist in further analysis of TWIC reader operational problems identified in the report.

Below are specific recommendations related to the NPRM.

In the final rule, USCG should be more specific in defining what are considered TIER A, B, and C facilities and utilize a risk-based approach to reader requirements that more clearly addresses the particular circumstances of each port area and the facilities that fall within the category requiring readers.

As noted in AAPA's May 13, 2009, comments on the TWIC rule, we support the Maritime Transportation Security Act (MTSA) regulatory system that is performance- and risk-based. Unlike earlier TWIC proposals, the NPRM proposes a risk-based approach. While this is an improvement from the previous proposal, we do not believe the system as proposed should be adopted. We are concerned that the three categories for TWIC reader use are based upon the passenger capacity of vessels, bulk of hazardous material, and the facilities that they use, rather than taking an approach that is more specific to the individual circumstances of each facility. (It is unclear, for example, how Strategic Ports will be classified based on the criteria listed.)

AAPA recommends that USCG expand the risk-based concept and include a more performance-based and flexible system as reflected in other MTSA regulations. Every port is different and in making evaluations about risk, USCG should aggregate risks to the port area first, followed by a second layer of risk at the facility level using a Maritime Security Risk Analysis Model (MSRAM), including an evaluation of what other facilities are in close proximity. This would result in a flexible, but risk-based system. Therefore, a facility's risk and associated reader requirements should be based on a variety of risk factors, not just what type of vessels call on it or the type of cargo that it handles.

At certain facilities, TWIC should be checked by electronic reader at the beginning of a shift but then afterward and for the duration of the shift employees should be able to walk into and out of the secure area only having to flash their card or show some other identification to the guard. At cruise terminals, for example, porters walk into and out of the secure area 25–30 times during their shifts. Having to stop and use the reader every time that movement into the secure area is made could well create an unnecessary burden, delay work, impact vessel schedule, and result

in unnecessary expenses. While it is true that, according to the NPRM, the Captain of the Port (COTP) has the power to suspend the reader requirement if it is unduly holding up cargo or passenger processing, this particular exception to the rule should be codified before the fact and not reliant upon an after-the-fact assessment. Differing assessments by individual COTP's could inequitably impact inter-port competitiveness.

According to the NPRM, the Captain of the Port is authorized to suspend the reader requirement in the event that a reader malfunctions or some other event transpires that makes the reader requirement unduly onerous. AAPA recommends that in the event of a minor occurrence, such as a reader malfunction, the port should immediately be able to continue to process workers using an alternative means that has previously been identified in the approved Facility Security Plan. Rather than being required to contact USCG for approval to resort to the previously-approved alternate plan, the port should be able to resort to the plan and then log the occurrence for review by USCG after the fact. USCG will be able to monitor how frequently or infrequently the alternate plan is used and address irregularities without holding up the process at the time.

The NPRM requires that ports submit an updated Facility Security Plan describing what procedures will be used to comply with the new reader requirement, once it goes into effect. AAPA recommends that ports be permitted to submit TWIC updates within the 5-year plan resubmission, rather than be required to submit immediate amendments to already-existing security plans.

Sincerely yours,

KURT J. NAGLE,
President and CEO.

Ms. JACKSON LEE. A letter from the American—excuse me, statement from the American Trucking Association on this issue.

Mrs. MILLER. Without objection.

[The information follows:]

STATEMENT OF AMERICAN TRUCKING ASSOCIATIONS, INC.

JUNE 18, 2013

INTRODUCTION

The American Trucking Associations (ATA), founded in 1933, is the Nation's preeminent organization representing the interests of the U.S. trucking industry. Directly and through its affiliated organizations, ATA encompasses over 37,000 companies and every type and class of motor carrier operation.

The trucking industry is an integral component of our Nation's economy, transporting more than 80% of our Nation's freight bill and employing approximately 7 million workers in trucking-related jobs, including over 3 million commercial drivers. It is important to note that the trucking industry is comprised primarily of small businesses, with 97% of trucking companies operating 20 trucks or less, and 90% operating six trucks or less.[1] More importantly, about 80 percent of all U.S. communities depend solely on trucks to deliver and supply their essential commodities.

BACKGROUND

As ATA has testified on several occasions at Congressional hearings, including before the House Homeland Security Committee, both the private sector and Government agencies continue to struggle to find the right balance between improving security while facilitating commerce throughout our Nation's transportation sector. The motor carrier industry believes that security and commerce are not mutually exclusive goals throughout the transportation system and the increasingly sophisticated supply chains that move global trade. To truly enhance security without disrupting the flow of commerce, security regulations and programs must be implemented in a cost-effective and coordinated manner. A key goal of such an effort must be that individual programs should be designed in a way that they can be leveraged to comply with a multiplicity of regulations and security requirements. The trucking industry believes that the Transportation Worker Identification Credential (TWIC) can be such a program if implemented and utilized in an appropriate manner.

[1] American Trucking Associations, *American Trucking Trends 2011* (March 2011).

ATA has long supported the original concept of the TWIC: One application/enrollment process, one fee, one security threat assessment (STA), and a single credential that transportation workers may utilize to demonstrate compliance with multiple security requirements. However, commercial drivers today continue to face multiple security credentialing requirements. For example, in addition to the TWIC, drivers must undergo separate STAs for the Hazardous Materials Endorsement (HME), the Free and Secure Trade (FAST) program for border crossings, to name a few. The cost to drivers and companies of these separate STAs and credentialing programs is almost $300 in fees alone, not including the costs associated with drivers' lost wages and fuel costs while traveling to and from multiple enrollment centers, and the aggravation of providing fingerprints multiple times for each program that performs the same background check.

Over 10 years ago, Admiral James Loy, then the second-most senior official at the Transportation Security Administration) TSA, summed up the concept and the purpose of the TWIC, stating:

"A fourth initiative also underway is development of a Transportation Worker Identification Credential or TWIC . . . The idea is to have these [transportation] employees undergo only one standard criminal background investigation . . . I've heard that there are some truck drivers currently carrying up to 23 ID cards around their necks. I wouldn't want to pay that chiropractor bill. Under the TWIC program drivers and other transportation workers will only have one card to deal with which would be acceptable across the United States.[2]

Unfortunately, the TWIC program/concept has not lived up fully to its promise and has become another expensive, duplicative security credential that truck drivers must obtain to access maritime facilities. TWIC works, but the goal of universal acceptance of a single security credential has yet to be implemented by TSA. It is not too late to enhance TWIC's capabilities and acceptance across multiple programs to improve its benefits and reduce the need for multiple screenings through the same databases. In essence, implement the long-established Department of Homeland Security principle of "enroll once, use many."

TWIC CHALLENGES AND OPPORTUNITIES

The TWIC program has had to confront strong criticism since it was first proposed in an NPRM in 2006 implementing statutory requirements mandated under the Maritime Transportation Security Act of 2002. Some of the key criticisms that the TWIC has encountered include:

- The excessively high cost of the TWIC: $132.50 (reduced to $129.50 in 2012);
- The extended time the application process requires of applicants, taking time off work twice: Once to apply and provide the biometrics, a second visit to pick up the credential;
- The failure to expand TWIC's utilization to satisfy other Federal STA regulatory requirements, including sister programs within TSA;
- The lack of TWIC enrollment facilities Nation-wide to facilitate the enrollment of transportation workers who live far from either coast;
- The failure to implement TWIC with its essential counterpart reader rule, annulling the credential's technology benefits and serving only as an expensive "flash-pass".

ATA generally agrees with these criticisms of the TWIC program and we have expressed such concerns in past testimony before Congressional Committees as well as in comments to TSA, The United States Coast Guard (USCG), and the Department of Homeland Security (DHS). However, our greatest concern at this point is the multiplicity of background checks, and their associated costs and burdens, which drivers undergo to perform their everyday work responsibilities, from transporting hazardous materials and delivering at maritime facilities, to crossing our international land borders and transporting air cargo.

As a matter of policy, ATA has long supported a system and process that provides for a Criminal History Records Check through National databases. But today's state of affairs in which commercial drivers undergo multiple STAs is untenable, excessively burdensome, and patently inefficient. Because of this, ATA has taken the position to support the TWIC as the potential single credential and STA that can demonstrate and provide compliance with multiple programs and regulations that re-

[2] Remarks of Admiral James M. Loy, Under Secretary of Transportation for Security, Transportation Security Administration, during Transportation Research Board 82nd Annual Meeting Chairman's Luncheon, January 15, 2003.

quire a STA through a single enrollment, a single fee, a single background check and a single credential.

Although TSA has not provided for full recognition of one STA for compliance with another regulatory STA, for example allowing TWIC holders seeking an HME to show their TWIC as proof of already having an equivalent STA—a policy supported statutorily by Section 1556 of the 9/11 Commission Act—other Federal agencies are accepting the TWIC for compliance with their credentialing requirements. For example, the Department of Defense (DoD) has an established policy allowing commercial drivers transporting freight in and out of appropriate military facilities to use a TWIC in lieu of obtaining a DoD issued Common Access Card (CAC). DoD acceptance of the TWIC for such purposes is recognition of the strength of the TWIC STA process and its compliance with Federal Personal Identity Verification (PIV) standards used by millions of Federal employees.

In its latest report regarding the TWIC card reader pilot results,[3] the U.S. Government Accountability Office (GAO) criticized TSA's planning shortfalls for implementing the TWIC reader pilot in a manner that did not yield usable information due to data-collection challenges. ATA is aware that TSA faced some technology challenges in collecting TWIC-reader functionality data, including that the first generation of TWIC cards had faulty antennas embedded in the cards which rendered them useless when utilized with contactless readers. However, ATA is also aware of certain facilities that have been using the TWIC readers successfully to verify the credential's status, identity, and improving throughput for truck operations. Perhaps additional focus should be given to facilities that have successfully implemented the TWIC readers and utilize such "lessons-learned" that can be applied to other facilities facing reader challenges.

GAO's concerns and suggestions should be given careful consideration by DHS in improving the development and implementation of TWIC-readers at regulated facilities. ATA also agrees that Congress should continue to carefully assess the overall implementation of the TWIC program. However, ATA is concerned with GAO's suggestion that Congress consider "alternative credentialing approaches, which might include a more decentralized approach for achieving TWIC program goals." A decentralized approach could result in an environment in which each State or location performs STAs and issues separate credentials for truck drivers to access maritime facilities throughout the country. Such a scenario would result in an increasingly burdensome, inefficient, and ineffective system for transportation workers who work and operate at multiple MTSA-regulated facilities. The TWIC is a robust, Nationwide and uniform STA that can be utilized at multiple locations when matched with the appropriate readers. TSA and USCG need to focus their efforts in ensuring the deployment of TWIC readers nationwide rather than creating a vast assortment of individual systems.

With the appropriate leadership within TSA and with clear guidance from Congress, the TWIC has the potential to serve as a valuable tool to ensure that personnel working throughout our country's critical transportation infrastructure have been screened appropriately and continue to be vetted frequently through relevant databases. Moreover, when the credential is utilized with the appropriate readers it can ensure the validity of the card, match the TWIC to the cardholder and allow for improved throughput when entering secure areas requiring such systems.

CONCLUSION

Notwithstanding that the TWIC continues to face several challenges to gain broad support from various sectors within Government—as demonstrated by the latest GAO TWIC report—as well as private-sector entities, the TWIC's future utility is robust if implemented as originally intended by leveraging its applicability throughout other security programs. But appropriate efforts and policies must be implemented by DHS, TSA, USCG, and other Federal entities to coordinate the utility of such a PIV for compliance with multiple STA requirements. The 2.4 million transportation workers in possession of a TWIC, including over 400,000 commercial drivers, are already heavily invested in the program. It would be a disservice to these workers to consider doing away with the TWIC when they have spent resources and time to obtain the credential.

ATA urges the Homeland Security Committee and its various relevant subcommittees to:

---

[3] U.S. Government Accountability Office; *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to be Reassessed;* May 2013.

- Continue supporting the TWIC as a viable STA program used by millions of personnel to access secure areas of maritime facilities as well as various Federal facilities;
- Authorize and mandate the use of the TWIC for compliance with equivalent STA programs;
- Analyze and require TSA to significantly reduce the high cost of the TWIC and ensure ample geographic coverage of enrollment centers;
- Not overlook the fact that the TWIC, as a stand-alone credential, provides a solid STA component and a perpetual vetting process that offers a high degree of security;
- Allow the USCG to move forward with the implementation of the TWIC readers, after careful consideration of industry comments and recommendations.

The implementation of the TWIC readers is essential to leverage properly the technology embedded in the TWIC and to establish uniform, secure, and efficient access procedures at secure areas of MTSA-regulated facilities. Even with the very high cost of the TWIC, at roughly $130.00, it is a more cost-efficient scenario rather than paying multiple fees and undergoing multiple enrollment and finger-printing processes. The trucking industry asks that these costs be reasonable and part of an efficient, risk-based process. ATA supports an approach that is good for security—and good for commerce.

ATA appreciates the opportunity to offer this written statement and we look forward to continue working with this subcommittee and the Homeland Security Committee to further improve the security of our transportation system, doing so in a coordinated and efficient manner.

Ms. JACKSON LEE. For the record, a question to the Coast Guard and TSA to provide us in writing whether you have the tools to assess and evaluate the effectiveness of using the TWIC with readers for enhancing port security. I think we need a—I need a focus one, two, three, four, in relation to the GAO report in 2011 and 2013.

I thank the Chairwoman, and I think this has been a very helpful hearing from all of the witnesses and look forward to maybe providing some legislative fix. I yield back to the Chairwoman.

Mrs. MILLER. I thank the gentlelady. Any Members of the committee that might have some additional questions for the witnesses there, we will—pursuant to the committee rule, the hearing record will be open for 10 days for those.

Ms. GABBARD. Excuse me, Madam Chairwoman. Just briefly request——

Mrs. MILLER. Gentlelady from Hawaii.

Ms. GABBARD [continuing]. Unanimous consent to insert testimony we have here submitted for the record from the Longshore and Warehouse Union, representing port workers in Hawaii and the western region for the record.

Mrs. MILLER. Without objection.

[The information follows:]

STATEMENT OF THE INTERNATIONAL LONGSHORE AND WAREHOUSE UNION

JUNE 18, 2013

The International Longshore and Warehouse Union ("ILWU") represents port workers in California, Oregon, Washington, Alaska, and Hawaii, as well as warehouse, maritime, agriculture, and hotel and resort workers. The ILWU's membership includes the approximately 22,000 longshore workers, marine clerks and foremen who load, unload, track, monitor and oversee the movement of cargo into and out of all of the major ports on the West Coast, Alaska, and Hawaii. We appreciate the opportunity to submit these comments on the TWIC Program.

The ILWU and its members have been active participants in the development and roll-out of TWIC since its inception. The union's experience of the program and deep knowledge of the waterfront have shown that TWIC does not improve port security and unfairly burdens working people. The program is now at a crossroads. The program stands poised to expand through the mandatory installation of expensive

TWIC readers at approximately 570 locations pursuant to proposed regulations currently under review by the Coast Guard.[1] According to the GAO, the TWIC Program has cost more than $500 million and will cost between $690 million and $3.2 billion more over the next 10 years, not counting the costs of installing and operating readers.[2] In one of its multiple recent reports critical of the program, GAO concluded: "11 years after initiation, the TWIC program continues to be beset with significant internal control weaknesses and technology issues, and . . . the security benefits of the program have yet to be demonstrated. The weaknesses we have identified suggest that the program as designed may not be able to fulfill the principal rationale for the program—enhancing maritime security."[3] Before proceeding further, we urge this committee to re-think the wisdom of TWIC. We believe that careful consideration of the facts on the ground will reveal that TWIC does not make our Nation safer, hurts American workers, and is a poor use of limited Government dollars.

First, the fundamental focus of the TWIC program is wrong. If preventing terrorism is the goal, then targeting American workers for screening, as opposed to targeting containers and cargo, is the wrong approach. On the modern container facilities through which most of our imports and exports travel, port workers like those whom we represent have no real access to the cargo or the documentation associated with the containers' contents. Thus, requiring that workers be screened does not help to prevent facilities from being used to transport items that could be used to commit an act of terrorism.

Moreover, the majority of the facilities themselves (whether container terminals or bulk operations) are large, decentralized spaces with workers, cargo, and equipment typically spread out across many acres. These characteristics make the facilities poor targets for a terrorist hoping to have a significant impact on commerce or on the public. Thus, screening the facilities' workforces is not a meaningful way to prevent a terrorist attack.

Second, the TWIC program unfairly targets working people and has caused substantial hardships for workers and their families with no added security benefit. In 2006, when TWIC was still in the planning stages, ILWU longshore workers and marine clerks went through a Coast Guard-mandated threat assessment screening to ensure that they did not pose a National security risk.[4] The ILWU cooperated with the Coast Guard and TSA to complete this process. The ILWU is not aware of any members being found to pose a risk.

In 2008, when the Department of Homeland Security began to require TWICs to obtain unescorted access to longshore workplaces, the ILWU membership was screened again.[5] ILWU members applied for TWICs, were fingerprinted, had their irises scanned, underwent criminal background checks, and paid $129.75 each out of their own pockets to obtain these technologically-advanced cards. Almost none of these expensive technologies were ever put to use.

The Government databases relied upon in evaluating TWIC applications contain an abundance of incomplete and faulty information.[6] Due to this fact and delays by TSA, some of our members languished for months, unable to work, and unable to

---

[1] Notice of Proposed Rulemaking on TWIC Readers, 78 Fed. Reg. 56 (March 22, 2013) at 17782, et seq.

[2] "Transportation Worker Identification Credential: Card Reader Pilot Results are Unreliable; Security Benefits Need to Be Reassessed", GAO–13–198, Appendix III, p. 59–60 (May 2013).

[3] "Transportation Worker Identification Credential: Card Reader Pilot Results are Unreliable; Security Benefits Need to Be Reassessed", GAO–13–198, at p. 42 (May 2013); see also "Security Benefits Need to Be Reassessed," GAO–13–198 (May 2013); "Transportation Worker Identification Credential: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Objectives," GAO–11–657 (May 2011).

[4] 71 Fed. Reg. 82 (April 28, 2006) at 25067 (requiring the ILWU to provide the Coast Guard with identifying information, including Social Security Numbers and alien identification numbers for all longshoremen to permit TSA to "analyze . . . whether or not an employee or longshoreman poses or is suspected of posing a security threat warranting denial of access to the port facility" and stating that anyone meeting those criteria will be denied access).

[5] 72 Fed. Reg. 3492 (Jan. 25, 2007); 33 CFR §§ 101.514, 104.115(d).

[6] U.S. Attorney General, "The Attorney General's Report on Criminal History Background Checks," at page 3 (June 2006) (concluding that FBI's database was "missing final disposition information for approximately 50% of its records"); see also "A Scorecard on the Post 9/11 Port Worker Background Checks: Model Worker Protections Provide a Lifeline for People of Color, While Major TSA Delays Leave Thousands Jobless During the Recession," National Employment Law Project (July 2009), available at *http://www.nelp.org/page/SCLP/PortWorkerBackgroundChecks.pdf?nocdn=1.*

support their families while they tried to obtain TWICs.[7] The following are only a few examples:

- William Ericson, a lonsghore worker from Seattle was erroneously denied a TWIC based on incorrect or incomplete information in the notoriously flawed FBI database. Despite 12 years of work history on the waterfront, Brother Ericson sat unable to work for 6 months, exhausted his savings and came close to having his home foreclosed upon before he was able to finally convince TSA that the agency had made a mistake.
- Another member from Seattle, Steven Richards, was born outside of the United States on a military base. Even though he was a citizen and met all of the qualifications to obtain a TWIC, TSA denied his application. He found himself stuck in the bureaucratic snarl and unable to work for months while TSA obtained the records that proved his citizenship and eligibility.
- Another member in the San Francisco Bay Area was denied a TWIC because he had previously been convicted of a marijuana-related offense even though the court had expunged his conviction.[8] He had been a hard-working longshore worker for 18 years and had no other convictions. He spent months waiting for TSA to rule on his initial application and, then even longer waiting for TSA to review his request for a waiver. In the meantime, he was unable to work and his family struggled to avoid losing their home.

These members and others like them posed no risk to the security of the United States.

These members are not alone. The Department of Homeland Security reports that, as of May 21, 2013, it had issued initial TWIC disqualification letters to 120,224 people.[9] TSA has two procedures whereby someone can challenge the denial of a TWIC—appeal and waiver.[10] Appeal is available to an applicant who was wrongly denied a TWIC. In other words, the applicant met all of the statutory and regulatory criteria for obtaining a TWIC but TSA erroneously denied his or her application anyway.[11] Waiver can be sought by an applicant who does not meet all of the statutory and regulatory criteria for obtaining a TWIC but who nonetheless "does not pose a security threat."[12] As of May 21, 2013, DHS had received 54,271 appeals and had granted 52,299 (more than 96%). In addition, DHS had received 14,593 waiver requests and granted 12,289 (more than 84%). While these numbers indicate the absolute necessity of having an appeal and waiver process available, they also indicate that TSA initially denied TWICs to more than 50,000 people erroneously and to more than 12,000 people who posed no security threat. Almost certainly, there are tens of thousands more workers who met the requirements to obtain a TWIC but did not or could not appeal their denial or seek a waiver. These people are being wrongly denied access to work for no good reason.

Third, TWIC has shown itself to be of little to no value if the goal of the program is to limit facility and vessel access. As ILWU members like those discussed above struggled and were denied the ability to work for lack of a TWIC, the ILWU has watched as unknown truckers, rail crews, vessel crews, maintenance workers, and construction crews without TWICs routinely enter and work at marine terminal facilities. Sometimes these workers are "escorted" by people with TWICs. However, in many cases the "escort" is more theoretical than real and individuals without TWICs work on the facilities largely unmonitored. What is more, these workers have no lasting relationship with the facility owner or operator and therefore pose an arguably more serious security risk than ILWU members.

In addition, while ILWU members' backgrounds have been scrutinized in the name of National security, the union has watched waterfront employers eliminate people and protocols that actually improve security and replace them with cost-cutting technologies that are no substitute. For example, many marine terminal operators used to require that seals on stuffed containers be visually checked to ensure that they had not been tampered with. They also previously required that empty

---

[7] The National Employment Law Project, which represented or assisted more than 450 workers seeking to obtain TWICs estimated that workers waited almost 4 months on average to obtain an initial decision from TSA on their TWIC applications and workers waited an average of 7 months for their appeals or waiver requests to be reviewed. "A Scorecard on the Post-9/11 Port Worker Background Checks: Model Worker Protections Provide a Lifeline for People of Color, While Major TSA Delays Leave Thousands Jobless During the Recession," National Employment Law Project (July 2009), at p. at 5–6.

[8] To protect the member's privacy, we do not include his name.

[9] *http://www.tsa.gov/sites/default/files/publications/pdf/twic/monthly_dashboard_current.pdf.*

[10] 49 C.F.R. § 1515.6–1515.7.

[11] Id. § 1515.6(b).

[12] Id. § 1515.7(b).

containers be opened and checked. To cut costs and speed up the movement of cargo, many employers now use only a camera linked to a monitor at a remote location. But a camera cannot tug on the seals to make sure they are intact, or open empty containers.

The ILWU has been advised by some facility owners and operators that, if TWIC readers become mandatory, the employers intend to use the readers to further cut costs by eliminating security guards. Facility security personnel know the regular workforce on the docks and, therefore, know who belongs and who does not. Again, technology is no substitute, particularly given the serious flaws with TWIC card technology and readers noted by the GAO.[13]

For all of these reasons, TWIC is misguided. It does not improve port security and it unfairly targets working people. Public monies can and should be put to better use.

The ILWU appreciates the opportunity to submit these comments and thanks the committee for its consideration.

Ms. GABBARD. Thank you.

Mrs. MILLER. Again, thank you to the witnesses very much. The committee is now adjourned.

[Whereupon, at 11:25 a.m., the subcommittee was adjourned.]

[13] GAO–13–198, "Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed," (May 8, 2013) at 25 ("according to officials from two pilot sites, approximately 70 percent of the TWICs they encountered when testing TWICs against contactless readers had broken antennas or malfunctioned. Further, a separate 2011 report commissioned and led by USCG . . . identified one site where 49 percent of TWICs could not be read in contact-less (or proximity mode, and two other sites where 11 percent and 13 percent of TWICs could not be read in contact-less mode. Because TWIC cards malfunctioned, they could not be detected by readers.").

APPENDIX

QUESTIONS FROM CHAIRWOMAN CANDICE S. MILLER FOR JOSEPH A. SERVIDIO

Question 1. A Coast Guard official started in an interview with a Fierce Homeland Security reporter "there is not a real strong nexus between the results of the pilot program and what is in the reader regulation." However, the pilot was referenced several times in the NPRM. What data from the TSA pilot were used to inform the NPRM? Could this information have been provided through other means? How can the Coast Guard be certain the NRPM will not have negative impacts on business operations knowing that this system has not truly been tested? Had the TSA pilot been more complete or shown a strong feasibility in carrying out the biometric requirements of the TWIC program, would the rule have sought to regulate more than 5 percent of all MTSA-regulated vessels and facilities?

Answer. The Coast Guard used the best available data to characterize economic impacts, which in some cases resulted in using sources other than the TWIC pilot. Specifically, the TWIC pilot was the main data source associated with the cost to install TWIC readers, as well as the number of readers required per access point, throughput times, and failure rates of readers. However, TWIC pilot data was supplemented with other available data sources to provide preliminary estimates of other costs and benefits. Other data sources included the Marine Information for Safety and Law Enforcement (MISLE) database for population figures, the Marine Security Risk Assessment Model (MSRAM) for risk hierarchy and consequence data, the General Services Administration (GSA) schedule for reader hardware and software costs, and other literature for basic background on TWIC reader deployment. Based on the judicious use of all data sources, the Coast Guard has confidence in the proposed regulation's limited impact on business operations as noted in the Regulatory Assessment.

Decisions regarding application of TWIC reader requirements were not driven by any limitations of the TWIC pilot, but rather by comparing costs of the requirements versus benefits gained. In the case of vessels, given the inherent limits on manning for barges (and thereby the limited utility for using a reader to verify the identity of mariners accessing any secure spaces on a barge), barges were excluded from TWIC reader requirements, thus eliminating approximately 51 percent of the MTSA population (includes vessels and facilities). Similarly, other vessels with lower risk (e.g., vessels not engaged in transport of hazardous cargoes) and/or with fewer than 14 TWIC-holding crewmembers were eliminated given relatively low utility for the cost. This eliminated another 32 percent of the MTSA population (for a total of about 83 percent of the MTSA population exempted in the current proposal). Similar logic was applied to facilities, with requirements imposed on those 20 percent of MTSA facilities that comprised approximately 80 percent of the risk exposure. By eliminating lower risk facilities, another 13 percent of the MTSA population was exempted from requirements for a total of about 95 percent of the MTSA population exempted from reader requirements.

Question 2. Since 9/11, Congress has implemented legislation specifically addressing perceived vulnerabilities with containerized cargo entering the United States. However, no container facilities will fall within Risk Group A, and thus will not be impacted by the proposed reader regulations at this time. Does containerized cargo deserve to be in a higher-risk group, or are earlier concerns regarding the threat within containerized cargo overstated? If container facilities are a major vulnerability, why are they not widely impacted by the proposed card reader rule?

Answer. In the development of the NPRM, the Coast Guard evaluated TWIC reader requirements alternatives to those proposed in the NPRM including an alternative that would have required the installation of TWIC readers at Risk Group A facilities and all container facilities.

The Coast Guard considered this alternative because container facilities are perceived to pose a unique threat to the maritime sector due to the transfer risk associ-

ated with containers (i.e., there is a greater risk of a threat coming through a container facility and inflicting harm or damage elsewhere than with any other facility type). However, as discussed in the preamble of the NPRM, many of the high-risk threat scenarios at container facilities would not be mitigated by TWIC readers. Although TWIC readers serve as an additional access control measure, they do not mitigate the threat associated with the contents of a container, and would not improve screening of cargoes for dangerous substances or devices.

Additionally, the costs/impacts for TWIC readers at container facilities would not be justified by the amount of potential risk reduction at these facilities. This alternative would increase the burden on industry by increasing the affected population from 532 facilities to 651 facilities. The discounted 10-year costs would go from $186.1 million to $624.9 million. The inclusion of container facilities would also potentially have adverse environmental impacts due to increased air emissions due to longer queuing times and congestion at facilities.

Question 3. In recent years, many port facilities have designated Port Security Grant funds specifically to procure TWIC readers and other equipment associated with TWIC implementation. How many facilities not in Group A, have received funding for TWIC card readers and infrastructure? Is it your expectation that Group B and C facilities, which are not required to purchase card readers, will still go ahead with the investment? Did the Coast Guard take into consideration, while drafting the NPRM, whether or not risk Group B or C facilities have already obtained Port Security Grant funding to purchase card readers?

Answer. In the development of the TWIC Reader NPRM, the Coast Guard specifically focused on risk, security, and economic impacts rather than taking into consideration whether or not facilities had voluntarily purchased electronic TWIC Readers (with or without PSG funding). The Coast Guard expects that each facility in Groups B and C will make a determination on whether to implement readers based on what best meets its specific business and security needs and assessments. Absent of regulatory requirement, there is no expectation for B and C facilities to implement readers.

The PSG Program allocates funds towards maritime security risk mitigation projects based on risk. Eligible PSG applicants may request several different projects within an application of which a TWIC project may be one of the projects or part of a project.

PSG Program financial data is maintained via methodology established by Congress for Federal grant funding. From fiscal year 2007 through fiscal year 2012, a total of 401 TWIC implementation projects were approved by DHS, and a total of $144.7 million was awarded for TWIC projects. Funding awarded for TWIC projects represented 7.5% of the total PSG Program funding ($1.92 billion) awarded during the period.

Question 4. The crewmembers operating the Saugatuck Chain Ferry, out of Saugatuck, Michigan are required to carry a TWIC card. Given the low threat nature of this vessel as it operates on a fixed chain system propelled by a hand crank does it make sense for crewmembers of this vessel to be required to carry a TWIC card? Has there been any consideration to waive the requirement for crewmembers to obtain a TWIC card for vessels like this?

Answer. The Saugatuck Chain Ferry (also known as the M/V DIANE) is a Coast Guard inspected 46 CFR Subchapter 'T' small passenger vessel that operates on the Kalamazoo River (a navigable waterway). In accordance with Coast Guard Policy Letter 11–15, since the Saugatuck Chain Ferry does not meet the applicability requirements of maritime security for vessels (33 CFR 104.105) and therefore is not required to maintain a Vessel Security Plan (VSP), a credentialed mariner operating the vessel is not required to retain a Transportation Worker Identification Credential (TWIC).

However, individuals applying for their initial Merchant Mariner Credential (MMC) are required to apply for a TWIC in order to undergo a Security Threat Assessment (STA). Such persons would only need to pass the STA in order to obtain their MMC. There is no requirement for that individual to actually hold a valid TWIC unless they are working on a vessel required to hold a VSP. Additionally, the Coast Guard will not require a mariner who holds or has held a TWIC to renew it in order to renew their current credential.

Because of the Saugatuck Chain Ferry's route and service, the operator of the vessel is required to possess a Coast Guard issued MMC. The Coast Guard does not have the authority to waive this statutory requirement. Therefore, any person applying for their initial MMC who would like to then use that MMC to operate the Saugatuck Chain Ferry would have to apply for a TWIC in order to undergo a STA, but would not be required to carry the TWIC.

QUESTIONS FROM CHAIRWOMAN CANDICE S. MILLER FOR STEPHEN M. LORD

[*Note.*—The responses are based on work associated with our previously issued products.][1]

Question 1. Although TWIC was originally intended to be the common credential for workers in all modes of transportation, it has been limited to strictly a maritime security access control credential. The Coast Guard has further limited its scope by developing a Notice of Proposed Rulemaking (NPRM) which applies to less than 5 percent of all MTSA-regulated vessels and facilities. Given that the reader requirement is not being applied to Group B and C facilities should TWIC be further reduced by limiting issuance and use to only the highest-risk maritime facilities?

Answer. Given the current uncertainties surrounding the implementation of the TWIC program in the maritime environment, and the program weaknesses highlighted in our 2011 and 2013 reports, limiting the use of TWIC to maritime facilities where the Coast Guard can clearly demonstrate that use of TWIC will effectively mitigate the three terrorist scenarios illustrated in the March 2013 NPRM (i.e., a truck bomb, a person/passenger carrying an improvised explosive device (IED), or a terrorist assault team) would be consistent with our findings and recommendations.[2] As highlighted in our May 2013 report, the TWIC pilot conducted to test the use of TWICs with biometric card readers and other supporting analyses did not provide DHS with complete and accurate information on the impact of TWIC on facility and vessel operations or the added security benefits that the TWIC may provide.[3] For example, we found that the pilot test's results were unreliable, and that DHS has not assessed the effectiveness of TWIC at enhancing security or reducing risk at Maritime Transportation Security Act (MTSA)-regulated facilities and vessels. While the current NPRM is aimed at implementing the use of TWIC with readers at Group A/highest-risk-vessels and facilities, the NPRM suggests allowing for the expanded use of TWIC with readers at lower-risk facilities in the future.

Question 2. DHS argues that the decentralized security credential similar to the airport's Secure Identification Display Area (SIDA) badge is not comparable to TWIC because airport workers generally work at only one airport and disagrees with the GAO assessment that "maintaining site-specific credentials enhances security." Why do you believe decentralized security "enhances security?" What examples of such a decentralized approach would you recommend DHS evaluate for use at port facilities?

Answer. Based on findings from our prior work, a decentralized credentialing approach could help remediate internal control weaknesses identified in our May 2011 report, and may therefore enhance security.[4] Among others, we reported that TWIC program controls are not in place to determine whether an applicant has a need for a TWIC, and that our investigators were successful in obtaining authentic TWIC cards despite going through the background-checking process. As implemented, a uniform TWIC credential is issued by TSA after it conducts a security threat assessment. Operator participation is not required as part of this centralized TWIC enrollment, security review, or issuance process. According to our review of the evidence, operator participation, as would be required under a decentralized credentialing approach using facility- or port-specific credentials, could help validate an individual's identity and need for a credential to access a specific facility or vessel prior to issuing the credential. Maritime vessel and facility operators have a paramount interest in securing their assets. Involving operators in the credentialing process gives them more control and insight into the risks posed by people seeking access to secure areas, and could better ensure operators and the Federal Government of the individual's identity, need for a credential, and need for access to specific vessels and facilities.

As we reported in May 2011, the TWIC program's internal controls for positively identifying an applicant, arriving at a security threat determination for that indi-

---

[1] See GAO, *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed,* GAO–13–198 (Washington, DC: May 8, 2013); *Transportation Security: Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload,* GAO–12–60 (Washington, DC: Dec. 8, 2011); *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives,* GAO–11–657 (Washington, DC: May 10, 2011); *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives,* GAO–11–648T (Washington, DC: May 10, 2011); and *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers,* GAO–10–43 (Washington, DC: Nov. 18, 2009).

[2] GAO–11–657 and GAO–13–198.

[3] GAO–13–198.

[4] See, for example, GAO–13–198; GAO–12–60; and GAO–11–657.

vidual, and approving the issuance of a TWIC, are not designed to provide reasonable assurance that only qualified applicants can acquire TWICs. If an individual presents an authentic TWIC acquired through fraudulent means when requesting access to the secure areas of a MTSA-regulated facility or vessel, the cardholder is deemed not to be a security threat to the maritime environment because the cardholder is presumed to have met TWIC-related qualifications during a background check. In such cases, these individuals could inappropriately gain unescorted access to secure areas of a MTSA-regulated facility or vessel, as our investigators did for our May 2011 report and again for our May 2013 report.

Through our work on the TWIC program, we have not identified any industry-wide common credential—beyond TWIC—that is used as a security tool for controlling access to individual, and often privately-owned, entities. Moreover, the Federal Government, which provides access to its many departments and agencies, does not use a single identification credential for controlling access to its facilities and vessels. Under the Federal model, agencies apply a standard for conducting background checks and creating the credentials. For example, as we reported in May 2011, TWIC is unlike other Federally-sponsored access control credentials, such as the Department of Defense's Common Access Card—the agency-wide standard identification card—for which sponsorship by an employer is required. For these Federal credentialing programs, employer sponsorship begins with the premise that an individual is known to need certain access as part of his or her employment. Further, the employing agency is to conduct a background investigation on the individual and has access to other personal information, such as prior employers, places of residency, and education, which it may confirm as part of the employment process and use to establish the individual's identity. According to our analysis, use of a decentralized credentialing approach could enhance the TWIC program's identity verification, vetting, and issuance controls by leveraging the employer and operator's knowledge of the individual's background and need for an access credential prior to conducting the Federal security threat assessment required as part of the TWIC program. In addition, localized control over credential issuance could enhance security by making it easier for individuals to replace lost or nonfunctioning credentials on site, and forgo potential travel times and waiting periods currently experienced under the TWIC program.

Similarly, the decentralized aviation model may enhance security to a greater extent than the TWIC because this model includes employer sponsorship, background vetting at the local level, a Federal security threat assessment, and card revocation at the local level. For example, based on our prior work, in order to receive a SIDA, a person seeking a credential is sponsored by a previously vetted and authorized individual within the airport. This process provides greater assurance that the person seeking the credential has a real need for the credential and that the person is the person he or she claims to be on the application. Further, since the credential is valid only within a given airport, the person holding the credential cannot use that credential to access other airports where he or she has no legitimate need to gain access. As demonstrated by our covert tests, having a TWIC provided the appearance of legitimacy for our testers and allowed them to access multiple facilities with a single card. Moreover, the SIDA vetting process allows local airport authorities to see the criminal background check information pulled by DHS from the Federal Bureau of Investigation (FBI). Airport authorities use this information to make the determination about whether to grant or deny a credential. This allows the totality of an individual's criminal background to be considered, not just disqualifying offenses. We found that the Transportation Security Administration (TSA) has the authority and discretion to do this for the TWIC program but has seldom done so as part of the adjudication process.[5] Consequently, under the SIDA model, airport authorities have greater control and ability to watch over the vetting process. Similarly, when local credentials are granted by local authorities, they can be customized for the unique needs of the facilities and can be revoked by the facilities, thus providing the facilities with greater control. As we found during our December 2011 work on local credentialing programs, when Florida repealed provisions of law requiring workers accessing the State's 12 active deepwater public ports to undergo a State criminal history records check, individuals with criminal backgrounds who were kept out of the ports were allowed to return to work because they possessed a TWIC.[6]

Regarding TSA's assertion that the lack of a common credential across the industry could leave facilities open to a security breach with falsified credentials, DHS has not provided or discussed with us any studies or evidence showing that use of

[5] GAO–11–657.
[6] GAO–12–60.

a centralized common access credential enhances security beyond use of port- or facility-specific credentials supplemented by a Federal security threat assessment. As we reported in May 2011, unlike prior access control approaches that allowed access to a specific facility, the TWIC potentially facilitates access to thousands of facilities once the Federal Government attests that the TWIC holder has been positively identified and is deemed not to be a security threat. Further, DHS argues that the aviation industry's SIDA badge is not comparable to TWIC because airport workers generally work at only one airport. However, during the course of our work, DHS did not provide us with analysis on the number of TWIC holders that are "transient" or for whom a local port-specific credential(s) could necessitate the need for multiple credentials. Further, DHS did not provide us with analysis demonstrating that the majority of people seeking access to maritime facilities require more access control credentials than individuals working in the airport environment, or showing the extent to which requiring multiple access control credentials negatively affects security. Use of a single credential to access thousands of maritime facilities Nationwide may prove to be more convenient for certain individuals or segments of the transportation industry. However, the TWIC program's primary intention is to enhance security. Given the lack of validated analysis available to support DHS's position on the security merits of using a common credential such as TWIC instead of a local port- or facility-specific credential supplemented by a Federal security threat assessment, we continue to believe that our May 2011 recommendation to DHS that it conduct an effectiveness assessment of the TWIC program, has merit and should be implemented. We also continue to believe that our May 2013 suggestion to Congress that it consider requiring that DHS complete such an assessment, including a comprehensive comparison of alternative credentialing approaches, which might include a more decentralized approach for achieving TWIC program goals, before implementing a final regulation requiring the use of TWIC cards with biometric readers, has merit and should be implemented.

Question 3. Considering the numerous delays and tribulations with the TWIC program over the past 11 years would the Department be able to produce a better product if only one component was responsible for the entire program?

Answer. It is unclear that making one component responsible for the entire TWIC program would enhance the program at this time. The Coast Guard has primary responsibility for ensuring the safety and security of maritime ports and has individuals stationed at the ports, among other things. However, TSA manages the resources for conducting required security threat assessments for TWIC and other transportation-related credentials. Therefore, moving the security threat assessment function to the Coast Guard may create duplication, though we have not conducted work in this area.